



Delinea

Privilege Manager

Documentation © 10.7.x



Table of Contents

Introduction to Privilege Manager	32
10.7.1 Cloud Specific	32
Product Overview	33
Privilege Manager Cloud - Layered Diagram	33
<i>Network Diagram (Cloud)</i>	33
Privilege Manager On-premises - Layered Diagram	34
<i>Network Diagram (On-prem)</i>	34
Least Privilege Explained	36
Integration with Secret Server	37
Component Definition	37
Single Site - Implementation Diagrams	37
<i>Minimum High Availability</i>	37
<i>Minimum High Availability (RabbitMQ Separation)</i>	38
<i>Minimum High Availability/DR - Lowest Cost</i>	40
Multi Site - Implementation Diagrams	41
<i>Average High Availability/DR (RabbitMQ Separation)</i>	41
<i>Best High Availability/DR (RabbitMQ Separation)</i>	43
<i>Best High Availability/DR (RabbitMQ Separation) - Highest Cost</i>	44
Feature Overview	46
Active Directory and Azure Active Directory	46
Agent & OS Reports	46
Application Discovery for Administrative or Root Privileges	46
Automated Local Account Password Rotation	46
Centralized Application & Execution Event Logging	46
Child Process Control	46
Custom & Scheduled Reports	46
Define Local Group Membership	46
End-user Justification & Admin Approval Workflow	46
Flexible Policy Deployment Configuration	46
High Availability & Load Balancing	46
Local Admin Rights Removal	46
Local User Account Management	46
Local User & Group Activity Auditing	46
Privilege Manager Mobile App	46
Real-time Application Analysis Reputation Check	46
Responsive & Actionable Reporting Dashboard	46

Reverse Proxy	46
Sandboxing	47
ServiceNow	47
Symantec Enterprise Platform (SEP)	47
SysLog / SIEM	47
System Center Configuration Manager (SCCM)	47
Tailored Block, Elevation, Justification, and Monitoring Policies	47
User Account Control (UAC) Override	47
Windows & Mac Account Discovery on Endpoints	47
Glossary	48
Getting Started Overview - On-premises	50
Preliminary Configuration	50
Rollout Recommendation	50
Local Security	50
Application Control	50
Integrations	50
Reports & Troubleshooting	50
Catalogs & Reference Guides	50
Getting Started Overview - Cloud	51
<i>Rollout Recommendation</i>	51
<i>Local Security</i>	51
<i>Application Control</i>	51
<i>Integrations</i>	51
<i>Reports & Troubleshooting</i>	51
<i>Catalogs & Reference Guides</i>	51
Cloud Quickstart Guide	52
<i>Initial Setup</i>	52
<i>Getting Started Screen</i>	54
Privilege Manager Cloud Login	55
Initial Login	57
Getting Started Banner	57
Home	57
Licensing	59
Cloud Licenses	59
Installing New Licenses - On-premises Only	59
<i>Steps for Standalone Privilege Manager Installation</i>	59
<i>Steps for Combined Secret Server + Privilege Manager Installation</i>	59
Converting from Trial Licenses	59
Expired Licenses	59
Client vs. Server Licenses	59

<i>When a license has expired or have exceeded the license count</i>	59
10.7 and up Reset Licensing	60
Installation and Upgrades	61
Privilege Manager System Requirements	62
Minimum Requirements	62
Recommended Requirements	62
Client Requirements	62
Details	62
Ports/Agent Access Information	62
Anti Virus Exclusions	63
Directories	63
Exclusions for Web Server	63
<i>Temporary ASP.NET Files</i>	63
Exclusions for Database Server	63
<i>SQL Server Data Files</i>	63
<i>SQL Server Backup Files</i>	63
<i>SQL profiler trace files</i>	63
Exclusions for Managed Endpoints	63
<i>Request Run As Administrator Registry Key</i>	63
<i>Client Item Database</i>	63
<i>Privilege Manager Application Control Agent Service</i>	63
Software Downloads	64
Product Installation - Basic	65
<i>Prerequisites</i>	65
ASP.NET Website	65
SQL Server Database	65
Administrative Access	65
Additional Recommendations	65
<i>Download the Latest Version of PM Installer</i>	65
<i>Running the Installer</i>	65
Manual Installation	70
<i>Download Privilege Manager Application Files</i>	70
Zip File Extraction Tool	70
<i>Manual Installation (no setup.exe)</i>	70
Installing as a Virtual Directory	70
Integrated Security=False	71
Integrated Security=True	71
<i>Continue: Installing as a Virtual Directory</i>	71
Installing as a Website	74
<i>Completing Privilege Manager Installation from Website</i>	74

Item Encryption	75
<i>What this means for Privilege Manager</i>	75
Agent Installation	76
Agent Install Codes	77
Agent System Requirements	78
<i>Supported Windows Operating Systems (both 32- and 64-bit):</i>	78
<i>Windows Management Framework download locations</i>	78
Windows Management Framework 2.0 or newer	78
.NET 4.0 Framework or newer	78
.NET 2.0 Framework SP1	78
Bundled Install	79
<i>Rollout to Multiple Systems</i>	79
<i>Agent Diagnostics</i>	79
Windows Agents	81
<i>Individual Agent Installers for Privilege Manager</i>	81
Hardened Agents	81
64-bit Windows Operating Systems	81
<i>Installation Command Lines</i>	81
32-bit Windows Operating Systems	81
<i>Installation Command Lines</i>	81
macOS Agents	82
<i>Installing macOS Agents</i>	82
Directly	82
Using an Unattended Install Method	82
<i>Network File Share</i>	82
<i>Distribution Tool</i>	82
<i>After Initial Deployment</i>	82
<i>Uninstalling an Agent</i>	82
Agent Uninstall via Command Line	84
<i>Manual Uninstall Steps</i>	84
Upgrades	85
<i>Setting up the NuGet Source</i>	85
<i>Updating Privilege Manager</i>	85
Primary Node	85
Secondary Nodes	86
Offline Upgrades	87
Offline Upgrades - Combined	88
Upgrading from Arellia Management Server 8.2 to Privilege Manager 10.4 and up	89
<i>Automatic Steps</i>	89
<i>Manual Steps</i>	89

Legacy System Extensions	90
Effect on Privilege Manager Customers by Apple Deprecating Kernel Extensions in macOS	90
How is this Going to Affect Privilege Manager?	90
Privilege Manager Agents	91
Agent Hardening (Windows)	91
Post Agent Installation	91
Diagnostics	91
Agent Encryption	91
Pertaining to All Agents	92
Setting the Privilege Manager Server Address	93
<i>Setting the Privilege Manager Server (TMS) Address via PowerShell</i>	93
<i>Changing the Privilege Manager Server (TMS) Address via the Registry Editor</i>	93
Connecting Agents to the Privilege Manager Sever	94
<i>Un-Installing Old Templates</i>	96
Agent Trust Revocation	97
Agent Uninstall Script	98
<i>Using a PowerShell Script to Uninstall an Agent</i>	98
How to prevent Backwards Compatibility for Agents v10.4 and earlier	99
<i>Resolve</i>	99
Configuring for a Test Environment	100
Agent Specific Tasks	102
<i>Windows Remote Client Scheduled Commands</i>	102
<i>MacOS Remote Client Scheduled Commands</i>	102
Agents on Windows Systems	103
Agent Hardening 10.7.1 and up	104
<i>Editing the Restrict Account Permissions on Agent Services (Windows) Policy</i>	104
Pre-10.7.1 Agent Hardening	106
<i>Editing the Agent Service Start / Stop Control (Windows) Policy</i>	106
<i>Restore Default Agent Permissions</i>	106
Agents on macOS Systems	109
Modify Update Agent Commands (MacOS) Policy	110
Finding Logs for Troubleshooting	111
Terminal Commands	112
<i>Command Usage</i>	112
The Privilege Manager UI	113
Gauges	113
<i>What is a Gauge?</i>	113
<i>Reports and Gauges Currently Available</i>	113
Alerts	114
Alert Notifications	115

<i>Endpoint Specific Alerts</i>	115
Configuration	116
<i>Advanced Tab</i>	117
<i>File Inventory Solution</i>	118
<i>General System Settings</i>	119
Allow Agent Certificate Mismatch	119
Maximum Application Event Count	119
Command Timeout	119
Encryption Provider	119
Inactivity Timeout	119
Max Time Skew	119
Prevent Legacy Agent Registration (10.4 and older)	119
Save Performance Counters	119
Session Timeout	119
<i>Session Timeout Warning</i>	119
System Secret Vault	120
Validate Agent Event Signatures	120
<i>Monitor Settings</i>	121
Base Local Address	121
Monitor Worker Role	121
Ping Interval	121
Timeout	121
<i>Proxy Settings</i>	122
Proxy Server	122
Proxy Server Credential	122
Port	122
Use Proxy Server	122
<i>ServiceBus Settings</i>	123
Connectivity Mode	123
<i>Authentication Tab</i>	124
<i>Credentials Tab</i>	125
<i>User Credentials and Roles</i>	126
Create User during Installation	126
<i>Discovery Tab</i>	127
<i>Foreign Systems Tab</i>	128
<i>General Tab</i>	129
Policy Targeting	129
Approval Types	129
Approval Processes	129
Markdig.Syntax.Inlines.LinkInline	129

<i>History Tab</i>	130
Looking at Details	130
<i>Drilling Down</i>	130
Item Change History Report	131
<i>Reputation Tab</i>	132
Cylance Rating Provider	132
VirusTotal Rating Provider	132
<i>Roles Tab</i>	133
Privilege Manager Administrators	133
Privilege Manager Field Engineering	133
Privilege Manager Helpdesk Users	133
Privilege Manager MacOS Administrators	133
Privilege Manager Users	133
Privilege Manager Windows Administrators	133
<i>Application Roles</i>	134
<i>Users Tab - Cloud Only</i>	135
How to Add Thycotic One Users Manually	135
Diagnostics Page	137
MacOS Specifics & Best Practices	138
Best Practices System Preferences	139
<i>Error Behavior of Preference Panes</i>	139
<i>User Based Behavior of Preference Panes</i>	139
Standard User	139
Admin User	139
Best Practices Printer Installs	140
Date & Time Preference Pane	141
<i>Standard User - System Defaults</i>	141
<i>Standard User - Managed by Policy</i>	141
<i>Local Administrator User - Not Managed by a Policy</i>	141
Energy Saver Preference Pane	142
<i>Standard User - System Defaults</i>	142
<i>Standard User - Managed by Policy</i>	142
<i>Local Administrator User - Not Managed by a Policy</i>	142
Network Preference Pane	143
<i>Standard User - System Defaults</i>	143
<i>Standard User - Managed by Policy</i>	143
<i>Local Administrator User - Not Managed by a Policy</i>	143
Preference Pane macOS	144
<i>Targeting Preference Panes</i>	144
<i>Catalina Preference Pane Behavior</i>	144

Menu Customization	145
Resource Explorer	146
<i>Example for Discovered Files</i>	146
<i>Example for User Resource</i>	149
<i>Error Message after Deleting a User Resource</i>	150
Tools Menu	151
File Upload	152
Password Disclosure	153
<i>Using the Disclose Password Tool</i>	153
Local Security	155
Computer Groups	155
Local Groups	155
Local Users	155
Local Security Home screen	155
Computer Groups	156
Create New Computer Group	156
<i>Computer List</i>	156
<i>Collection</i>	157
<i>OU (Organization Unit)</i>	157
<i>Security Group</i>	157
Local Groups	158
Create New Local Group	158
Manage Local Groups	158
Local Users	160
Create New Local User	160
Manage Local Users	160
Randomize Local Account Passwords	160
Shared Folder Inventory	162
Enable the Policy	162
Disable Local Guest Accounts	163
Logon User Tracking	164
Viewing the Resource	165
macOS Secure Token	166
Agent Configuration	166
Password Management	168
Reports Relating to Managed Accounts	170
Active Directory Synchronization	171
Set-up AD Default User Credential	171
Setup Foreign Systems	171
Setting up Scheduled Synchronization Task	172

Viewing Imported Users and Groups	173
Migrate Local Security Policies	174
Migration Steps	174
Personas	176
Viewing your Personas	176
Creating a Persona	176
Application Control	178
Dashboard	178
Policies	179
<i>Using Policy Templates</i>	179
<i>Overview of the Configuration Process</i>	179
<i>Collecting File Data</i>	179
<i>Points to Consider</i>	179
Sending Policies to Endpoints	180
<i>View Deployment Status</i>	180
<i>Update Policies on an Endpoint using Powershell (prior version 10.7)</i>	180
<i>Agent Event Log Viewer</i>	181
Learning Mode Policies	182
<i>Discover Applications that Require Administrator Rights</i>	182
macOS specific Support 10.7 and up	182
<i>Discover All Events on Test Endpoints</i>	182
<i>View Policy Results</i>	183
<i>View Files</i>	183
<i>New Loaded Resource</i>	183
Application Control Events	185
Events	185
<i>Storage and Manual Purging of Events</i>	185
Manually Purge Events	185
<i>Maximum Event Count Option</i>	187
Maximum Event Count: Basics	187
Maximum Event Count: Additional Information	188
Best Practices	189
<i>What's First</i>	189
Event Discovery	189
Never Disable Event Discovery	189
<i>Purpose of Event Notifications</i>	189
<i>Best Practices</i>	189
<i>Examples</i>	190
Send Policy Feedback	190
Don't Send Policy Feedback	190

Priority	191
<i>Why Policy Priority Matters</i>	191
Deny MMC.EXE Policy setup	191
<i>Allow specific MMC Snap-in</i>	191
<i>Test this use case</i>	191
Agent Policy State	192
Using RegEx in Policies and Filters	193
<i>Special RegEx Characters</i>	193
Escape Example	193
Wildcard Example	193
<i>File Name Examples</i>	193
Match with Wildcard before the File Name	193
Match File Name Containing String and File Type	193
Match with Wildcard at end of File Name and before File Type	193
Match with Wildcard in the Middle of Two Strings	193
Match with Wildcard at End of File Type	193
<i>File Path Examples</i>	193
Wildcard at the End of the Path	193
Wildcard in IP Address for Network File Path	194
Wildcard for Application Updates for all Users	194
<i>Example Policies</i>	195
Approval Policies	196
Offline Approvals	197
<i>Creating an Offline Approval Policy</i>	197
<i>Endpoint Offline Approval</i>	197
<i>Privilege Manager Offline Approval</i>	198
Help Desk Approvals	200
<i>Creating a Helpdesk Policy</i>	200
<i>Workflow</i>	201
<i>Approve requests</i>	201
Google Authenticator	202
XML for Challenge Response Message Action	203
Whitelisting Policies	206
Google App with File Upload	207
MS Security Catalog	208
Elevation Policies	209
Setting up ActiveX Policies	210
<i>Overview</i>	210
<i>Creating the Policy</i>	210
<i>Task and Resource Targeting</i>	210

<i>Configure the Triggers and the Targets</i>	211
<i>Test the Policy</i>	212
MS Visual Studio Installations	213
<i>Import the XML Example</i>	213
<i>Background Notes</i>	213
<i>XML Example Code</i>	213
Elevate MSI Files on the Network Share	216
<i>Option 1</i>	216
<i>Option 2</i>	216
Network Share Applications	219
<i>Applying Administrator Rights to a Network Share</i>	219
<i>Creating the Filter</i>	219
<i>Creating the New Policy</i>	219
<i>Using the UNC Elevation Policy Template</i>	219
UAC Override Policy	221
<i>Using the Default Policy</i>	221
Elevating the Privilege Manager Remove Programs Utility Policy	223
Application Execution Requires Approval	224
<i>Create a workflow policy to assign to this filter</i>	225
<i>To Approve Requests</i>	227
User Justification Required to Run	228
<i>How to Create the Policy</i>	229
<i>To adjust this policy to apply to specific users or endpoints</i>	230
Monitoring Policies	231
Catch-All Policy	232
Reputation Checking	234
<i>Creating Security Rating Filter</i>	234
<i>Creating User's Downloads Location, Temp Dir, and Collection Filters</i>	235
<i>Creating a Policy</i>	236
<i>Viewing a File Security Ratings Report</i>	237
Blocking Policies	238
Catch-all Deny	239
iTunes with File Upload	240
Quarantine Specified Malware	241
Specific Applications	242
macOS Specific Policies	243
<i>Actions supported by macOS Agents</i>	243
<i>Available Topics</i>	243
Allow Copy to Install Applications	244
<i>Updating Existing Policies to Use the Copy Install Application Filter</i>	245

Deny Photos Application	246
<i>Event Discovery</i>	246
<i>Assign to Policy</i>	247
<i>Policy Verification</i>	249
<i>Create a Filter Only</i>	249
Determine Admin Requirement	250
Require Justification - FireFox	252
Request Application Installation	253
Application Self-elevation	254
<i>Configuring Application Self-elevation</i>	254
<i>How to Request an Application Run as Administrator</i>	254
<i>Troubleshooting: Verify the Finder Extension is Installed</i>	254
Adding macOS Agents to a Computer Testing Group	256
<i>Setting Up Learning Mode Policies for macOS</i>	256
Inventoring .pkg Files	257
List of Default Policies	258
<i>Process Hardening</i>	258
<i>System Options</i>	258
<i>Privilege Management</i>	258
<i>Application Analysis</i>	258
<i>Windows Policies</i>	258
<i>macOS Policies</i>	258
<i>Automatic Elevation via Windows Client System Settings</i>	259
<i>ActiveX</i>	259
<i>Firewall</i>	259
<i>General</i>	259
Not Enabled	260
Filters	261
<i>Types of Filters</i>	261
<i>Creating New Filters using Event Discovery</i>	262
Creating a New Filter Manually	262
<i>Creating macOS Filters Manually</i>	262
Create A Copy - How to Use Filter Templates	262
<i>Filter Types and Descriptions</i>	263
Common Filter Characteristics	263
Application Filters	264
Blank Win32 Executable Filter	265
<i>Parameters</i>	265
<i>Examples</i>	265
Commandline Filter	266

<i>Search for Commandline Filters</i>	266
<i>Create a new Commandline Type Filter</i>	266
<i>Parameters</i>	267
<i>Examples</i>	267
Download Source Filter	268
<i>Parameters</i>	268
<i>Examples</i>	268
Environment Variable Filter	269
<i>Parameters</i>	269
<i>Examples</i>	269
Network Location Filter	270
<i>Parameters</i>	270
<i>Examples</i>	270
Parent Process Filter	271
<i>Parameters</i>	271
<i>Examples</i>	271
Using Secondary File Filters	272
<i>Batch File Example</i>	272
<i>Creating the File Filter for .bat Files</i>	272
<i>Creating the Secondary Filter</i>	272
<i>Creating the Policy</i>	273
<i>PowerShell Script Example</i>	274
<i>Creating the File Filter for .ps1 Files</i>	274
<i>Creating the Secondary Filter</i>	275
<i>Creating the Policy</i>	276
<i>MSI File Example</i>	277
<i>Creating the File Filter for .msi Files</i>	277
<i>Creating the Secondary Filter</i>	278
<i>Creating the Policy</i>	279
<i>Best Practices</i>	280
<i>Creating the Allow notepad</i>	280
<i>Creating the Secondary Filter</i>	281
<i>Creating the Allow a Specific .msi File to Run Policy</i>	282
<i>Creating the .msi Deny Policy</i>	283
<i>Updating the Endpoints with the Policies</i>	284
<i>RegEx Examples</i>	284
Security Rating Filter	285
<i>Parameters</i>	285
<i>Examples</i>	285
Signed File Filter	286

<i>Parameters</i>	286
<i>Examples</i>	286
Time of Day Filter	287
<i>Parameters</i>	287
<i>Examples</i>	287
Using User Context Filters	288
<i>On-Premise</i>	288
<i>Cloud</i>	288
File Filters	290
Application Compatibility Filter	291
<i>Examples</i>	291
Application Manifest Filter ("Manifest Filter")	293
<i>Examples</i>	293
File Collection Security Catalog Filter	295
<i>Parameters</i>	295
File Existence Filter	296
<i>Parameters</i>	296
File Owner Filter	297
<i>Examples</i>	297
File Specification Filter	299
<i>Example</i>	299
File Type Filter	301
<i>Parameters</i>	301
Internet Zone Filter	302
<i>Parameters</i>	302
Security Catalog Filter	303
<i>Parameters</i>	303
Unable to Access Cortana and Search for Windows 10	304
<i>How to Resolve</i>	304
Inventory Filters	306
File Collection from List of Sha1 Hashes Filter	307
<i>Parameters</i>	307
File Scan Results Filter (Computer)	309
<i>Parameters</i>	309
File Scan Results Filter (Policy)	310
<i>Parameters</i>	310
MSI File Contents Filter	311
<i>Parameters</i>	311
<i>Viewing and Editing the Parameters</i>	311
<i>Viewing and Adding the Resource(s)</i>	311

MSI Package Contents Filter	313
<i>Parameters</i>	313
<i>Viewing and Editing the Parameters</i>	313
<i>Viewing and Adding the Resource(s)</i>	313
Package Contents Filter	315
<i>Parameters</i>	315
<i>Viewing and Editing the Parameters</i>	315
<i>Viewing and Adding the Resource(s)</i>	315
Security Catalog Contents Filter	317
<i>Parameters</i>	317
Virtual Disk File Contents Filter	318
<i>Parameters</i>	318
<i>Viewing and Editing the Parameters</i>	318
<i>Viewing and Adding the Resource(s)</i>	318
Virtual Disk Package Contents Filter	320
<i>Parameters</i>	320
<i>Viewing and Editing the Parameters</i>	320
<i>Viewing and Adding the Resource(s)</i>	320
MacOS Specific Filters	321
<i>List of MacOS Filters</i>	321
<i>Application Filter Types</i>	321
<i>File Filter Types</i>	321
<i>List of Default Filters for Event Discovery</i>	321
<i>Available Preference Pane Filters</i>	321
App Bundle Filter	322
<i>Pre-10.7.1 Example</i>	322
<i>Parameters</i>	322
<i>Info.plist Example for Photos</i>	323
Default App Bundles File Specification Filter	324
<i>Example</i>	324
Default File Specification (MacOS)	326
<i>Example</i>	326
<i>Preference Pane Filters</i>	328
<i>Date and Time Preference Pane Filter</i>	329
<i>Energy Saver Preference Pane Filter</i>	330
<i>Network Preference Pane Filter</i>	331
Default Applications Folder (MacOS)	332
System Applications Folder (MacOS)	333
Default Applications Bundle Filter (MacOS)	334
macOS Executables	335

System Applications Bundle Filter (MacOS)	336
Resource Targets and Collections	337
<i>User Defined Resource Targets</i>	337
Interface to View or Create/Modify User Defined Targets	337
<i>Target Definition</i>	337
Operation	337
List Type	337
<i>Performance Considerations</i>	338
<i>Active Directory as Related to Resource Targets</i>	338
<i>Assigning Policies to Targets</i>	338
<i>Collections</i>	338
List of Default Filters	339
<i>Win32 Executable Filters</i>	339
<i>Commandline Filters</i>	340
<i>Environment Filters</i>	340
<i>Network Location Filters</i>	340
<i>Parent Process Filters</i>	340
<i>Secondary File Filters</i>	341
<i>Security Rating Filters</i>	341
<i>Time of Day Filters</i>	341
<i>User Context Filters</i>	341
<i>File Filters</i>	341
Application Compatibility File Filters	341
Manifest Filters	341
File Owner Filters	341
File Specification Filters	342
Security Catalog Filters	343
<i>Miscellaneous Filters</i>	343
App Bundle Filters	343
Coff Header Filters	343
File Parameter Collections	343
Mach-O Header Filters	343
Actions	344
<i>Creating a New Action Manually</i>	344
<i>Message Actions</i>	345
Basic vs. Advanced Messages	345
Types of Advanced Message Actions	345
<i>Advanced Feedback Messages</i>	345
<i>Authentication Justification Message Action</i>	345
<i>Group Member Authenticated Message Action</i>	345

<i>Justify Application Elevation Action</i>	345
<i>Justify Application Message Action</i>	346
<i>Approval Request Messages</i>	346
<i>Approval Request Form Action</i>	346
<i>Approval Request (with Offline Fallback) Form Action</i>	346
<i>No Required Input Messages</i>	347
<i>Application Denied Message Action</i>	347
<i>Application Denied Notification Action</i>	347
<i>Application Warning Message Action</i>	347
Types of Basic Messages	348
<i>Deny Execute Message</i>	348
<i>Deny Files Read and Write Access Message</i>	348
<i>Windows Hooking Message</i>	348
<i>Limit Process Rights for New Applications Message</i>	348
<i>Remove Rights Message</i>	348
<i>Quarantine Message</i>	348
<i>Display User Message Action</i>	349
Parameters	349
Examples	349
<i>Deny Execute Message</i>	350
Customization	350
<i>Display Advanced Message Action</i>	352
Parameters	352
Examples	352
<i>Create Custom Notifications</i>	353
Enable View as XML	353
Customizing the Application Denied Notification Action	353
Editing the Text in the UI	355
Editing the Text via XML	355
Updating the Policy with the new Action	356
<i>For Privilege Manager Versions Prior to 10.7</i>	357
<i>Display Advanced User Message Action (MacOS)</i>	359
Parameters	359
Adjust Process Rights Action	360
<i>Adjust Process Rights Action Settings Explained</i>	360
What is a Restricted SID?	360
<i>When to use restricted ID</i>	360
<i>Using Apply Restricted SID</i>	360
How to Add Windows Permissions	360
How to Use Well-known Accounts	360

<i>Example Scenario</i>	361
<i>Additional Options Explained</i>	361
Enabling Unrestricted Token Use	361
<i>Adjust Process Right for Resource Monitor</i>	361
Related Item - Policy	361
ActiveX Installer Action	363
<i>Parameters</i>	363
Allow Copy Action (MacOS)	364
<i>Parameters</i>	364
Application Classification Action	365
Apply Application Compatibility Fix Action	366
<i>Parameters</i>	366
Deny Execute Action	367
<i>Deny Execute Message</i>	367
Deny File Access Action	368
<i>Parameters</i>	368
<i>Deny Files Read and Write Access Message</i>	368
Deny Windows Hooking Action	369
<i>Windows Hooking Message</i>	369
Encrypt Application Files Action	370
<i>Parameters</i>	370
Execute Application Action	371
<i>Parameters</i>	371
Sandbox Action	372
Set Environment Variable Action	373
<i>Parameters</i>	373
Set Process Security Descriptor Action	374
<i>Parameters</i>	374
List of Default Actions	375
<i>Actions Catalog</i>	375
Adjust Effective Process Rights Action	375
Adjust Process Rights Action	375
Allow Copy Action	375
Application Verifier Action	375
Apply SVS Layer Action	375
Advanced Message (Windows)	375
De-elevate Child Processes	375
Deny Actions	375
Display Advanced Message Actions	376
Display User Message - Basic	376

Encrypt Application Files	376
Execute Application Action	376
Enable UAC Virtualization	376
Meter Application Action	376
Quarantine File Action	376
Restrict File Dialogs	376
Set Environment Variable Action	376
Set Process Security Descriptor	376
Operations	378
Deleting Items	379
Tasks	380
Client Tasks	381
Basic Inventory	382
<i>Basic Inventory (Initial, Windows)</i>	382
<i>Basic Inventory (Windows)</i>	382
<i>Basic Inventory (Initial, Mac OS)</i>	382
<i>Basic Inventory (Mac OS)</i>	383
Cleanup Agent Inventory Transfer	384
<i>Cleanup Agent Inventory Transfers (Windows)</i>	384
Cleanup Sent Privilege Manager Events	385
<i>Cleanup sent Privilege Manager Events (Windows)</i>	385
<i>Cleanup sent Privilege Manager Events (Mac OS)</i>	385
COM Inventory Policy	386
Configure Privilege Manager Remove Programs	387
Default File Inventory Policy	388
<i>Default File Inventory Policy (Windows)</i>	388
<i>Default File Inventory Policy (MacOS)</i>	388
Ensure UAC Override Setting (Windows)	389
Local User Inventory Policy	390
<i>Local User Inventory Policy</i>	390
<i>Local User Inventory Policy (MacOS)</i>	390
Perform Resource Discovery	391
<i>Perform Resource Discovery (Windows)</i>	391
<i>Perform Resource Discovery (Mac OS)</i>	391
Retry Errored TMS Events	392
<i>Retry errored TMS Events (Windows)</i>	392
<i>Retry errored TMS Events (Mac OS)</i>	392
Scheduled Check for Pending Tasks	393
<i>Scheduled Check Pending Client Tasks - Internet Clients (Windows)</i>	393
Scheduled Registration	394

<i>Scheduled Registration (Windows)</i>	394
<i>Scheduled Registration - Internet Clients (Windows)</i>	394
<i>Scheduled Registration (Mac OS)</i>	394
Set Agent Log Size	396
Shared Folder Inventory Policy	397
Update Agent Commands	398
<i>Update Agent Commands (Windows)</i>	398
<i>Update Agent Commands (Mac OS)</i>	398
Update Applicable Policies	399
<i>Update Applicable Policies (Windows)</i>	399
<i>Update Applicable Policies - Internet Clients (Windows)</i>	399
<i>Update Applicable Policies (Mac OS)</i>	399
Update Provisioned Resource Client Items	401
<i>Update Provisioned Resource Client Items (Windows)</i>	401
<i>Update Provisioned Resource Client Items (MacOS)</i>	401
User Logon Inventory Policy	402
Windows Server Inventory Policy	403
Server Tasks	404
<i>Component Based List of Default Tasks</i>	404
HelpDesk Tasks	405
Infrastructure Scheduled Activities	406
Scheduled Tasks	408
<i>AD Import and Synchronization Tasks</i>	408
<i>Task Parameter Conflicts</i>	408
E-mail Reports Task	409
Tasks Launching Executables	411
Example Scenario	411
Workaround	411
Maintenance	412
Maintenance Tasks	412
<i>Assign Orphaned Agent Uploads</i>	412
<i>Delete Old Performance Counter Events</i>	412
<i>Initialize Item Change History</i>	412
<i>LSS Migration Tasks</i>	412
<i>Purge Agent and Gauge Data for Deleted Computers</i>	412
<i>Purge Duplicate Computers</i>	412
<i>Purge Maintenance - Agent Logs</i>	412
<i>Purge Maintenance - Application Control Events</i>	412
<i>Purge Application Control Events older than</i>	412
<i>Purge Maintenance - Audit Events</i>	412

<i>Purge Maintenance - Completed File Upload Sessions</i>	412
<i>Purge Maintenance - Files Undiscovered</i>	413
<i>Purge Maintenance - Incomplete File Upload Sessions</i>	413
<i>Purge Maintenance - Message History</i>	413
<i>Purge Maintenance - Orphaned Local Users and Groups</i>	413
<i>Purge Old Computers</i>	413
Reset Licensing	414
Using the Reset Licensing Task	414
Reports	415
Export Options	415
Reports and Queries	416
View the Existing Reports in Privilege Manager	416
Determine the SQL Query Object Used by a Report	416
View the SQL Query in Privilege Manager	417
<i>Access the Query from the Folder View</i>	418
<i>Obtain a Resolved Query</i>	418
Change History Report	419
Domain Users in Administrator Group	420
Logon Session Summary Report	421
Performance Reporting	422
Setting up Performance Reporting	422
Primary User	423
How to find the primary user for a specific machine	423
Default Update Primary User for Collection	423
Configuration Feeds	424
Exclude File Extensions during File Hashing	425
Create File Exclusion through Config Feed	425
Manually Test on Endpoint	426
Ignoring macOS Updates	427
Configuration Feeds	427
Enabling the Policies	428
Scheduling	429
Foreign Systems	430
Thycotic Foreign Systems	430
AD Integration	430
Third-Party Foreign Systems Integration	430
How to Remove Integrations	430
Thycotic Products Integrations	431
Setting up Integration between Privilege Manager and Secret Server	432
<i>Verify Web Services are Enabled in Secret Server</i>	432

<i>Setup Authentication Data in Privilege Manager</i>	432
<i>Configure Privilege Manager Credential Vault (optional)</i>	433
<i>Password Migration</i>	434
Important Notes	434
<i>Templates</i>	435
Active Directory Integration	436
10.5 Azure AD Integration with Privilege Manager	437
<i>Summary</i>	437
<i>Introduction</i>	437
Part I: Establish Credentials for Privilege Manager to Access Azure AD	437
<i>Part I, Step A: Create a Service Account in the Azure Portal</i>	437
<i>Part I, Step B: Add the Service Account as a User Credential in Privilege Manager</i>	438
Part II: Add Azure AD as a Foreign System in Privilege Manager	439
Part III: Complete the Azure AD Integration with Privilege Manager	441
<i>Overview of the Azure Authentication Page</i>	441
<i>Details and Setting Sections</i>	442
<i>Step One: Import Users & Groups</i>	442
<i>Step Two: Assign Azure User to Role</i>	443
<i>Step Three: Complete Setup</i>	444
<i>Step Four: Set as Authentication Provider</i>	447
<i>Logging back into Privilege Manager after completion of Step Four</i>	448
Additional Information	449
<i>Allowing Azure AD Accounts to Login with a Privilege Manager Role</i>	449
<i>Options for Activating or De-Activating the Azure AD Authentication Integration</i>	449
Activating	449
De-Activating	450
<i>Deleting Azure AD Domains</i>	450
<i>Locked Out?</i>	450
Setting Up Azure Active Directory Integration in Privilege Manager	451
<i>Prerequisites</i>	451
<i>Setting up Azure AD with Privilege Manager</i>	451
Steps in the Azure Portal	451
<i>Steps in your Privilege Manager Instance</i>	453
Set-up Foreign Systems	453
Viewing Imported Users and Groups	454
Import Users and Groups via Privilege Manager Task	454
<i>Create Scheduled Task for Users/Groups Synchronization</i>	455
Third-Party Foreign Systems Integration	456
Set-up Cylance Integration	457
<i>Cylance Connector Installation Steps (On-prem only)</i>	457

<i>Configuring the Cylance Connector</i>	457
<i>Create a Cylance Security Rating Filter</i>	458
<i>Create a Cylance Policy</i>	459
Set-up Microsoft System Center Configuration Manager (SCCM) Integration	461
<i>Create a Credential</i>	461
<i>Connecting to SCCM</i>	461
<i>Import Computers</i>	461
Verify the Computers have been Imported (optional)	462
<i>Create a Collection</i>	462
<i>Inventory Software Packages</i>	463
Create a SCCM Package Content Filter	464
Set-up Symantec Management Platform (SMP) Integration	466
<i>Create a Credential</i>	466
<i>Connecting to SMP</i>	466
<i>Import Computers</i>	466
Verify the Computers have been Imported (optional)	467
<i>Create a Collection</i>	467
<i>Inventory Software Packages</i>	468
Create a SMP Package Content Filter	469
Set-up ServiceNow Integration	471
<i>ServiceNow Steps</i>	472
<i>Define Action and Policy</i>	472
<i>Integration Workflow</i>	474
<i>Create Approval Request Items Task</i>	474
<i>How to create ServiceNow Approval Request Items Task</i>	474
<i>Variables</i>	474
CreateExecuteAppApprovalRequest	475
Script Input	475
Script Output	475
GetExecuteAppApprovalRequestStatus	475
Script Input	475
Script Output	475
CancelExecuteAppApprovalRequest	475
Inputs	475
Outputs	475
<i>Required Integration Points</i>	475
What Can Change vs. What Must Remain	475
Set-up SMTP Connection	477
<i>SMTP in Cloud Environments</i>	477
<i>Configuring the SMTP Connection</i>	477

<i>Setting up Email Alerts</i>	477
Approval Requests	477
Set-up SysLog Connection	478
<i>Configuring SysLog Connection</i>	478
<i>Setting up SysLog Server Tasks</i>	478
Template Options	479
Data Sources	479
<i>Troubleshooting if SysLog Option is Missing under Foreign Systems</i>	479
Set-up VirusTotal Connection	480
<i>VirusTotal API Key</i>	480
<i>Install VirusTotal</i>	480
Collection of Miscellaneous Integration Related Topics	482
Remove RDP Monitoring from Privilege Manager	483
How to...	484
Best Practices	485
<i>Privilege Manager Disaster Recovery</i>	486
Maintaining Privilege Manager in a Disaster	486
<i>Simple Installation and Architecture</i>	486
<i>Restoring from Backup</i>	486
<i>Restoring Privilege Manager from a Backup</i>	486
<i>High Availability</i>	486
Summary & Additional Support Resources	486
Using a Service Account to run the IIS App pool	487
<i>Creating a Domain Service Account</i>	487
<i>Granting Access to SQL Database</i>	487
<i>Assigning Identity of Application Pool(s) in IIS</i>	488
<i>Granting Folder Permissions</i>	489
<i>Configuring User Rights Assignment</i>	490
<i>Setting User Rights Assignment on the Domain</i>	490
<i>Setting User Rights Assignment Locally</i>	491
Prevent Read and Write Access to File Types or Locations	492
<i>Create a Deny File Access Action</i>	492
<i>Create an Application Control Policy</i>	492
<i>Test Access</i>	494
Infrastructure	495
Privilege Manager High Availability Setup	496
<i>Pre-Requisites</i>	496
System Requirements Overview	496
Using the Installer to Install/Confirm Pre-Requisites	496
<i>Manual Set-up of Secondary Node</i>	496

Folder Permissions to C:\Windows\Temp	500
Folder Permissions to the Privilege Manager Application Folder	501
Permission to Certificate Private Key (prior to 10.6 only)	502
Verify Login on Secondary Node	502
<i>Re-encrypt ConnectionStrings.config</i>	502
Setting up Internet Connected Clients	503
<i>Azure Service Bus Queue Configuration</i>	503
<i>Setting up the Service Bus Foreign System</i>	503
<i>Configuring Agents to Use the Service Bus</i>	504
Using regedit	504
Using PowerShell	504
Moving SQL DB	505
<i>Moving the Privilege Manager DB</i>	505
Step 1: Backup and Restore the Database	505
Step 2: Connect to the new database (configure the database connection details)	505
Setting up a Reverse Proxy	506
<i>System Specifications</i>	506
<i>Server Configuration</i>	506
Testing Agent URLs	508
<i>Agent Configuration</i>	509
VM Deployments	510
<i>Identifying Agents to The Console</i>	510
Persistent VMs	510
Dynamic VMs	510
Multiple VMs Collapsed to a Single Resource	510
<i>Pool of Values to Support Multiple VMs</i>	510
<i>Managing Agent Trust and Certificates</i>	510
<i>Minimizing Time Between VDI Deployment and Policy Enforcement</i>	510
<i>Licensing Concerns with Windows 10 Amazon Workspaces</i>	511
Maintenance	512
How to Purge Computers	513
Purging Action Items Table	515
<i>Creating a Scheduled Event for Purging</i>	515
Using the Remove Programs Utility	518
<i>Using the Configure Privilege Manager Remove Programs Policy</i>	518
Configuring the Remove Programs Utility	518
<i>Use the Utility</i>	520
Export and Import Items	521
<i>Exporting Items</i>	521
Specific Policy Export	521

Folder Exports	521
<i>Importing Items</i>	522
Using Import Items	522
Using Diagnostics Upload Items File	523
Troubleshooting	524
Markdig.Syntax.Inlines.LinkInline	524
Markdig.Syntax.Inlines.LinkInline	524
Markdig.Syntax.Inlines.LinkInline	524
Markdig.Syntax.Inlines.LinkInline	524
Markdig.Syntax.Inlines.LinkInline	524
Markdig.Syntax.Inlines.LinkInline	524
Markdig.Syntax.Inlines.LinkInline	524
Agents Troubleshooting	525
Agent updateclientitems.ps1 Error	526
Agent Registration Issue	527
<i>Detailed Information</i>	527
Using a PowerShell Script	527
Client Item List Downloads	529
<i>Resolve</i>	529
Advanced Messages not Working for Child Processes of Microsoft Edge	530
<i>Detailed Information</i>	530
<i>Workaround</i>	530
Endpoint Troubleshooting	531
Endpoint Issues	532
<i>Agent Install Codes</i>	532
<i>Agent Utility</i>	532
Status Button	532
Register Button	532
Update Button	532
View Cache Button	532
View Logs	533
Export Logs Button	533
<i>Policy Troubleshooting</i>	533
Policies Not Getting Updated	533
Specific Files or Applications Not Being Elevated or Blocked	533
Catalina FileSystemWatcher Issue	535
How to Recover an Unresponsive macOS Endpoint	537
Errors	538
Common Errors	539
<i>Access Denied</i>	539

<i>Server Error in...</i>	539
<i>SSL Connectivity or Certificate Issues</i>	539
Trusting an SSL Certificate on a Client Machine (KB)	539
Granting Permissions on New SSL Certificate for Privilege Manager (KB)	539
<i>To grant permissions manually, follow these steps</i>	539
<i>Grant Read Access to the account(s) that TMS is running under</i>	539
<i>Tasks Stuck at Ready</i>	540
<i>CPU Issue</i>	540
<i>System Critical Error</i>	540
Error: Space Allocation	541
<i>Resolving the Error</i>	541
Installation Hangs with Error: Worker Role Monitor received exception during ping	542
<i>Resolve</i>	542
Error: Invalid product identifier:	545
<i>Resolve</i>	545
Notify User Justification failed	547
<i>Resolve</i>	547
UI Storage Error	548
<i>Resolution</i>	548
Installation and Upgrade Issues	549
10.5 Folder Permissions - MachineKeys	550
Installation Issues	551
<i>Internet Connection</i>	551
<i>.NET Dependency</i>	551
<i>IIS not Installed</i>	552
<i>HTTPS Binding Error</i>	552
<i>PowerShell Error</i>	552
<i>Secret Server and Privilege Manager Installed</i>	553
<i>Error in DB File Path</i>	553
<i>Outdated Browser</i>	554
<i>Integrated Authentication Error</i>	554
Retrieving the COM Class Factory Error	556
<i>Resolve</i>	556
Performance Issues	558
Increase Boot-up Performance	559
<i>Enable Pausing Policy Analysis during Boot-up</i>	559
Unable to Access Privilege Manager	560
<i>Resolve</i>	560
Privilege Manager Logs	562
Where are My Server Logs	563

Where are My Agent Logs	564
SQL Server Transaction Log	565
User Interface and Ports	566
<i>Connectivity</i>	566
Troubleshoot with Tools	567
Using Thycotic Monitor	568
Using Process Explorer for Troubleshooting a Policy	570
<i>Detailed Troubleshooting Steps</i>	570
Using Process Hacker for Troubleshooting	573
Privilege Manager Mobile Application	574
Detailed Instruction Topics	574
Configure Azure Active Directory	575
Configure the Service Bus for Mobile	577
Creating a Service Bus and Queue in the Azure Portal	577
Adding the Service Bus as a Foreign System	577
Install and Configure the Mobile Console in Privilege Manager	579
Install the Privilege Manager Mobile Console	579
Set the Client ID and Tenant ID	579
Configure the Notification Settings	580
Authentication Provider Warning	582
Mobile App Install and Sign In	583
Troubleshooting	583
Use the Mobile Application	584
Approval requests	584
Password Disclosure	584
Alerts	584
Release Notes	586
10.7.1 Release Notes	587
Enhancements	587
<i>macOS Specific Features</i>	587
<i>Cloud Specific Features</i>	587
Bug Fixes	587
<i>Agent Updates</i>	587
Known Issues	588
10.7 On-prem Release Notes	589
Enhancements	589
Bug Fixes	589
Known Issues	590
10.6 On-prem Release Notes	591
Enhancements	591

Bug Fixes	591
Known Issues	591
10.6 Cloud Release Notes	592
Enhancements	592
Bug Fixes	592
Limitations in Privilege Manager Cloud 10.6 vs. On-prem	592
Known Issues	593
10.5 and Previous Releases	594
10.5.4	594
<i>Enhancements</i>	594
<i>Bug Fixes</i>	594
10.5.000003	594
<i>Bug Fixes</i>	594
<i>Mac Agent Updates (version 10.5.12)</i>	594
10.5.000001	594
<i>Bug Fixes</i>	594
10.5.000000	595
<i>Overview</i>	595
Important for Secret Server Combined Upgrades	595
<i>10.5 Agent Upgrades</i>	595
<i>Enhancements</i>	595
<i>Bug Fixes</i>	595
<i>Known Issues</i>	595
10.4.001233	595
<i>Bug Fixes</i>	595
10.4.001231	595
<i>Enhancements</i>	595
<i>Bug Fixes</i>	595
10.4.000000	596
<i>Enhancements</i>	596
<i>Bug Fixes</i>	596
<i>Known Issues</i>	596
10.3.000014	596
<i>Enhancements</i>	596
<i>Bug Fixes</i>	597
10.3.000000	597
<i>Enhancements</i>	597
10.2.000000	597
<i>Enhancements</i>	597
10.1.000000	597

<i>Enhancements</i>	597
<i>Bug Fixes</i>	597
Documentation Changelog	598
June 2020	598
Support	599
Obtaining a Support PIN	599
Support by Phone	599
Support by Email	599
Support Ticketing	599

Privilege Manager is an endpoint least privilege and application control solution for Windows and Macs, capable of supporting enterprises and fast-growing organizations at scale. The two major components are Local Security and Application Control.

Using Privilege Manager, administrators can automatically discover local administrator privileges and enforce the principle of least privilege through policy-driven actions. Those policy-driven actions include

- blocking, elevating, monitoring, allowing
- application quarantine, sandbox, and isolation,
- application privilege elevation, and
- endpoint monitoring

All this is seamless for users, reduce IT/desktop support workload, and support compliance obligations.

Privilege Manager does not require Secret Server or any other Thycotic product to run. Secret Server's vaulting and workflow capabilities can be extended to privileged endpoint accounts when the two products are used together.

The typical Privilege Manager user is part of an IT team that is tasked with implementing and overseeing a company's security business requirements and framework. In the Privilege Manager product this role is known as the Privilege Manager Administrator. Although there are a few other kinds of [Privilege Manager user roles](#) that may use Privilege Manager now and then for minor tasks, the Privilege Manager Administrator is the main user of Privilege Manager.

It is useful (although not necessary) for Privilege Manager Administrators to be familiar with the basics of IT administration, such as the Group Policy feature from Microsoft.

10.7.1 Cloud Specific

The following features and options are different from On-premises or previous Privilege Manager Cloud releases:

- The ServiceNow connector is automatically installed for all new cloud instances.
- The SMTP server is automatically configured during the cloud instance setup.
- The setup is managed by Thycotic and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection option to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Thycotic during maintenance periods.
- All license key management is done via Thycotic and license keys are not visible on the licensing page. There are presently no options for customers to add additional licenses directly.

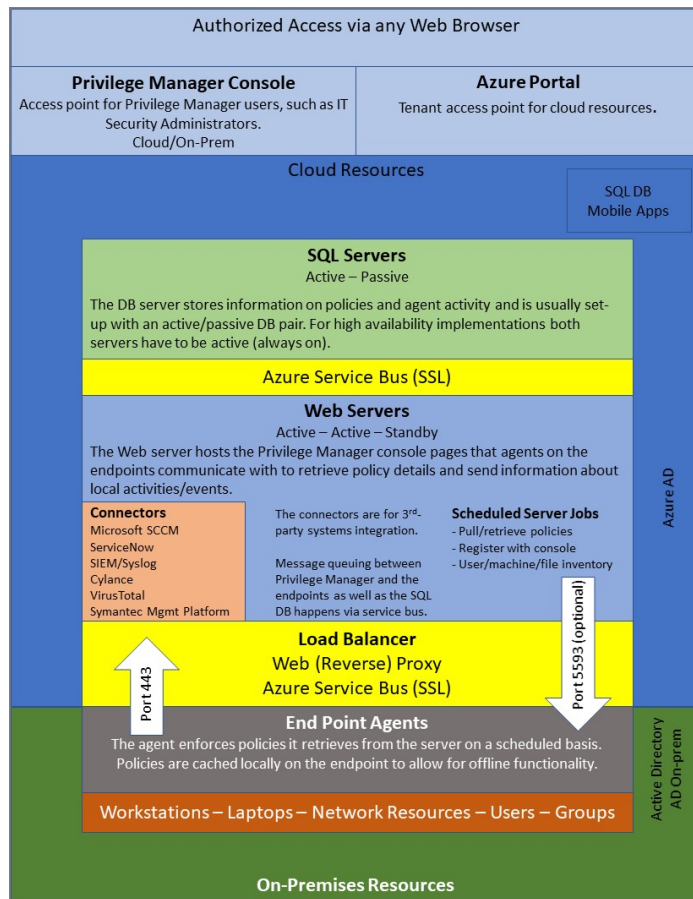
The following features and options are **not** available in Privilege Manager Cloud:

- The Local Active Directory features exists, but requires a direct connection to the domain controller, which is often not permissible due to firewall configurations.
- Access to the Security Manager console (Silverlight version) is not available.
- Personas are not available.
- Server-side Powershell scripts not signed by Thycotic are not allowed. Custom server-side work can be done via Professional Services engagements.

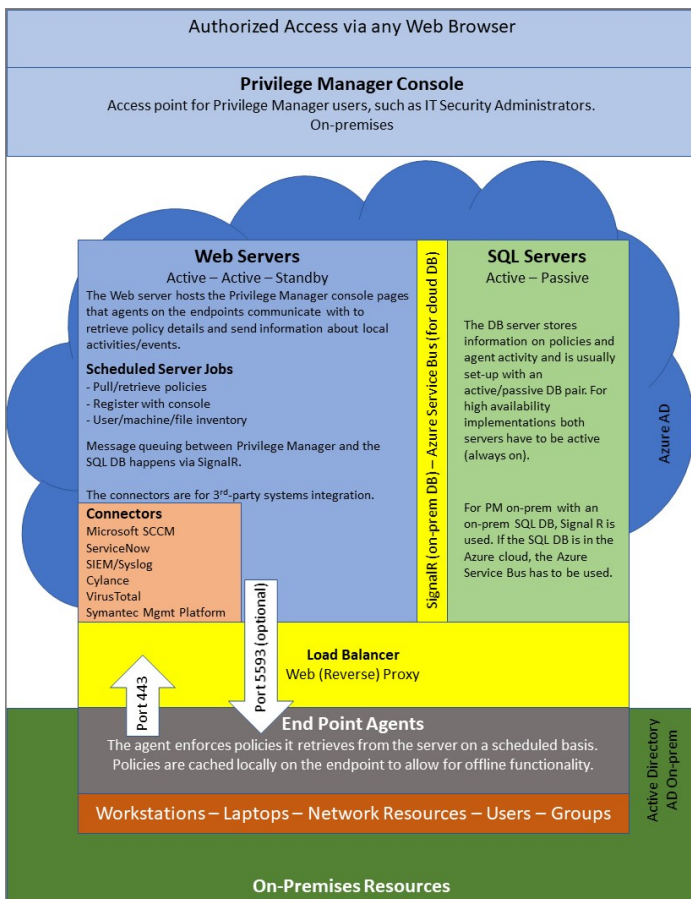
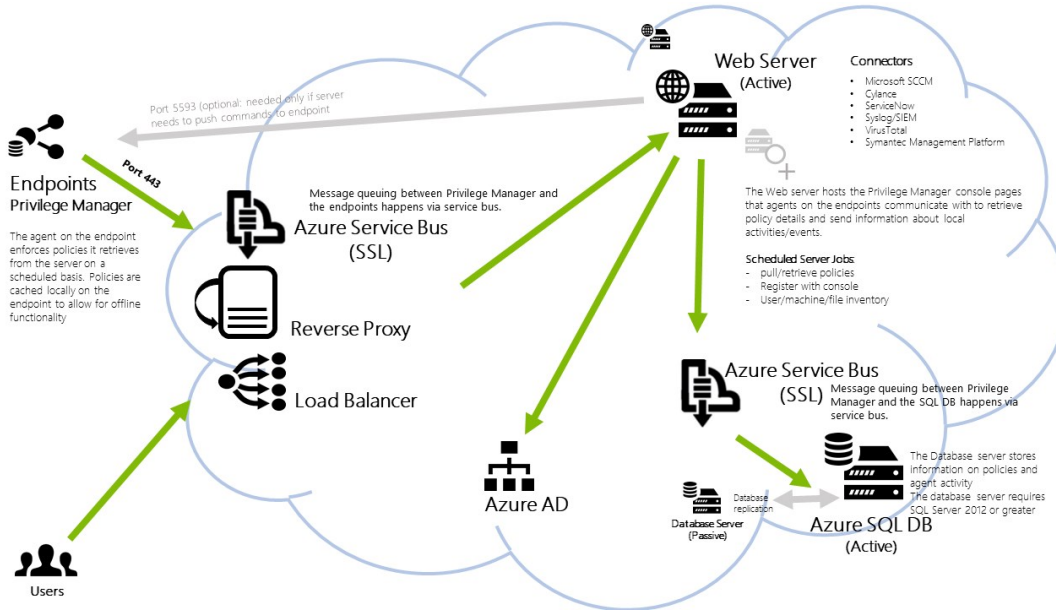
All other features and functionality of Privilege Manager On-premises and Cloud are the same unless otherwise specified.

Product Overview

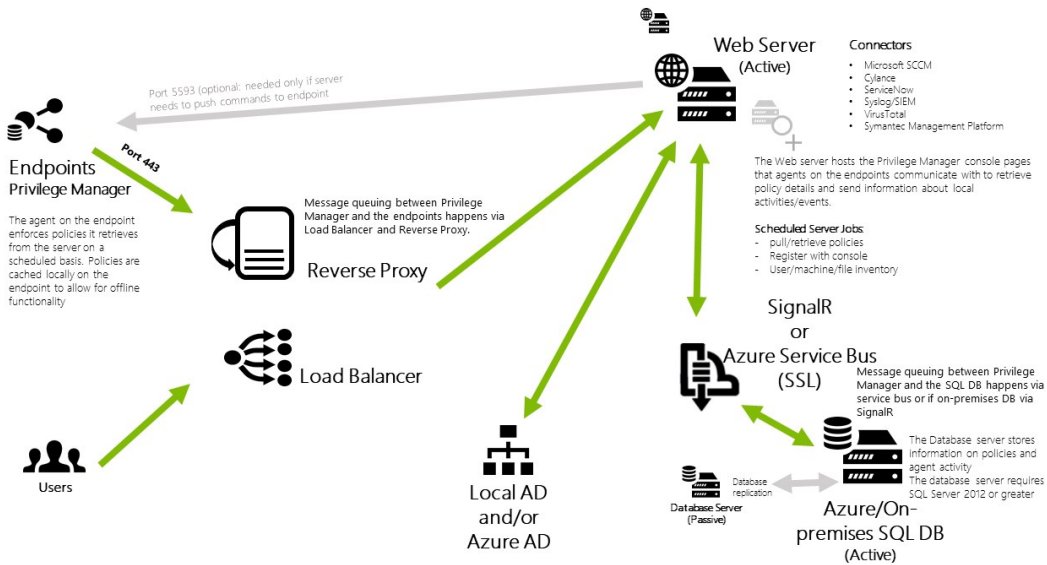
The following diagrams provide an architectural overview of Privilege Manager, its components, and available integrations.



Network Diagram (Cloud)



Network Diagram (On-prem)



Least Privilege Explained

Least Privilege is a security-driven management philosophy that models a system where all employees are given the minimum level of access rights necessary to carry out their job functions on endpoint machines. This is to protect each machine from malicious applications, rogue employees, or attackers. Privileged local admin or root accounts on endpoints give unfettered access to the entire endpoint and can potentially be used to access other computers, domain resources, and critical servers unless a least privilege security model is implemented. But implementing Least Privilege can be difficult for IT teams to enforce because there are plenty of daily, trusted activities that employees must perform that require access to privileged credentials.

Privilege Manager's toolset is two-fold. First, Local Security discovers all accounts that exist on endpoints and allows Privilege Manager Administrators to control the exact membership of every local group. This will ensure the correct admin and root accounts are permanently set. Additionally, credentials will be controlled by enforcing password rotation on those accounts.

Second, Application Control allows Privilege Manager administrators to manage application activity on endpoint machines. Applications that require admin rights or root access can be automatically elevated, allowed applications are whitelisted, and malicious applications are blocked.

In other words, tailoring a robust, role-based Application Control system is key to keeping your organization's employees working both securely and effectively, without notable disruptions. But managing local administrator and root accounts through Local Security is arguably the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.

Every implementation looks different when configuring Privilege Manager to work best for your organization. The key is to know your goal and be smart about getting there. The [Getting Started section](#) will walk you through beginning configurations for both Local Security and Application Control.

Integration with Secret Server

Privilege Manager and Secret Server integration is supported in a co-hosted setting when installed on the same server or on separate servers. If integrated on separate servers, Privilege Manager communicates with Secret Server via Secret Server's REST API.

The benefits of Privilege Manager's integration with Secret Server include:

- Secret Server can be the authentication source for Privilege Manager, which:
 - Adds Secret Server's MFA login options to Privilege Manager logins.
 - Gives one place for role assignments for both products.
- Allows Privilege Manager to use Secret Server as a storage container. If Secret Server is used as a storage container for Privilege Manager credentials, Privilege Manager
 - creates Secrets for each local credential managed by Privilege Manager.
 - creates Secrets for each Configuration Credential stored in Privilege Manager. This includes credentials used for Foreign Systems, such as AD Sync, ServiceNow, etc.
 - does not pull any changes for these Secrets. Privilege Manager only stores the credentials in Secret Server to utilize Secret Server's workflow options for other users to view.

When Secret Server is used as the authentication source for Privilege Manager, Role Permissions assigned in Secret Server are important and determine user access levels in Privilege Manager. Without Secret Server integration, Privilege Manager uses NTLM for WebServer and Azure AD as possible authentication sources.

End User - These are the users connecting to your Secret Server and Privilege Manager websites. These users may be performing administrative tasks (admins), or just using the solution.

Load Balancers - Load Balancers are often involved in the solution to help distribute web traffic to more than one web server. Load balancers may also be involved for distributing traffic to a RabbitMQ cluster. Local and Global load balancers, if available, may be used in the solution to further lower potential application downtime during upgrades, patching, and single site failures.

Web Server - This is a primary component of the solution. Our web servers use IIS 7 and newer and will only work on Windows Server 2008 R2 or newer. For multiple web server (clustered) solutions, The web application itself can be made cluster aware and does not require being built as part of an IIS farm. Each web server acts as its own stand alone web server.

Database Server - This is a primary component of the solution. SQL Server hosts the Secret Server and Privilege Manager databases. We are compatible only with SQL Server 2012 or newer running on Windows Server 2008 R2 or newer. The Thycotic databases can be put on a stand alone server, a FCI, or preferably using an AlwaysOn AG for clustered environments. The databases can be added to an existing production SQL cluster or instance, but proper sizing of the environment should be done. Windows authentication only is advised.

MemoryMQ - MemoryMQ is our built in message brokering solution for Secret Server. It is not as robust as RabbitMQ and cannot be made highly available. Web Servers themselves have a built in MemoryMQ function so that out of box Secret Server can do all work by just having a Web and Database server. Alternatively, MemoryMQ can be installed on its own dedicated system. It is used by Secret Server, but not Privilege Manager.

RabbitMQ - This is an optional but often recommended component of the solution for any Secret Server environment involving multiple Web Servers or Distributed Engines. RabbitMQ is the most robust and widely used message brokering solution. Secret Server can utilize RabbitMQ for offloading work to Distributed Engines within the environment. This allows the solution to be more robust and efficient by making work done within the environment more distributed. You will see recommendations to use RabbitMQ in many web pages within our product. It is used by Secret Server, but not Privilege Manager. - <https://www.rabbitmq.com/>

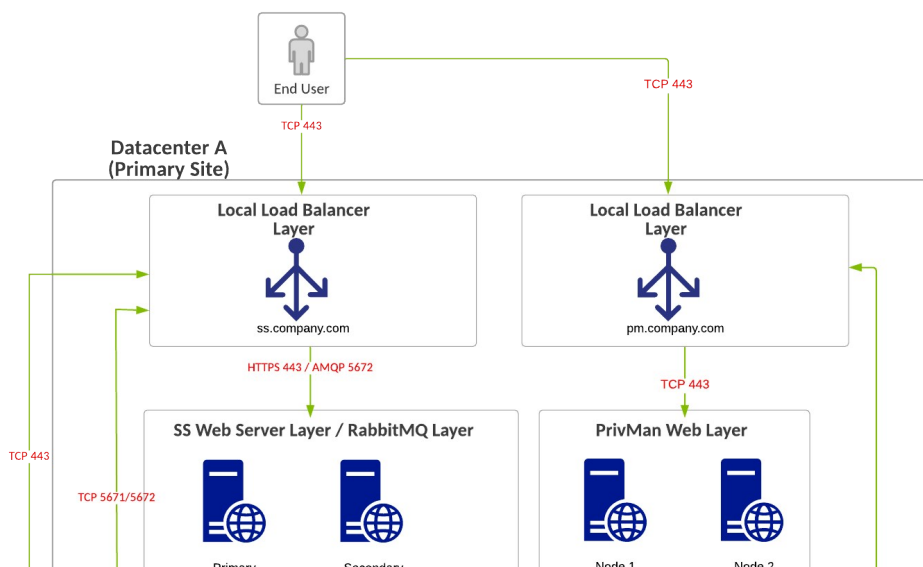
Distributed Engines - Distributed Engines are used by Secret Server for two primary reasons. The first reason is to do work on behalf of the web servers and allow the architecture to be more distributed. You can consider distributed engines your "workers" within a Secret Server environment. Out of box without Distributed Engines, the Web Servers are doing all of the work. Distributed Engines are also useful for when you have systems in isolated network segments within your environment that you would like to manage with Secret Server. Distributed Engines are used by Secret Server, but not Privilege Manager.

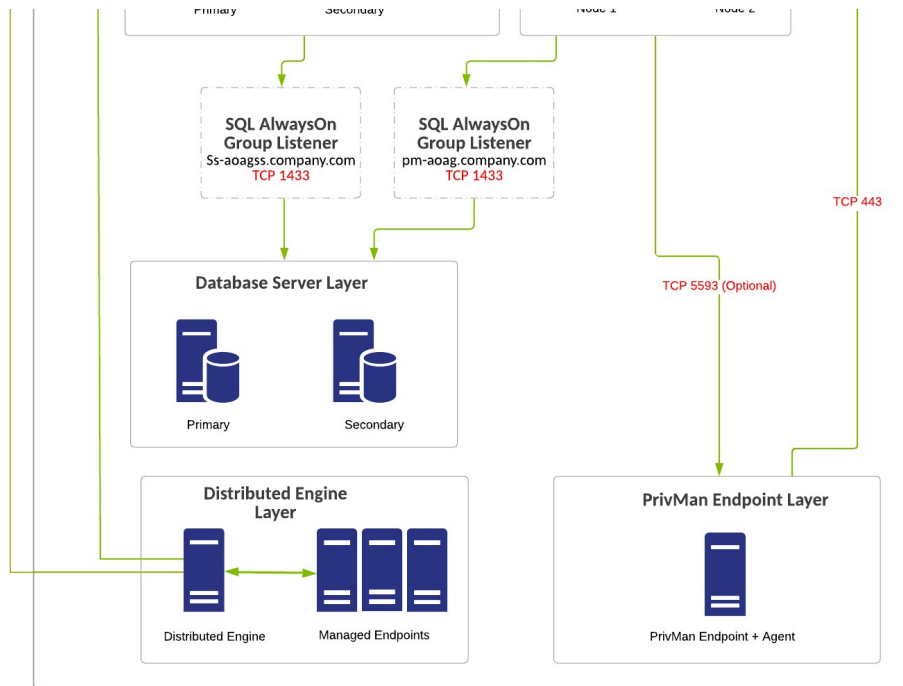
Privilege Manager Agents - These are used for application control and local user/group management for our Privilege Manager solution. Privilege Manager Agents are used by Privilege Manager, but not Secret Server.

Note: Every component of Secret Server and Privilege Manager can be made highly available to ensure a redundant architecture and to scale for future growth.

Minimum High Availability

A-1





thycotic Secret Server + PrivMan Reference Architecture #06

Created By: Thycotic Solution Architects Created On: 5/21/2019

Legend

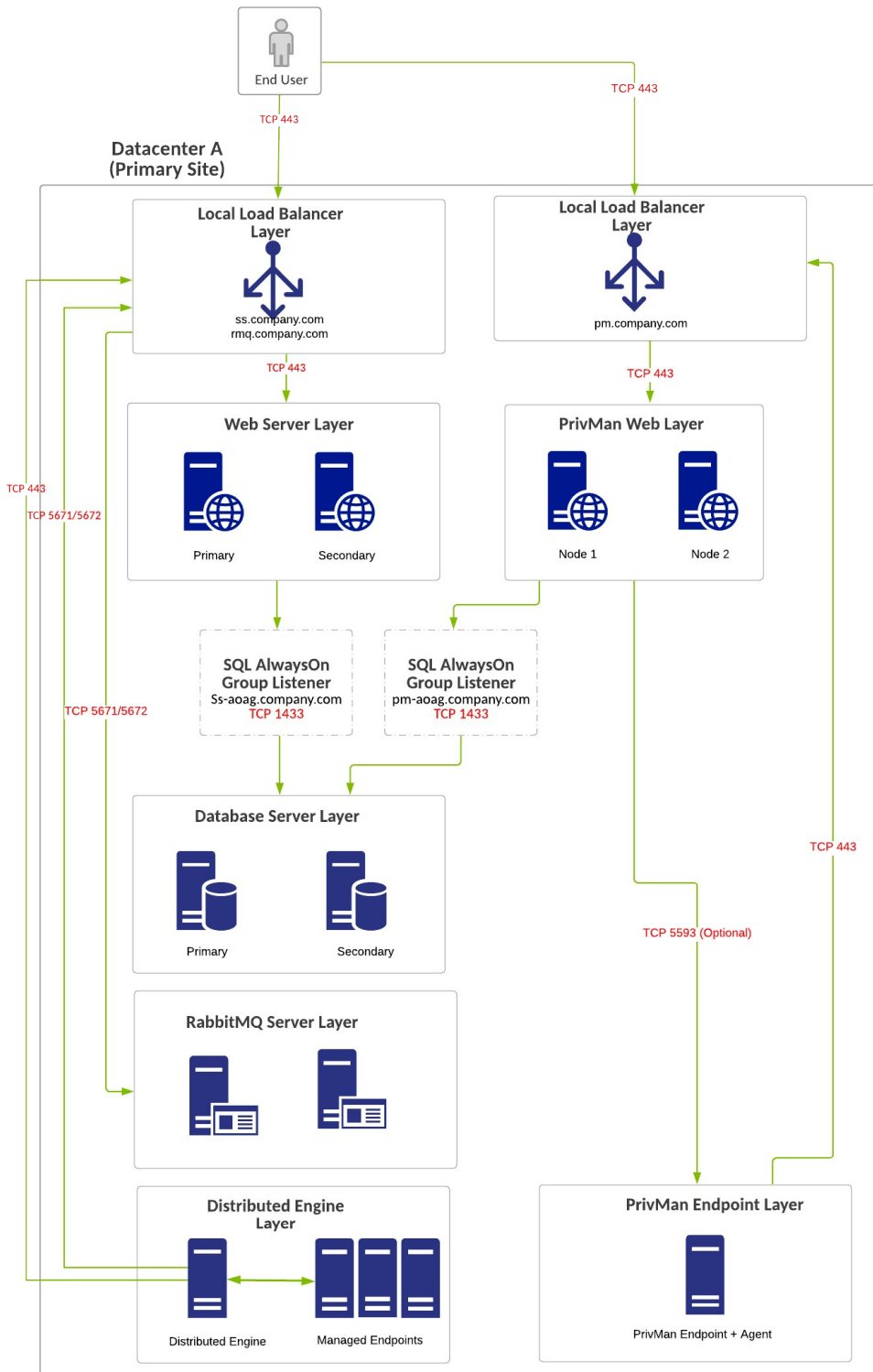
- Active Connection: Solid green line
- Replication/Inactive: Dotted green line
- Global/Local Load Balancers: Blue icon


Definitions for Reference Architecture #06- A-1 - "Minimum HA" Enterprise Scale Deployment - Single Site




- Minimum Cost HA Configuration - No Shared Storage Requirement.
- RabbitMQ Installed on Secret Server Web Servers (Typically in a cluster on a primary + secondary node).
- Single Site design, no native DR capacity. DR can be provided by means of VM replication if subnets are spanning locations, otherwise re-ip + DNS changes may be necessary.
- Privilege Manager is preferably installed on separate web servers. For smaller environments, Privilege Manager can be installed on the same web servers as Secret Server and can be used for integrating authentication and can store credentials in Secret Server.
- Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself. Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a separate AlwaysOn availability group configuration.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.

Requirements for Reference Architecture #06 - A-1 - "Minimum HA" Enterprise Scale Deployment - Single Site

- SQL Standard Edition - Basic Availability Group Configuration
- Local load balancers can be utilized for all web server nodes
- Configuring a file share witness for SQL quorum voting is required for SQL to stay online during single node unplanned failures



 Secret Server + PrivMan Reference Architecture #06	
Created By: Thycotic Solution Architects	Created On: 5/21/2019

Legend	
Active Connection	
Replication/Inactive	
Global/Local Load Balancers	

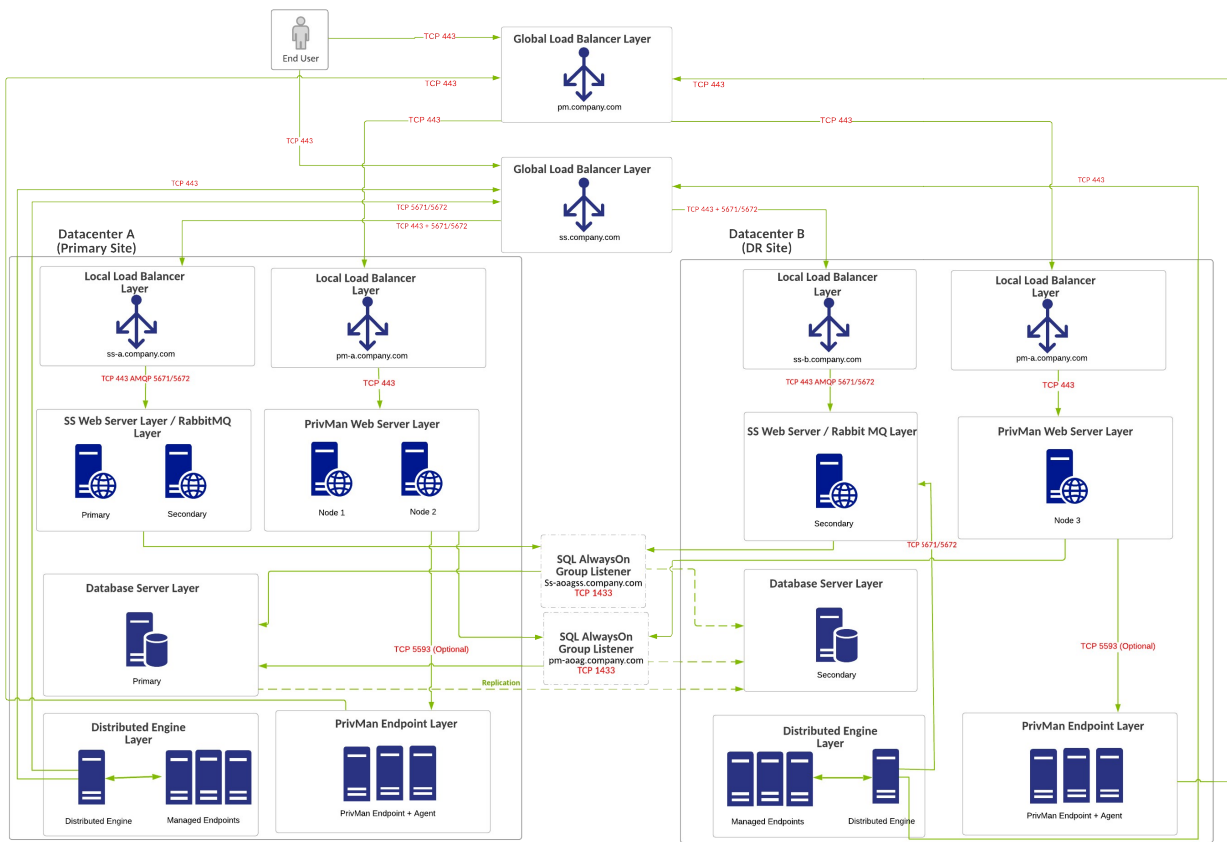
Definitions for Reference Architecture #06 – A-2 – "Minimum HA" Enterprise Scale Deployment - Single Site

- Minimum Cost HA Configuration – No Shared Storage Requirement.
- RabbitMQ Installed on separate servers.
- Single Site design, no native DR capacity. DR can be provided by means of VM replication if subnets are spanning locations, otherwise re-ip + DNS changes may be necessary.
- Privilege Manager is preferably installed on separate web servers. For smaller environments, Privilege Manager can be installed on the same web servers as Secret Server and can be used for integrating authentication and can store credentials in Secret Server.
- Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself. Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a separate AlwaysOn availability group configuration.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.

Requirements for Reference Architecture #06 – A-2 – "Minimum HA" Enterprise Scale Deployment - Single Site

- SQL Standard Edition – Basic Availability Group Configuration
- Local load balancers can be utilized for all web server nodes
- Configuring a file share witness for SQL quorum voting is required for SQL to stay online during single node unplanned failures

Minimum High Availability/DR - Lowest Cost

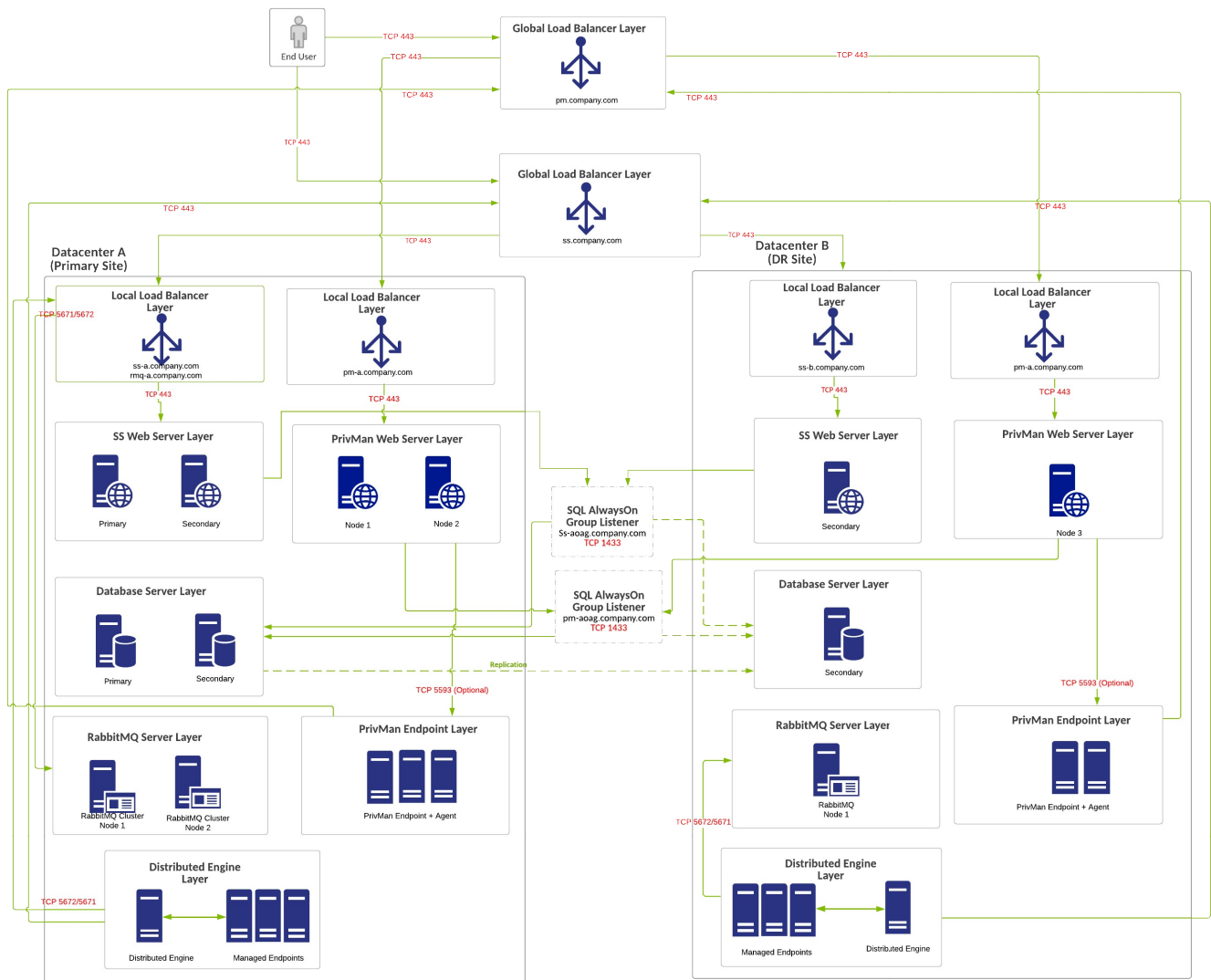


thyctic Secret Server + PrivMan Reference Architecture #06		Legend Active Connection: ——— Replication/Inactive: - - - - Global/Local Load Balancers: [Icon]
Created By: Thyctic Solution Architects	Created On: 5/21/2019	

- Definitions for Reference Architecture #06 - A-3 - "Minimum HA/DR" Enterprise Scale Deployment - Multi Site**
- Minimum Cost HA Multi-Site Configuration - No Shared Storage Requirement.
 - RabbitMQ Installed on Secret Server Web Servers (Typically in a cluster on a primary + secondary node).
 - Multi-Site Design. SQL AlwaysOn configurations will be either synchronous/asynchronous for Secret Server database and asynchronous only for Privilege Manager database.
 - DR site acts as temporary site only with no intention for long-term usage. Services in DR site being down can incur downtime.
 - Privilege Manager is preferably installed on separate web servers. For smaller environments, Privilege Manager can be installed on the same web servers as Secret Server and can be used for integrating authentication and can store credentials in Secret Server.
 - Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself. Due to SQL Basic Availability groups with Standard Edition, you will need to have multiple instances of SQL and a separate AlwaysOn availability group configuration.
 - Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.

- Requirements for Reference Architecture #06 - A-3 - "Minimum HA/DR" Enterprise Scale Deployment - Multi Site**
- SQL Standard Edition - Basic Availability Group Configuration
 - If no Global Load Balancers Exist due to costs/infrastructure missing, local load balancers can be utilized for all web server nodes but DNS change may be required if primary location goes offline
 - Configuring a file share witness for SQL quorum voting is required for SQL to stay online during single node unplanned failures. A cloud witness is recommended.

Average High Availability/DR (RabbitMQ Separation)



thyctic Secret Server + PrivMan Reference Architecture #06

Created By: Thyctic Solution Architects
Created On: 5/21/2019

Legend

- Active Connection (Solid Green Line)
- Replication/Inactive (Dashed Green Line)
- Global/Local Load Balancers (Blue Load Balancer Icon)

Definitions for Reference Architecture #06 – C – "Average HA/DR" Enterprise Scale Deployment

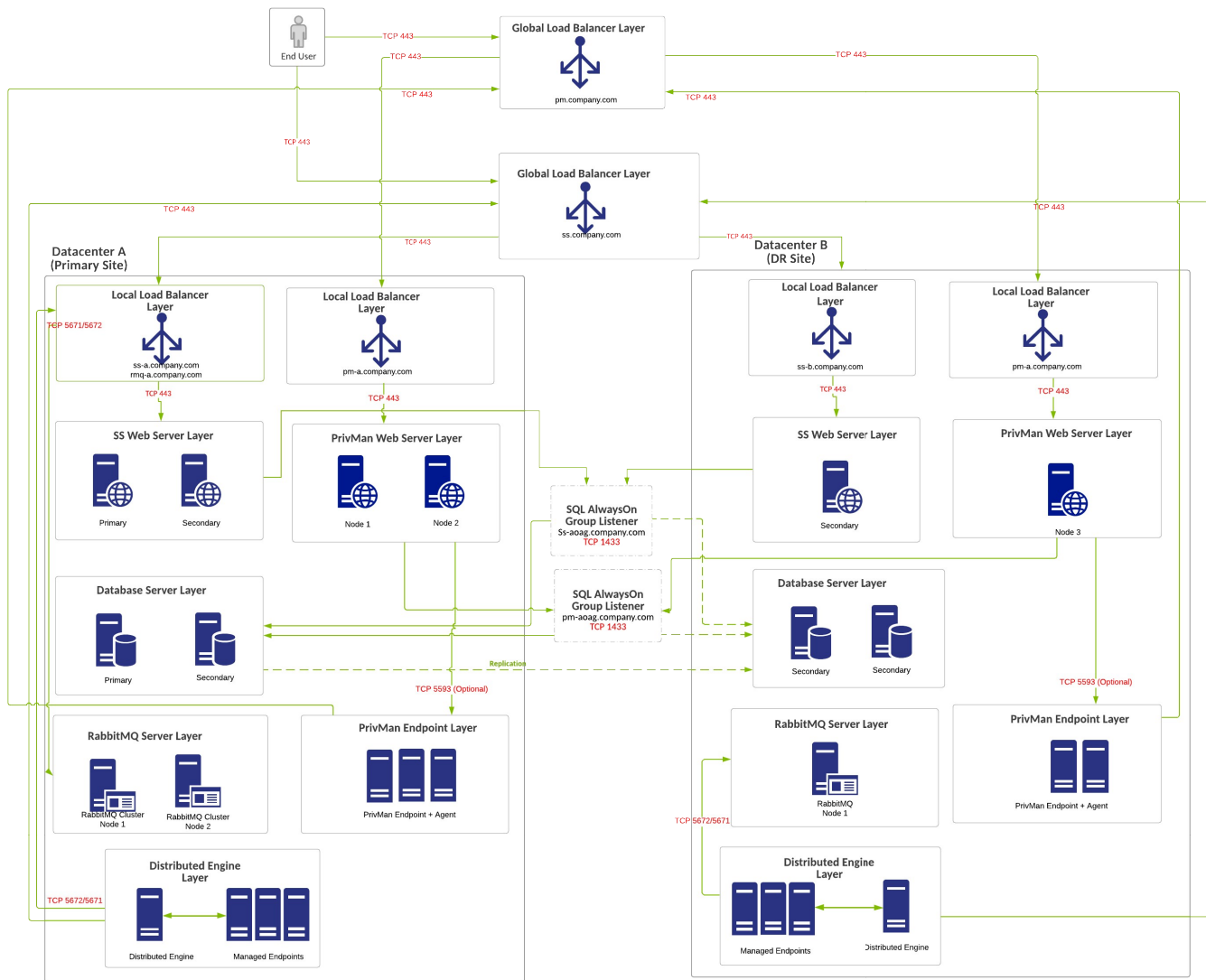
- Average Cost HA Multi-Site Configuration – No Shared Storage Requirement.
- RabbitMQ installed on separate servers.
- Multi-Site Design. SQL AlwaysOn configurations will be either synchronous/asynchronous for Secret Server database and asynchronous only for Privilege Manager database.
- DR site acts as temporary site only with no intention for long-term usage. Services in DR site being down can incur downtime.
- Privilege Manager is preferably installed on separate web servers. For smaller environments, Privilege Manager can be installed on the same web servers as Secret Server and can be used for integrating authentication and can store credentials in Secret Server.
- Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself.
- Secondary SQL Node at Primary Site for Planned Failover "Patching", Secondary SQL Node in DR Site for Unplanned Failover.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.

Requirements for Reference Architecture #06 - C - "Average HA/DR" Enterprise Scale Deployment

- SQL Enterprise Edition
- Global and Local Load Balancers
- Configuring a file share witness for SQL quorum voting is recommended. A cloud witness or DFSR share is recommended for witness configuration. Simultaneous failure of both SQL nodes in the primary location can cause the failover cluster to not survive.

Best High Availability/DR (RabbitMQ Separation)

D-1



thycotic Secret Server + PrivMan Reference Architecture #06

Created By: Thycotic Solution Architects Created On: 5/21/2019

Legend

- Active Connection
- Replication/Inactive
- Global/Local Load Balancers

Definitions for Reference Architecture #06 - D-1 - "Best HA/DR" Enterprise Scale Deployment

- Highest Cost HA Multi-Site Configuration - No Shared Storage Requirement.
- RabbitMQ installed on concrete servers.

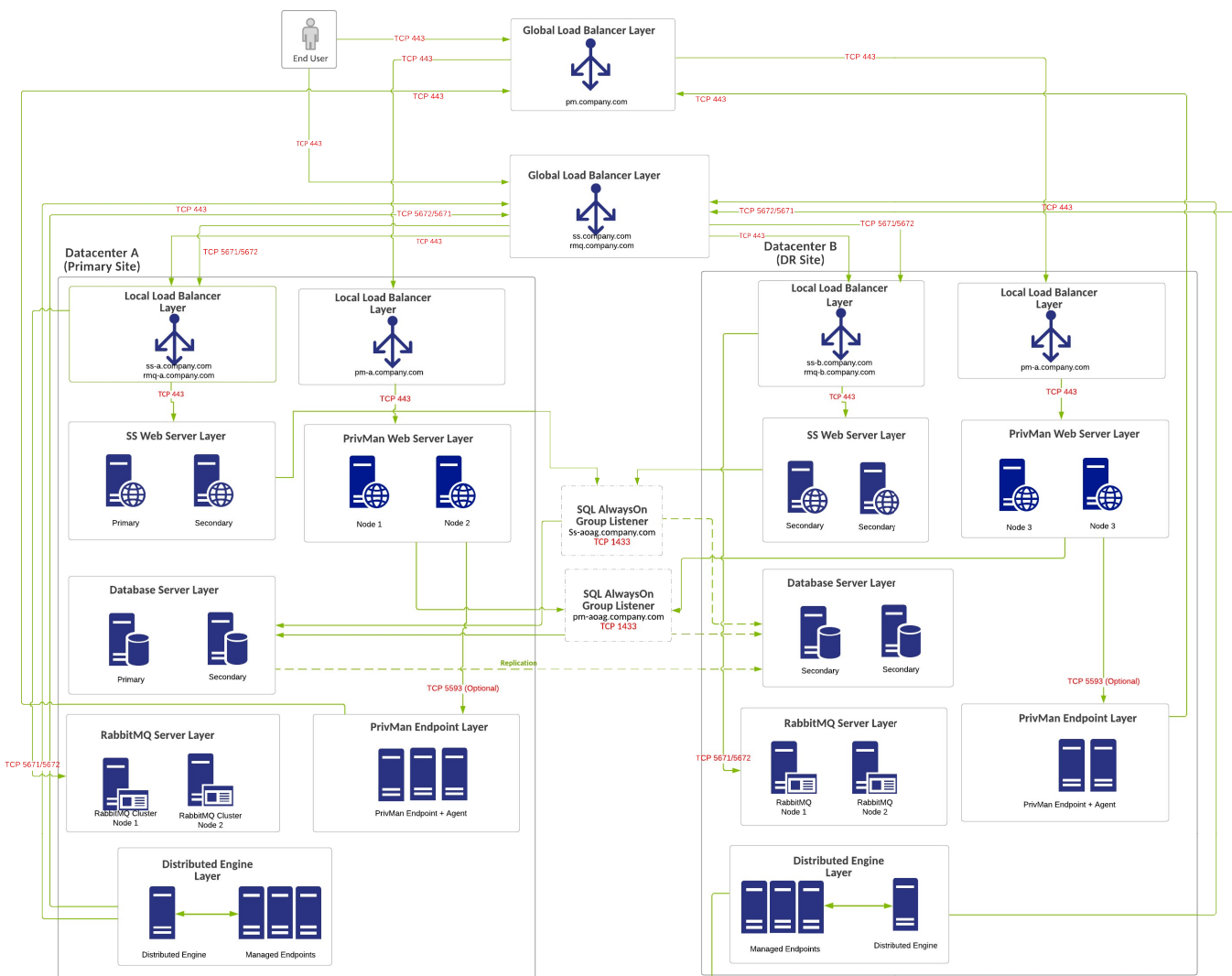
- RabbitMQ installed on separate servers.
- Multi-Site Design. SQL AlwaysOn configurations will be either synchronous/asynchronous for Secret Server database and asynchronous only for Privilege Manager database.
- DR site acts as temporary site only with no intention for long-term usage. Services in DR site being down can incur downtime.
- Privilege Manager is preferably installed on separate web servers. For smaller environments, Privilege Manager can be installed on the same web servers as Secret Server and can be used for integrating authentication and can store credentials in Secret Server.
- Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself.
- Secondary SQL Node at Primary Site for Planned Failover "Patching", Secondary SQL Node in DR Site for Unplanned Failover.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.

Requirements for Reference Architecture #06 – D-1 – "Best HA/DR" Enterprise Scale Deployment




- SQL Enterprise Edition
- Global and Local Load Balancers
- Clustering or Federation for RabbitMQ
- Configuring a file share witness for SQL quorum voting is recommended. A cloud witness or DFSR share is recommended for witness configuration. Can sustain simultaneous failure of both SQL server nodes in primary location and the cluster will survive.

Best High Availability/DR (RabbitMQ Separation) - Highest Cost

D-2



Created By: Thycotic Solution Architects		Created On: 5/21/2019	
--	--	-----------------------	--

Legend	
Active Connection	
Replication/Inactive	
Global/Local Load Balancers	

Definitions for Reference Architecture #06 - D-2 - "Best HA/DR" Enterprise Scale Deployment

- Highest Cost HA Multi-Site Configuration - No Shared Storage Requirement.
- RabbitMQ Installed on separate servers.
- Multi-Site Design. SQL AlwaysOn configurations will be either synchronous/asynchronous for Secret Server database and asynchronous only for Privilege Manager database.
- DR site acts as temporary site only with no intention for long-term usage. Services in DR site being down can incur downtime.
- Privilege Manager is preferably installed on separate web servers. For smaller environments, Privilege Manager can be installed on the same web servers as Secret Server and can be used for integrating authentication and can store credentials in Secret Server.
- Privilege Manager can reside on the same database servers as Secret Server or separate database servers, but Secret Server and Privilege Manager should not share the same database itself.
- Secondary SQL Node at Primary Site for Planned Failover "Patching", Secondary SQL Node in DR Site for Unplanned Failover.
- DR site can act as permanent secondary site for long term use.
- Some customers may choose to use a separate web reverse proxy or azure service bus configuration for Privilege Manager agent TCP 443 communication.

Requirements for Reference Architecture #06 - D-2 - "Best HA/DR" Enterprise Scale Deployment

- SQL Enterprise Edition
- Global and Local Load Balancers
- Clustering or Federation for RabbitMQ
- Configuring a file share witness for SQL quorum voting is recommended. A cloud witness or DFSR share is recommended for witness configuration. Can sustain simultaneous failure of both SQL server nodes in primary location and the cluster will survive.

Feature Overview

For those organizations leveraging [Active Directory \(AD\)](#) and/or [Azure AD](#) as their identity authentication and authorization service, deploying a least privilege program that works seamlessly with AD is absolutely critical. Privilege Manager integrates with AD so administrators can synchronize Domain Objects such as computers, OUs, and security groups from AD with their application control policies. Privilege Manager can leverage the user, group and privilege associations managed by Active Directory in its policy deployment and ensure unauthorized changes to AD made by endpoint users – such as adding a user to a local administrator account – can't be blocked automatically and in real time.

The [Privilege Manager Agents](#) are a critical component of Thycotic's application control, giving you the ability to evaluate the health and status in real time. Privilege Manager provides pre-configured and fully customizable reporting on the status of agents and endpoint operating systems. In the Privilege Manager reporting dashboard, you can drill into reports based on any dimension and easily export report data to other reporting applications or Excel.

The most powerful applications installed on endpoints are those that require administrator credentials or root privileges to run. Privilege Manager discovers all applications that run on endpoints through its Learning Mode, giving you a precise snapshot of how these applications are used before you implement any changes. You can set up Discovery policies to target any new application action that requires administrator or root access, so no privileged action goes unnoticed.

Non-Domain Endpoint Support - Privilege Manager provides management and application control support for endpoints even if they are not associated with your organizational network. Because it utilizes agents it can manage endpoints outside the network – such as those used by vendors, contractors, and partners - with the same dexterity and precision control as those within the network.

Rotate [local account passwords](#) on endpoints based on a pre-defined, fully customizable schedule, ensuring that password best practices are followed.

Privilege Manager can record all executable events on managed endpoints so you can review, search, and analyze these logs in a unified manner without leaving the console.

Child processes are those that execute from within a file such as a PDF and are frequently how malware executes on an endpoint. Privilege Manager allows you to prohibit execution of Child Processes to ensure unknown executables are restricted on your organization's network.

Privilege Manager's ability to quickly generate fully customized reports and schedule the execution and delivery of these reports is essential to maintaining a real-time understanding of every aspect of your least privilege program.

Review and manage local groups, including Group membership. This powerful capability prevents Group membership changes from being made on an endpoint, as all changes must be made via the Privilege Manager console.

This policy type requires that people provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition.

Enforce least privilege through policies for application control. You'll start with access to a broad library of out-of-the-box policies, all of which are completely customizable. Layered policies create the parameters that dictate precisely how privileges are accessed across your network. They define what actions people can run, and where. When policy conditions are met, Privilege Manager automatically applies an action (e.g. blocking, monitoring, application elevation, etc.) on one or multiple assets.

Web server clustering provides both [high availability and load balancing](#) by allowing multiple web servers to run Privilege Manager software. A clustered environment is key in disaster recovery scenarios as you can automatically failover to a separate web server with no downtime. Additionally, performance can be improved through load balancing by having multiple servers processing requests simultaneously.

Privilege Manager can automatically revoke all local administrative privileges on endpoints so you can adhere to a least privilege policy. With application-level privilege elevation, user-level privileges are not required and people can still access all the systems they need.

You can [manage all local users](#) on all endpoints across your organization, including the automatic rotation of local user password(s), all from a central console.

The ability to audit and review the activity of local users and groups is essential to retroactively identify problematic activity and reduce risk. Privilege Manager lets you swiftly review and search across all User and Group activity associated with privilege escalation on every managed endpoint.

The Privilege Manager mobile app for iOS and Android lets you manage endpoints, configure policies, process approvals, and receive event alerts via a mobile device so you can learn of requests and address issues quickly.

Privilege Manager integrates with reputation checking software like [VirusTotal](#) to provide application analysis in real time. This unique feature allows for reputation analysis of any unknown applications in order to mitigate risk of endpoint attacks from ransomware, zero-day attacks, drive-by downloads, and other unknown malicious software. With Privilege Manager, all applications that meet a general condition (i.e. executed from a specific directory or directories, file names, types, or any applications that are disassociated with existing policies) can be sent to VirusTotal for a reputation check and analysis.

Successful application control demands that you have a complete, real-time understanding of the status and activity of all endpoints. Privilege Manager provides a unified reporting dashboard so you can quickly evaluate the status of endpoints, review activity logs and event data, and access a broad library of reports. Responsive and fully configurable, Privilege Manager's dashboard reporting enables you to quickly drill down into reports across any dimension (time, geo-region, OS, status...) to evaluate activities and trends. From the dashboard you can also set up automated alerts to stay informed of potential problems.

Many organizations choose to protect their Privilege Manager web server by restricting it from direct outbound internet access. To secure your environment according to best practices, it is not enough to simply set your server offline because

Privilege Manager still will communicate directly to agents across your network that DO have direct internet access, therefore attackers can potentially use the connection between your endpoint agent and Privilege Manager to breach your web server. To prevent this direct connection between agent endpoints and your Privilege Manager web server, Privilege Managers allows for the setup of a [Reverse Proxy](#) machine with limited permissions. A properly configured Reverse Proxy will act as a buffer between Privilege Manager agents and the Privilege Manager server to limit server exposure.

Sandboxing quarantines applications so they are not allowed to execute, or only allowed to execute in a limited way so they don't touch any system folders or underlying OS configurations. Privilege Manager supports sandboxing for applications that are not known, to ensure they do not negatively impact productivity or introduce threats to the endpoint or network.

Many organizations leverage ticketing systems to streamline their support workflow and like to view and report on all support requests within a single system. Privilege Manager can be fully integrated into [ServiceNow](#), so support requests and IT responses can be managed, tracked, and reported via the ticketing system itself.

For those organizations utilizing the [Symantec Endpoint Protection](#) or Symantec Endpoint Protection Cloud solution for whitelisting and reputation, Privilege Manager can utilize the SEP whitelist and reputation engine to inform and prescribe its provision of application control capabilities across endpoints.

You can integrate your least privilege and application control program with a SIEM tool or other cyber security reporting and analytics services and tools. Privilege Manager can push out [SysLog](#) messages on a fully configurable schedule to any application or service that accepts the SysLog format.

Privilege Manager can integrate with [Microsoft System Center Configuration Manager](#) and scan SCCM software delivery "packages" for applications that can be whitelisted by Privilege Manager.

Privilege Manager supports allowing trusted applications, blocking to deny known malicious applications based on attributes, file hash, location, or certificates, and monitoring to prevent unknown applications from running. Monitoring provides a system for discovering the unknowns and adding an action that hinges on a reputation check. Distinct from allowing applications to run with default user level privileges, an elevation policy applies admin credentials to specified applications. This type of policy is often paired, so that employees can perform trusted tasks that require administrator credentials to complete, like installing a trusted application (Adobe) or device (printer), without involving IT support.

By only elevating application privileges based upon specific policies and criteria, Privilege Manager ensures people don't use Microsoft's UAC capabilities to grant a dangerous or unknown application administrative rights under any circumstance.

Privilege Manager identifies all local accounts on agent-installed endpoints and flags those with local admin rights, including hidden or hardcoded admin privileges. A single, comprehensive view makes management easy.

Glossary

Action - An action is not required in a policy. A policy can be designed, for example, to simply listen for specific application activity, and provide auditing information back to Privilege Manager. However, to apply controls to a process (executable), one defines an action in the policy.

Some common actions include:

- Adjust process rights,
- Add administrative rights,
- Remove administrative rights,
- Deny application execution,
- Require user justification - user provides a reason why they need to run the application,
- Application warning,
- Bypass UAC prompt,
- Require workflow approval - user needs approval to run an application, etc.

Agent - An agent is installed on every endpoint in your network and will 1) Receive and apply defined policies to govern application/process execution on the endpoint, 2) Execute tasks on the endpoint and feed audit and inventory data back to Privilege Manager.

Agent BaseUrl - The agent must be set to communicate directly with Privilege Manager. There exists a registry entry that is set upon agent installation - this registry key is called BaseUrl.

Agent Registration - The Privilege Manager agent completes a registration process when it initially contacts Privilege Manager following installation, but also at regular configurable intervals. So, registration occurs regularly.

Arellia - Arellia was the original name for Privilege Manager. Because of this, many file paths and back end notations include the term Arellia or AMS instead of Privilege Manager or TMS.

Computer Groups - (also called Resource Targets) Specified sets of computers that meet certain criteria (e.g. type of operating system, location of the computer, etc) that are targeted by certain policies and scheduled tasks.

Condition - Policy Conditions contain one or more filters that defines what a policy is 'listening' for. If the condition is satisfied in a policy, then an action is applied.

Config Feeds - Config Feeds can be found on the ADMIN page access from the Privilege Manager main page. Configuration feeds allow Thycotic to deliver new components to Privilege Manager. Simply click through the options in the Config Feeds page starting with the Select Items button and download anything appropriate. Once the item is downloaded, it is immediately available in Privilege Manager.

Dashboard - Dashboard is the term for Privilege Manager's landing page, or Home screen.

Event - Any notable file data on your network that is targeted by Privilege Manager is called an Event.

Discovery - Discovery is a term used by Thycotic for any information that is scanned or "found" on a network and imported or used by our products.

Least Privilege - Least Privilege is a security strategy organized around best practices. When effectively implemented, an organization's employees can navigate their network system with the lowest level of privileges. Higher credentials are flexibly (and often automatically) granted or denied based on users and the tasks being performed. This dynamic strategy significantly reduces the threat of security breaches across an organization without interfering with daily operations.

Filter - The Policy Condition lists one or more filters. A filter is defined to identify many things about an executable or process, or 'situation' when an executable or process is initiated.

Common Filters include:

- File specifications,
- Network location,
- Directory location,
- Application reputation,
- Application digital certificate,
- Time of day, User context (what AD security group a user belongs),
- Download source,
- Drive type,
- File owner,
- Internet Zone,
- Security Catalogs, etc.

Inclusion Filter/Exclusion Filter - When a filter is placed in the Inclusion Filters or Exclusion Filters under the Conditions tab of a policy definition, it can be used to explicitly include or exclude what is defined in the filter with respect to a policy. (I.e. Exclusion: apply this policy only if the user is NOT an administrator; Inclusion: apply this policy only if the computer is on the company network; Inclusion: apply this policy only to applications signed by a specific company's digital certificate, etc.)

Persona - Personas manage sets of privileges that are assigned to users on specific Windows computers or Computer Groups. A Persona includes a set of pre-defined filters and provide an easy way to assign policies based on Computer Groups and users. Filter parameters in a Persona are limited and specifically designed to be applied to Windows administrative users.

Policy - A set of conditions (Filters) that, when met, will apply an action to managed resources (target computers).

- **Blocking** - Type of policies that will deny an application from running based on a determined set of criteria.
- **Catch-All** Policy - A Catch-All policy is a type of Learning Mode policy that will gather information about any unknown events that happen in your network.
- **Elevation Policy** - An Elevation Policy will allow specified applications to run with administrator credentials.
- **Monitoring** - Monitoring is a dynamic method of managing applications that might not be included on a safelist or blocklist. Instead of trying to anticipate every executable users will run, you can apply a flexible policy that includes actions or reputation checking for unknown applications.
- **Non-Blocking** - Types of policies that will allow applications to run according to normal user credentials. This is often considered a neutral policy to specify trusted applications.

Policy Priority - Policies are evaluated in a certain order for each application that runs. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block will occur. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent.

RDP Monitor - Discontinued with version 10.6. The RDP Monitor is used to configure the Enhanced Session Monitoring feature in Secret Server. It is found in Privilege Manager because this feature uses the agent architecture defined by Privilege Manager, however this feature typically is not used in a Privilege Manager PoC.

Reputation Engine - Privilege Manager can call upon a reputation engine (e.g. VirusTotal) in real-time to check an application's public reputation. One can create a reputation checking policy in Privilege Manager through Monitoring policies. This type of policy can take application information and send it to the engine in real-time and act on the application based on the returned reputation. For example, if the reputation engine returns a BAD grade, the application can be denied. It is recommended to apply this type of policy to specific directories where new or unknown applications might reside - like the Downloads, TEMP, or Desktop directory.

Resource Targets - (also called Computer Groups) Specified sets of computers that meet certain criteria (e.g. type of operating system, location of the computer, etc) that are targeted by certain policies and scheduled tasks.

Scheduled Tasks - A Privilege Manager policy may be defined to be applied based on a schedule. These items run using the Task Scheduler on each endpoint, and are only accessible by Privilege Manager administrators.

Secret Server - Secret Server is a second Thycotic product that many IT teams use to securely manage privileged accounts and passwords in an organization. Privilege Manager and Secret Server are separate products but often used together for a holistic approach to network security. The two products are highly integrated and some of the features cross between products. For example, the Secret Server license page houses Privilege Manager licenses, and Secret Server clients rely on Privilege Manager agent (RDP Monitor) when using the advanced session recording feature.

Send Policy Feedback - Send Policy Feedback is a setting that can be enabled for any policy that sends information to Privilege Manager. This is used in Learning Mode Policies and often valuable during testing, configuration, or auditing projects.

TMS - TMS is shorthand for Thycotic Management Server. It is an umbrella term for our base application layer that Privilege Manager runs on top of.

VirusTotal – The VirusTotal reputation service is supported by Privilege Manager as a reputation engine. A free VirusTotal API key will need to be obtained to use VirusTotal in Privilege Manager. Note that the free API has limits and may not be appropriate for a production environment that functions with over four requests per minute.

Getting Started Overview - On-premises

The following topics provide a guided path through the on-premises installation and setup steps that are part of the initial stand-up of an on-premises Privilege Manager deployment. For cloud specific getting started instructions refer to [Getting Started Overview - Cloud](#).

Preliminary Configuration

Refer to these topics to learn more about the initial installation and setup steps:

1. [System Requirements](#)
2. [Antivirus Exclusions](#)
3. [Privilege Manager Installation](#)
4. [Agents Installation](#)
 - o [Setting the Server Address for Privilege Manager Agents](#), if the address provided during the agent installation requires updates.
5. [Login](#)
6. [Licenses](#)

Familiarize yourself with the [Least Privilege](#) concept. Thycotic recommends a phased roll-out between the Application Control and Local Security, for example:

1. **Application Control:** Set up learning mode policies on a group of test endpoints to learn about applications running on your endpoint machines ([Event Discovery](#))
2. **Local Security:** Begin [managing your local user accounts](#) (only) and defining local group membership (Local Security | Manage Local Users)
3. **Application Control:** Tailor your policies so that they won't disrupt employee work ([Creating Policies](#)) but will block known malicious applications (Creating Policies | Example: Quarantine Specified Malware). Implement these basic policies across agents in production
4. **Application Control:** Continue to tailor policies according to employee roles. Create a "Request Access" system for any unknown applications. ([Creating Policies](#) (Workflow))
5. **Local Security:** Once a workflow has been established between employees and the Privilege Manager Helpdesk, begin managing all local privileged accounts (ex: local admins) on endpoints. (Local Security | Details Tab)

Refer to the Local Security documentation pages to learn more about:

- [Create & Manage Computer Groups, Local Groups, and Users](#)

Refer to the Application Control documentation pages to learn more about:

- [Application Control - Policy & Config Overview / Collecting File Data](#)
- [Sending Policies to Endpoints - View Deployment Status / Update Using Powershell / Agent Event Log Viewer](#)
- [Event Discovery - Learning Mode Policies & Examples / View Policy Results](#)
- [Creating Policies - Whitelisting, Blacklisting, Quarantine, Elevation, Greylisting, & Reputation Checking Examples](#)
- [Policy Priority Overview & Example](#)

Refer to the Integration documentation pages to learn more about:

- [Integration & Foreign Systems](#)

Refer to these documentation pages to learn more about:

- [Reports](#)
- [Troubleshooting](#)

Refer to these documentation pages to learn more about:

- [Policies Catalog](#)
- [Filters Catalog](#)
- [Actions Catalog](#)
- [Privilege Manager Glossary](#)

The following topics provide a guided path through the instance setup and subsequent initial sign-in steps of a cloud Privilege Manager instance.

- [Cloud Quickstart Guide](#)
- [Cloud Login](#)
- [Agents Installation](#)
 - [Setting the Server Address for Privilege Manager Agents](#), if the address provided during the agent installation requires updates.

Rollout Recommendation

Familiarize yourself with the [Least Privilege](#) concept. Thycotic recommends a phased roll-out between the Application Control and Local Security, for example:

1. **Application Control:** Set up learning mode policies on a group of test endpoints to learn about applications running on your endpoint machines ([Event Discovery](#))
2. **Local Security:** Begin [managing your local user accounts](#) (only) and defining local group membership (Local Security | Manage Local Users)
3. **Application Control:** Tailor your policies so that they won't disrupt employee work ([Creating Policies](#)) but will block known malicious applications (Creating Policies | Example: Quarantine Specified Malware). Implement these basic policies across agents in production
4. **Application Control:** Continue to tailor policies according to employee roles. Create a "Request Access" system for any unknown applications. ([Creating Policies](#) (Workflow))
5. **Local Security:** Once a workflow has been established between employees and the Privilege Manager Helpdesk, begin managing all local privileged accounts (ex: local admins) on endpoints. (Local Security | Details Tab)

Local Security

Refer to the Local Security documentation pages to learn more about:

- [Create & Manage Computer Groups, Local Groups, and Users](#)

Application Control

Refer to the Application Control documentation pages to learn more about:

- [Application Control - Policy & Config Overview / Collecting File Data](#)
- [Sending Policies to Endpoints - View Deployment Status / Update Using Powershell / Agent Event Log Viewer](#)
- [Event Discovery - Learning Mode Policies & Examples / View Policy Results](#)
- [Creating Policies - Whitelisting, Blacklisting, Quarantine, Elevation, Greylisting, & Reputation Checking Examples](#)
- [Policy Priority Overview & Example](#)

Integrations

Refer to the Integration documentation pages to learn more about:

- [Integration & Foreign Systems](#)

Reports & Troubleshooting

Refer to these documentation pages to learn more about:

- [Reports](#)
- [Troubleshooting](#)

Catalogs & Reference Guides

Refer to these documentation pages to learn more about:

- [Policies Catalog](#)
- [Filters Catalog](#)
- [Actions Catalog](#)
- [Privilege Manager Glossary](#)

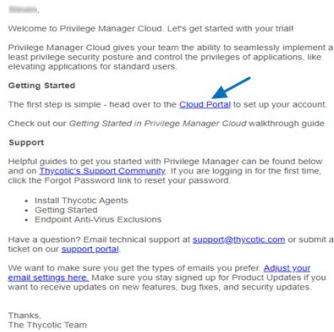
Privilege Manager Cloud is a scalable cloud platform, where all backend services, databases, and redundancy are securely managed by Thycotic and hosted on the Microsoft Azure platform. Customers do not have direct access to the databases or application file system.

This guide will walk you through an initial configuration of your cloud instance.

Initial Setup

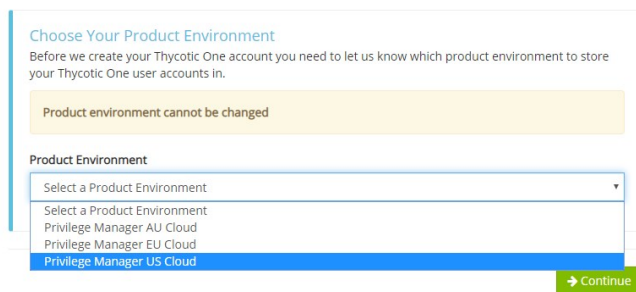
After you've signed up for a Privilege Manager Cloud trial, you will receive 2 emails. The first one is from Customer Support and will ask you to create a password to log into the customer support portal.

The second email you will receive is from Thycotic Sales titled Privilege Manager Cloud Trial. This email directs you to the **Cloud Portal** to begin your instance setup.

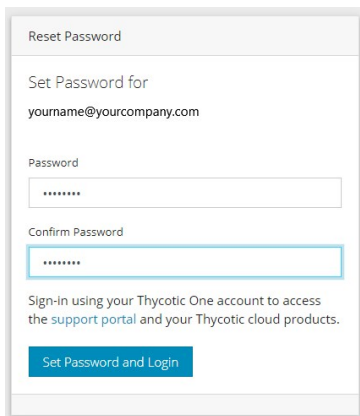


Select the Cloud Portal link. On the Setup page, choose your Cloud Environment location from the dropdown menu. Then click **Continue**.

Setup

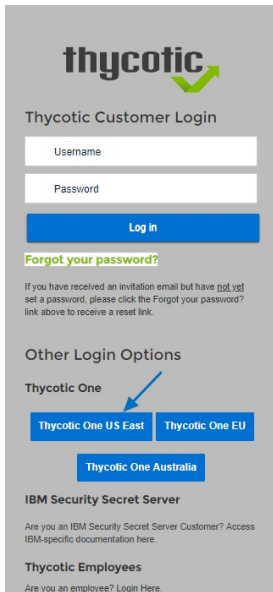


You will be directed to the **Thycotic One** portal to create the password for your first user account with Administrator credentials. This account will be assigned to the email address you entered to request the trial. After confirming the password, click **Set Password and Login**.



Important: Thycotic recommends that you store the password in a secured physical location such as a safe or locked file cabinet. You can reset the password using an email reset, but **if this password is forgotten or you no longer have access to the email account, Thycotic will not be able to reset this password.**

On the Thycotic Login page, click the blue button that corresponds to your new Cloud's Thycotic One location (chosen above).



thycotic

Thycotic Customer Login

Username

Password

Log in

Forgot your password?

If you have received an invitation email but have not yet set a password, please click the Forgot your password? link above to receive a reset link.

Other Login Options

Thycotic One

Thycotic One US East Thycotic One EU

Thycotic One Australia

IBM Security Secret Server

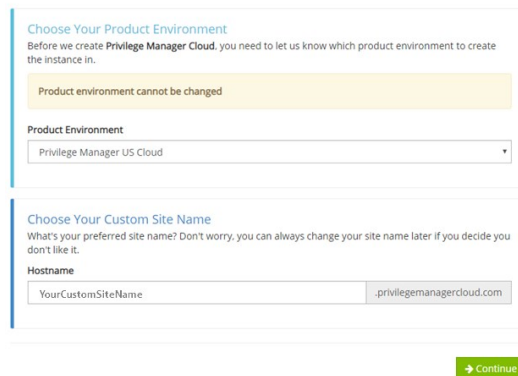
Are you an IBM Security Secret Server Customer? Access IBM-specific documentation here.

Thycotic Employees

Are you an employee? Login Here.

Next, on the Setup page choose the location of your cloud environment and enter the **Name** for your subdomain. Do not use special characters or spaces.

Setup



Choose Your Product Environment

Before we create **Privilege Manager Cloud**, you need to let us know which product environment to create the instance in.

Product environment cannot be changed

Product Environment

Privilege Manager US Cloud

Choose Your Custom Site Name

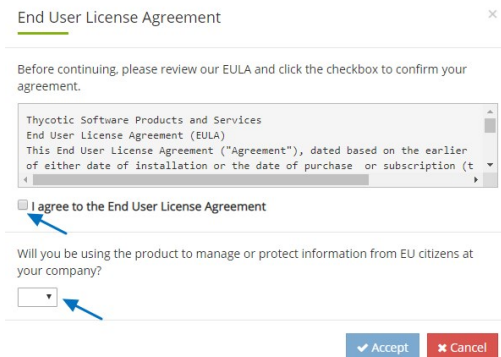
What's your preferred site name? Don't worry, you can always change your site name later if you decide you don't like it.

Hostname

YourCustomSiteName .privilegemanagercloud.com

Continue

Read the End User License Agreement and click the box to signify agreement. From the dropdown, select Yes or No to signify your organization's oversight of EU information. Click **Accept**.



End User License Agreement

Before continuing, please review our EULA and click the checkbox to confirm your agreement.

Thycotic Software Products and Services
End User License Agreement (EULA)
This End User License Agreement ("Agreement"), dated based on the earlier of either date of installation or the date of purchase or subscription (t

I agree to the End User License Agreement

Will you be using the product to manage or protect information from EU citizens at your company?

Yes

Accept Cancel

It will take approximately **20 minutes** for your new Privilege Manager Cloud to spin up.

Working

Please wait while we build your product. The process may take up to 20 minutes to complete.



When complete, click **Go to your Privilege Manager Cloud** instance and **Login with Thycotic One**.



Ready

Your product is ready

[Go to your product](#)

You will be automatically redirected to your new Privilege Manager Cloud Dashboard.

Select the *Privilege Manager* link



Privilege Manager Server Setup Home

Privilege Manager

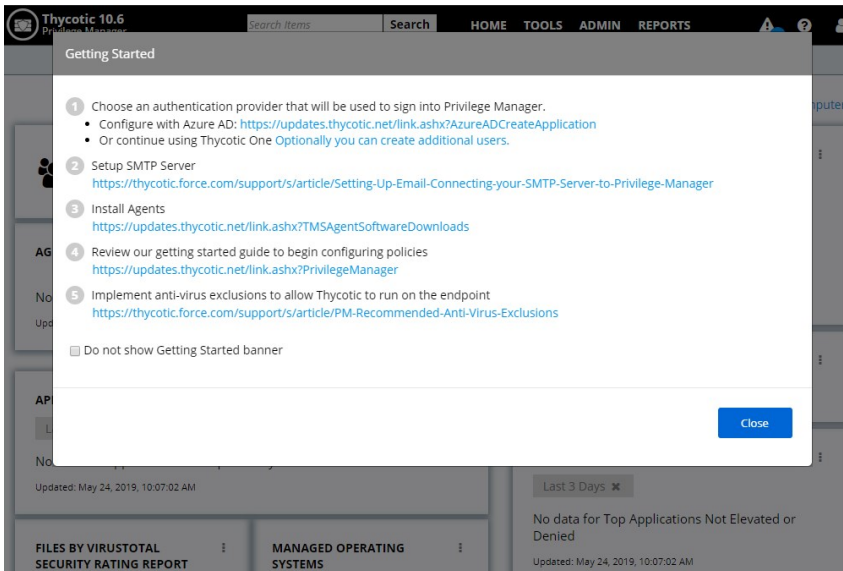
[Privilege Manager](#)

Online Setup Resources

[Getting Started with Privilege Manager](#)

Getting Started Screen

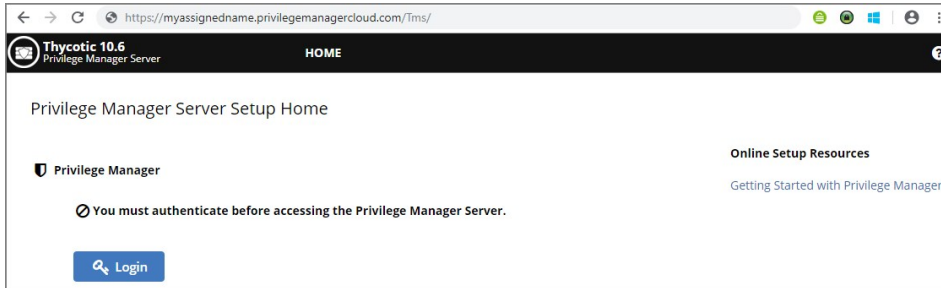
Follow the steps on the Getting Started screen. Start with step 1 to allow other users to access Privilege Manager and make sure all 5 steps are completed or reviewed before continuing.



To login to a Privilege Manager Cloud instance, use the URL and credentials provided to you. The URL is in the format of:

<https://myassignedname.privilegemanagercloud.com/TMS/>

1. Navigate to your assigned login URL.



2. Click the Login button. This opens the Sign In dialog:

The 'Sign In' dialog box has a title 'Sign In'. Below it is a label 'Email address' followed by a text input field containing the placeholder 'Enter Email Address'. A blue 'Next' button is positioned below the input field. At the bottom of the dialog, there are two links: 'Create New Account' and 'Reset My Password'.

- a. Enter your Email address and click Next.
- b. Enter your password and click Sign in.

3. Select Privilege Manager on the Server Setup Home page:



The Privilege Manager cloud console home page opens:

The screenshot shows the main dashboard of the Thycotic 10.6 Privilege Manager cloud console. The top navigation bar includes 'HOME TOOLS ADMIN REPORTS' and a search bar. Below the navigation, there's a header 'Showing results for All 64-bit Windows Computers with Application Control Agent Installed (Target)'. The dashboard is divided into several sections:

- Local Security:** Manage your Local Users and Groups.
- Application Control:** Control Applications on your Network.
- AGENT POLICY STATE:** A green circular gauge shows '1 Total Count' with '100% Normal' status.
- AGENT REGISTRATION STATE:** A red circular gauge shows '1 Total Count' with '100% Critical' status.
- EVENT SUMMARY:** Shows counts for 'Events', 'Elevations', and 'Blacklist', all currently at 0.
- PENDING APPROVAL REQUESTS:** Lists a request for 'chrome.exe' with 'Approve' and 'Deny' buttons.
- TOP APPLICATIONS NOT ELEVATED OR DENIED:** A section for listing problematic applications.

Note: To import and synchronize Azure Active Directory Groups and Users, refer to the following topic: [Setting Up Azure Active Directory Integration in Privilege Manager.](#)

To add Thycotic One Users manually refer to the following topic: [How to Add Thycotic One Users Manually.](#)

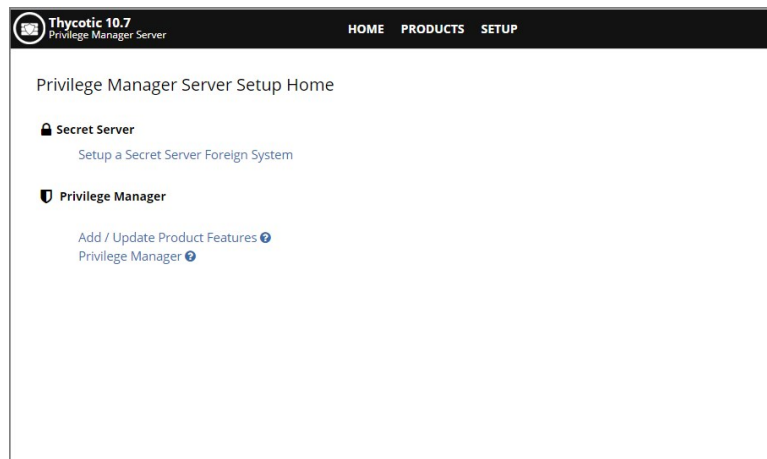
Initial Login

Using the credentials configured in the Create User section of the on-premises installation, validate that you can login to Privilege Manager and view the home screen.

The login URL for an on-premises Privilege Manager instance has this form:

`https://[server-domain]/TMS/PrivilegeManager`

Note: On combined Secret Server/Privilege Manager installations you are initially logged in through Secret Server. If this is the case, you can find Privilege Manager by navigating to **Tools | Privilege Manager**.



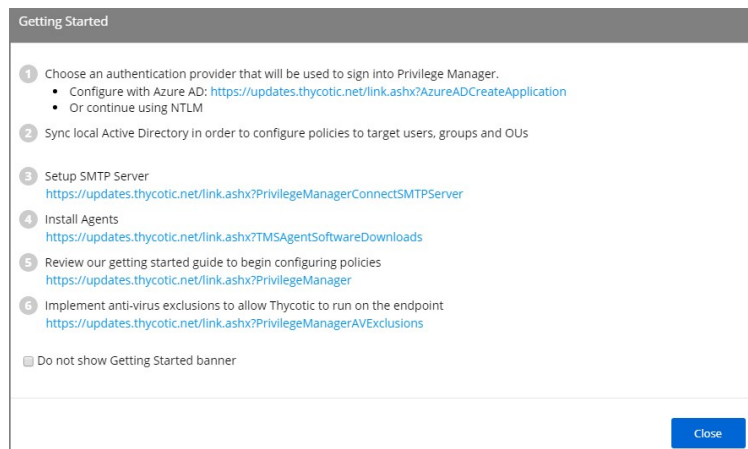
Use the Privilege Manager link to login to the product. If you need to add or update product features, such as connectors for foreign systems, use the Add / Update Product Features link.

The **Setup a Secret Server Foreign System** link can be used to set-up an integration with Secret Server. This will also allow you to use Secret Server as an authentication provider. Also refer to [Setting up Integration between Privilege Manager and Secret Server](#)

At initial login the Getting Started Banner displays with help tips and next steps:

- Choose an authentication provider that will be used to sign into Privilege Manager.
- Setup the SMTP Server.
- Install Agents.
- Review the documentation to begin configuring policies.
- Implement anti-virus exclusions to allow Thycotic to run on the endpoint.

You may choose to not show the Getting Started Banner on subsequent logins.



The Home screen of Privilege Manager can be found by clicking Home in the top banner of any page inside of Privilege Manager. From this dashboard you can jump into either Application Control or Local Security, depending on what you want to do. You also will be given different snapshots of various important information about your environment. Once you have agents installed and policies setup, you'll have a lot going on from the Home Dashboard:

Thycotic 10.7
Privilege Manager

Search Items **Search** **HOME** **TOOLS** **ADMIN** **REPORTS**

[Getting Started - Show Getting Started checklist](#)

Showing results for Windows Computers

Local Security Manage your Local Users and Groups	Application Control Control Applications on your Network
AGENT POLICY STATE No data for Agent Policy State Updated: Jan 9, 2020, 6:38:48 PM	AGENT REGISTRATION STATE No data for Agent Registration State Updated: Jan 9, 2020, 6:38:48 PM
APPLICATION EVENTS PER POLICY Last 3 Days No data for Application Events per Policy Updated: Jan 9, 2020, 7:21:10 PM	
FILES BY VIRUSTOTAL SECURITY RATING REPORT No data for Files by VirusTotal Security	MANAGED OPERATING SYSTEMS No data for Managed Operating Systems

EVENT SUMMARY
Last 3 Days
Events: 0 | Elevations: 0 | Blacklist: 0
Updated: Jan 9, 2020, 7:21:10 PM

PENDING APPROVAL REQUESTS
Updated: Jan 9, 2020, 7:21:10 PM, showing 0 of 0

TOP APPLICATIONS NOT ELEVATED OR DENIED
Last 3 Days
No data for Top Applications Not Elevated or Denied
Updated: Jan 9, 2020, 7:21:10 PM

Licensing

Licensing for Privilege Manager Cloud customers is managed via Thycotic.

To install new Privilege Manager licenses, it will depend on whether you chose to

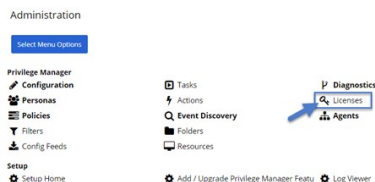
- perform a standalone install, or
- install Secret Server in tandem with Privilege Manager.

Note: Online activation is not required for Privilege Manager licenses.

Steps for Standalone Privilege Manager Installation

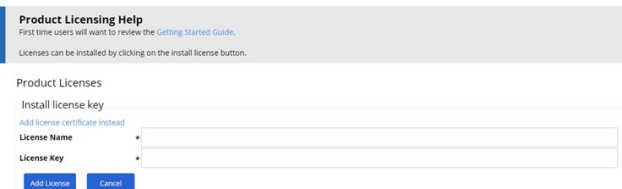
To install licenses without Secret Server:

- Navigate to **Admin | Licenses** or **click** the Product Licenses Installed link in the top banner.



- On the Privilege Manager Licenses page, click **Add License**, then

- enter your License Name(s) and
- Key(s) one at a time,
- select Add License to finish.



Steps for Combined Secret Server + Privilege Manager Installation

To install licenses with Secret Server on the same server as Privilege Manager, you will need to install licenses through the Secret Server UI and then import the new licenses into Privilege Manager.

- To access Secret Server's licensing page, either click the Secret Server link listed in the banner at the top of the Privilege Manager Licenses page or navigate to **Admin | Setup – Licenses**.
- From Secret Server's License page, select Install New License.
- Enter your License Names and Keys individually or through the Bulk Entry Mode.
- Click Save or Add Multiple Licenses to save the License Keys. Installing these licenses in Secret Server will automatically import the licenses into Privilege Manager.
- Navigate back to the Privilege Manager License page to verify under: **Tools | Privilege Manager | Admin | Privilege Manager–Licenses**.

Note: If your license keys do not appear or you have too many keys listed, click the import task link and then Run Task to reset.

If you previously had evaluation licenses and recently purchased, you will need to install your new license keys for production via the same steps as above. Normal trial licenses offer 50 endpoint agents and expire 30 days after issue.

When your Privilege Manager licenses expire or have exceeded the licensed count, Privilege Manager will stop processing new inventory and application control events. Endpoints will continue to enforce policies.

- Client License:** This license provides coverage for endpoints that are workstations, such as Windows 10, windows 7, etc.
- Server License:** This license provides coverage for endpoints that are server machines, Windows Server 2019, Windows 2016, etc.
- Support License:** Without having a support license you will not be able to complete upgrades and will not be able to receive support or maintenance.

PRODUCT	OS TYPE	STATUS	TOTAL LICENSES	IN USE	START DATE	ALP RENEWAL	EXPIRES
Privilege Manager Suite	Client	OK	500		12/31/2024	12/31/2024	
Privilege Manager Suite	Server	OK	500		12/31/2024	12/31/2024	

When a license has expired or have exceeded the license count

The Server will stop accepting data sent from agents that are in violation of the licensing. New endpoints will register, but will not be recorded, which means the endpoint:

- Will not get added to the resource targets and will not collect application or user inventories
- No password changes will occur, etc.
- Policies will run on the endpoint, but the server will completely discard the data, and it won't be stored.
- Tasks will not run - all automation will stop and event Discovery will not inventory users or applications, new endpoints won't be discoverable.

If you need to reset licenses for your Privilege Manager instance refer to the [Reset Licensing](#) topic.

Installation and Upgrades

This section contains all you need to know about installation and upgrading Privilege Manager and all its components.

The following topics are available:

- [System Requirements](#)
- [Recommended Anti Virus Exclusions](#)
- [Software Downloads](#)
- [Installation](#) - recommended installation procedure
 - [Manual Installation Instructions](#)
 - [Item Encryption](#)
- [Agent Installation](#)
 - [Agent System Requirements](#)
 - [Install Codes](#)
 - [Windows Bundled Agent Install](#)
 - [Windows](#)
 - [Mac OSx](#)
 - [Uninstall via Command Line](#)
 - [Agent Hardening](#)
- [Upgrades](#)
 - [Upgrading from 8.2 to Privilege Manager 10.4 and up](#)
 - [Offline Upgrades Privilege Manager](#)
 - [Offline Upgrades - Combined Secret Server and Privilege Manager](#)

Privilege Manager System Requirements

These are requirement for an on-premises integration.

Note: Verify that the .NET version between the Privilege Manager and Database Server in use are matching, especially if installed on different Windows Server versions.

4 CPU Cores	4 CPU Cores
8 GB RAM	16 GB RAM
40 GB Disk Space	150 GB Disk Space
Windows Server 2012 R2 or newer	Windows Server 2012 R2 or newer
IIS 7 or newer	SQL Server 2012 or newer
.NET 4.6.1 or newer	
Powershell 3.0 or newer	

Note: Environments with over 25,000 Endpoints require a scoping call with a Thycotic engineer.

8 CPU Cores	8 CPU Cores
32 GB RAM	64 GB RAM
40 GB Disk Space	500 GB Disk Space
Windows Server 2016 or newer	Windows Server 2016 or newer
IIS 7 or newer	SQL Server 2012 or newer
.NET 4.6.1 or newer	
Powershell 5.0 or newer	

- RAM, CPU, and Disk Space - negligible
- Windows XP SP 3 or newer. Thycotic performs validation on the latest Windows OS that is available via the Microsoft Insider Program to ensure any required changes are made prior to a new OS version release.
- MacOS 10.11 (El Capitan) or newer.

- System Requirements apply to both physical and virtual machines.
- For best performance, we recommend using dedicated (clean) servers for Thycotic products.
- PowerShell must be allowed to execute and cannot be blocked on the server or the endpoint by other products.
- If .NET and/or IIS features are not already installed on the web server, the Thycotic Installer will add and configure them automatically.
- If SQL is not already installed on a database server, the Thycotic Installer can setup SQL Express on the web server, however SQL Express is intended for Trials and Sandbox environments ONLY. Though Thycotic will support SQL Express, users will likely experience performance issues due to the memory and product limitations. If experiencing performance issues while using SQL Express, it is highly recommended to upgrade to SQL Server prior to contacting Thycotic Support.
- A link to Microsoft documentation on the use and limitations of SQL Express can be found at: <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017>
- Web Servers that are NOT supported: Small Business Server (SBS), The Essentials Edition, Domain Controllers, Sharepoint Servers.

- **Outbound (port 443 - HTTPS):** This is the default access port through which the agent connects to the server. You may specify a different port based on your environment.
- **Inbound (port 5593):** This is the default and only port that the agent listens on. This port is not required and you can block port 5593. If you block the port, the agents pull updates from the server based on a set schedule.
- **SQL (port 1433):** This is the default SQL DB port. The SQL port can be customized.

Anti Virus Exclusions

For Privilege Manager users we recommend several antivirus exclusions to maintain application performance and integrity. These guidelines apply to both real time and on-demand antivirus scanning.

Exclude these two directories from your antivirus filters to ensure Privilege Manager processes will not be blocked (or for a more granular approach to these exclusions, see the Client Item Database and Privilege Manager Application Control Agent Services sections at the end of this article):

```
%ProgramData%\Arellia\  
%ProgramFiles%\Thycotic\
```

Exclude the following antivirus programs for Privilege Manager's web server, also sometimes called Thycotic Management Server (TMS):

Temporary ASP.NET Files

Exclude the following directory to prevent degradation in performance and possible unexpected restarts of the Tms and TmsWorker IIS application pools:

```
%SYSTEMROOT%\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
```

Exclude the following antivirus programs for databases.

SQL Server Data Files

These files contain data and typically have the following extensions:

- .mdf - primary data filegroups
- .ndf - secondary data filegroups
- .ldf - transaction log filegroups

SQL Server Backup Files

These files contain the backup files and typically have the following extensions:

- .bak - database backup files
- .trn - transaction log backup files

By default the directories that contain the Data and Backup files are located under C:\Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL.

SQL profiler trace files

These files contain SQL Profiler Trace log data and can be contained in any folder.

They usually have the file extension .trc.

Exclude the following antivirus programs for managed endpoints.

Request Run As Administrator Registry Key

Privilege Manager Application Control installs a context menu item that allows executables to be "Request Run as Administrator."

This context menu is added under the following registry key which some antivirus programs incorrectly flag as malware:

```
HKLM\SOFTWARE\Classes\exe\Shell
```

Client Item Database

This directory contains the Thycotic Agent client item database and should be excluded from antivirus to prevent corruption:

```
%ProgramData%\Arellia\ClientItems
```

If required you can further limit this exclusion to all files with the .db and .db-* extensions under this location

Privilege Manager Application Control Agent Service

Some antivirus products require that the Privilege Manager Application Control service be excluded from tamper protection rules because Application Control manipulates other applications which antivirus products may mistake as malicious.

```
C:\Program Files\Thycotic\Agents\ApplicationControl\ArelliaACSvc.exe
```

Software Downloads

This page provides links to Thycotic Privilege Manager product and agents software downloads.

10.7.1	Combined Secret Server and Privilege Manager Installer - Authentication required!
	Bundled Privilege Manager Agent Installer - Windows
	Core Thycotic Agent (x64)
	Core Thycotic Agent (x86)
	Application Control Agent (x64)
	Application Control Agent (x86)
	Local Security Solution Agent (x64)
	Local Security Solution Agent (x86)
	Privilege Manager macOS Agent
10.7.0	Combined Secret Server and Privilege Manager Installer - Authentication required!
	Bundled Privilege Manager Agent Installer - Windows
	Core Thycotic Agent (x64)
	Core Thycotic Agent (x86)
	Application Control Agent (x64)
	Application Control Agent (x86)
	Local Security Solution Agent (x64)
	Local Security Solution Agent (x86)
	Privilege Manager macOS Agent

Prerequisites

ASP.NET Website

Privilege Manager is installed as an ASP.NET website. The setup.exe file will set up the website with the correct permissions and create the settings in IIS.

SQL Server Database

Thycotic products require an instance of SQL Server for the database backend and an instance of SQL Express will be installed by the setup.exe file if missing. The SQL Server database will require a SQL account with db_owner permission to complete the installation. SQL Express edition is intended for Sandbox and trial environments, Thycotic recommends purchasing SQL licensing for use in production environments.

Administrative Access

Throughout the installation process, you will be required to be an administrator to perform most actions. Please ensure that you are logged onto your system with a Windows account that has administrative rights before beginning your install.

Additional Recommendations

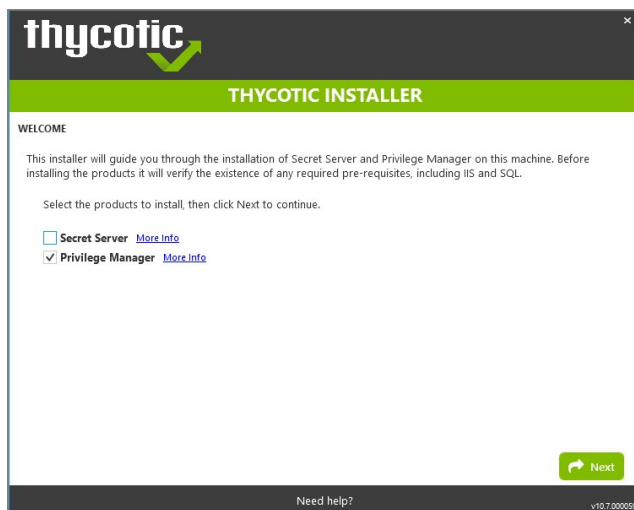
1. Use an SSL certificate for Privilege Manager.
2. Run Microsoft Update on your server to make sure all components are up to date.

Download the Latest Version of PM Installer

The latest version of Privilege Manager is available for download under the [Software Downloads](#) topic. It is recommended to run the downloaded setup.exe file as an administrator.

Running the Installer

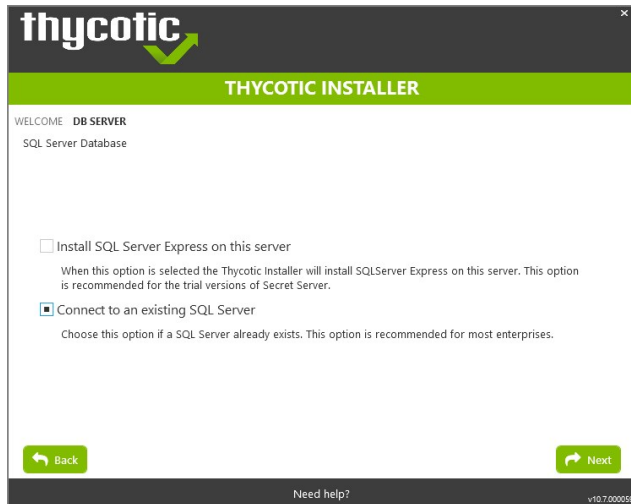
1. Double-click the downloaded setup.exe to run the installer. The installer opens on the **Welcome** tab:



2. Verify that the Privilege Manager box is checked.

Note: Privilege Manager as a standalone product comes with three roles Administrator, Basic User, and Help Desk User roles. Please refer to [Application Roles](#).

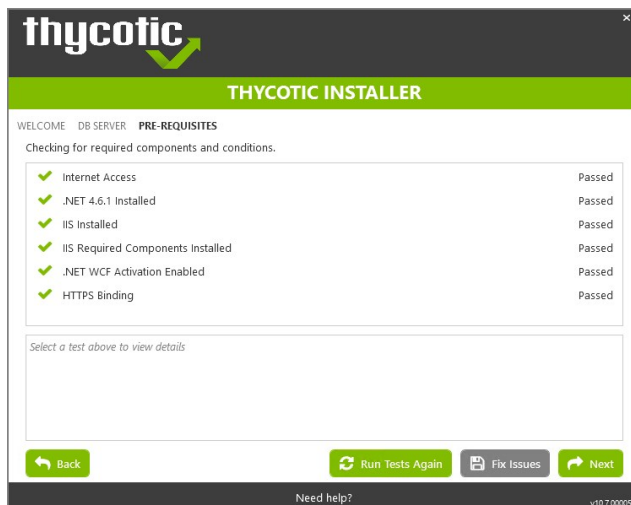
3. On the **Database** tab you can choose to either install SQL Express or connect to an existing SQL Server. SQL Express requires a internet access for the installer to download the installation package for SQL Express.



Note: For production environments Thycotic recommends installing a licensed edition of SQL before installing Thycotic products. The Express edition is only recommended for trial and sandbox environments.

- o If Internet access is not available a link to download SQL Server Express will be presented to the user. At that point, they are expected to install SQL Server Express and then restart the installer.
- o If Internet Access is available SQL Server Express will be installed.
- o After SQL is installed select Connect to an existing SQL Server.

4. The **Pre-Requisites** tab makes sure everything that is required to install Privilege Manager is setup correctly. Everything on this page can be installed outside of the installer, but if not, the installer will install and configure them for the user. Think of this page as the non-Thycotic configuration. If there are issues with this page it is very likely that the Internet will be able to help as these are not installation features that are specific to Thycotic. Click Fix Issues to automatically install the necessary pre-requisites. When Successful, click Next.



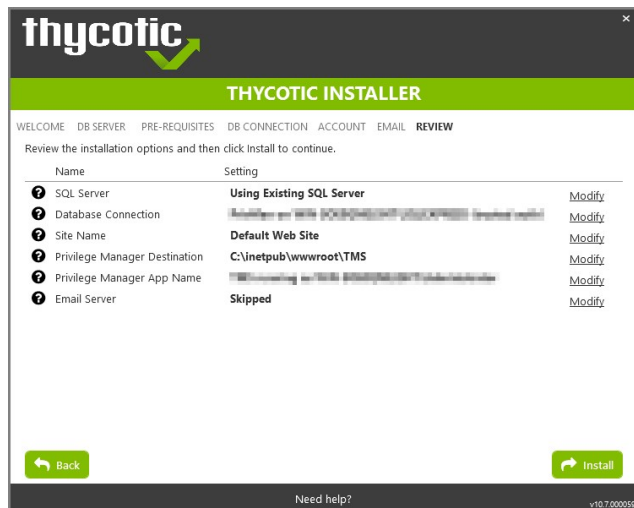
5. If you chose the "Connect to an existing SQL Server" option on the Database page, the **Database Connection** tab will now prompt you for the connection information that Privilege Manager will use. The Test Connection button must be run successfully before installation can continue. Once connection is established, click **Next**.

Note: If you are not using a default InstanceName on the SQL Server for the Privilege Manager database, provide the SQLServerName\InstanceName for **ServerName** or **IP**.

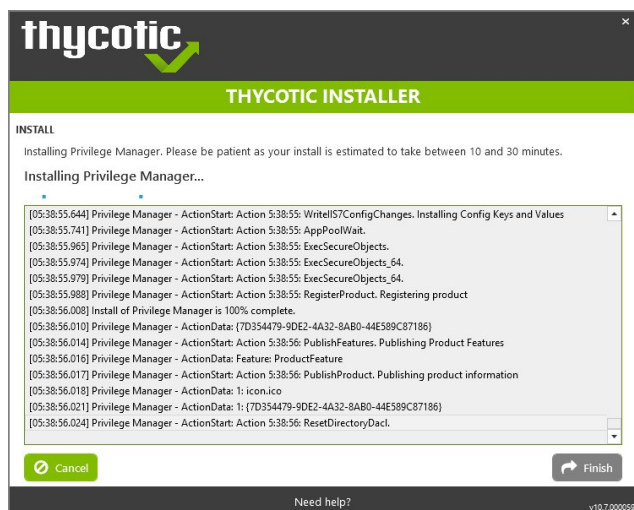
1. If you choose SQL Server Authentication, next the Account tab will prompt for the server location where your SQL database is currently installed. Provide the Server Name or IP address for your Database server and Authenticate with Administrator SQL credentials. If your Secret Server database does not yet exist when you click "Test Connection" the Installer will create it. When the connection has been tested successfully, click Next.

6. The **Email Server** tab opens, here the connection information for the email server can be entered. This is also optional and can be skipped to be configured later in the application by clicking Skip Email. This page will configure email for Privilege Manager.

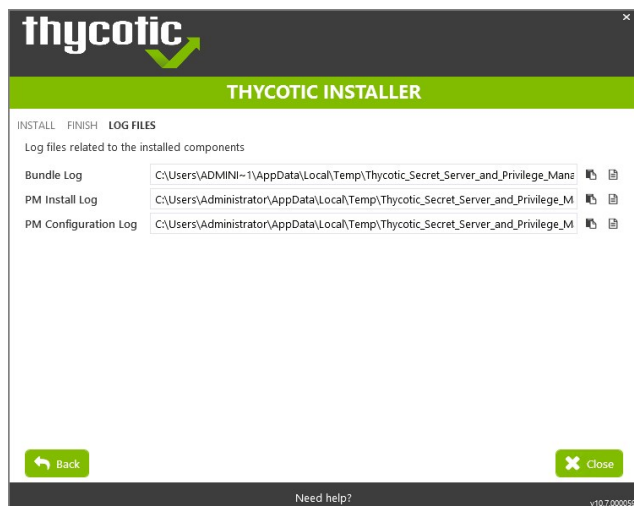
7. On the **Review** tab, most settings are defaulted for a user and they can choose to modify settings at this step. Certain validations will occur on these settings before the install can begin. Click Install to proceed.



8. The Install page will show the status from log files as Secret Server and/or Privilege Manager are installed. Installs vary depending on your environment, most installs last between 20-60 minutes.

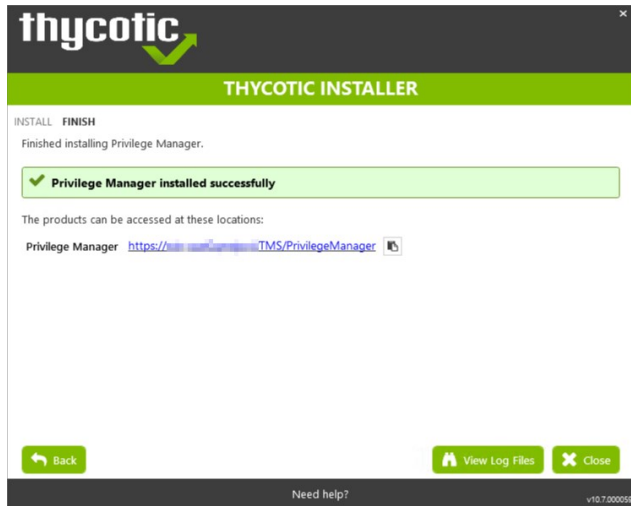


9. The **Log Files** tab is available after the applications are installed. The installer provides the link to open a web browser to the product login page. At this point, everything is installed and ready for you to begin using your new Thycotic product. If the installation failed or you wish you view the logs from the installation you can click the View Log Files button.



10. On the **Finish** tab, when the install has successfully completed, click the provided Privilege Manager URL to navigate directly to your setup landing page or open a browser and navigate to where your Privilege Manager is located, for

example: <http://localhost/TMS/PrivilegeManager>.



Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

If you need to manually install Privilege Manager on a system and you already have an existing server installation, refer to the installation instructions described under the [High Availability Set-up for Privilege Manager](#). Otherwise follow the steps below.

Note: Thycotic recommends to always use the setup.exe installer to verify that your system meets the pre-requisites.

Download Privilege Manager Application Files

Make sure you have the prerequisites (IIS, .NET Framework, and SQL Server) installed before following the steps listed below.

After clicking the download link on the [Software Downloads](#) page, you will be able to download a .zip file that contains both Privilege Manager and Privilege Manager files.

Zip File Extraction Tool

You will also need to install a zip application like winzip or 7-zip to extract files for this install. 7-zip is used in the instructions below and can be downloaded for [free here](#).

Manual Installation (no setup.exe)

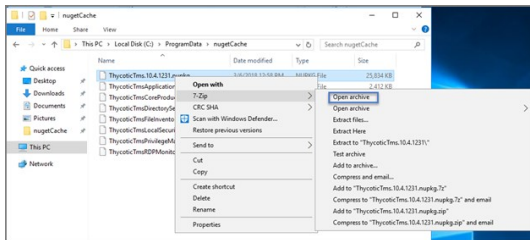
Clicking the download link above will take you to a portal page where you can choose to download a .zip file that contains the application files. Use this .zip file for the instructions below. Privilege Manager can be installed in a few different ways, as a:

- Virtual Directory
- Website

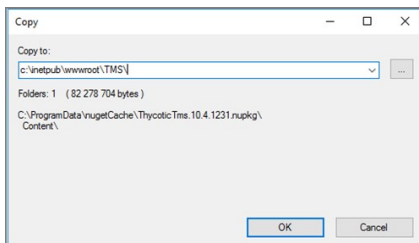
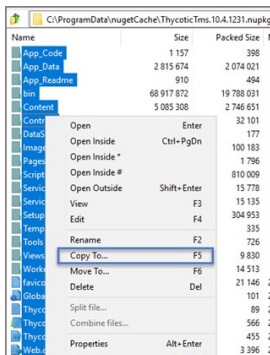
Installing as a Virtual Directory

1. Extract the contents of the .zip file and select the nugetCache folder. Move the contents of that folder to a temporary location like C:\ProgramData\ (Recommended)
2. Create a folder called TMS in the location C:\inetpub\wwwroot\
3. Navigate back to c:\ProgramData\nugetCache\ and using any zip application (ex: 7-zip, winzip, winrar, etc), open ThycoticTms.xx.x.xxx.nupkg

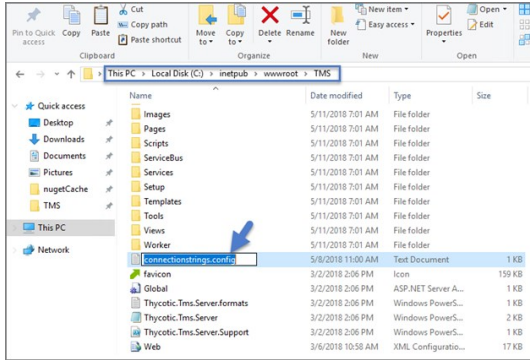
To do this with 7-zip: right-click ThycoticTms.xx.x.xxx.nupkg | 7-zip | Open Archive.



4. Open the Content directory and ctrl-A to select all of its contents. Copy these to the location C:\inetpub\wwwroot\TMS\



5. In C:\inetpub\wwwroot\TMS\ where you have extracted the TMS Site files, create a new file right-click **New | Text Document** called connectionstrings.config



6. Next, decide what mode you want to use to access your SQL database and follow the corresponding steps:

- **Mixed Mode/Integrated Security=False*** (for easiest configuration): Mixed Mode is required if you intend on using a SQL Server account to authenticate Privilege Manager to your SQL Server instance. If you are doing an evaluation and using the Privilege Manager setup.exe installer, we recommend using Mixed Mode with a SQL authentication account. This option will also require you to set a password for the SQL Server system administrator (sa) account. See the Integrated Security=False section below to use Mixed Mode.
- **Windows Authentication Mode/Integrated Security=True*** (recommended for best security): This will prevent SQL Server account authentication and requires a Windows Service account to run the Privilege Manager website. This will also require additional configuration in IIS once Privilege Manager is installed. Follow the steps under the Integrated Security=True section below to use Windows Authentication.

Integrated Security=False

Open in Notepad the connectionstrings.config file created in step 5 and copy in the following text; replacing the SQL Server Name, Database Name, User Name, and Password (highlighted in bold below) with values for your environment. Save changes.

```
<connectionStrings>
<add name="ApplicationServerWorkflowInstanceStoreConnectionString"
connectionString="Data Source=SQLServerAddress;Initial Catalog=DatabaseName;Integrated Security=False;User ID=myUserName;Password=myPassword;Application Name='Arellia Management Server - WF'" />
<add name="AmsConnectionString"
connectionString="Data Source=SQLServerAddress;Initial Catalog=DatabaseName;Integrated Security=False;User ID=myUserName;Password=myPassword;Application Name='Arellia Management Server'" />
</connectionStrings>
```

Integrated Security=True

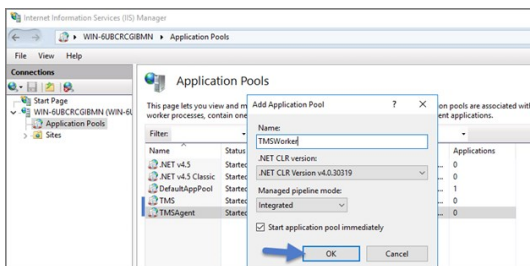
If you choose to set Integrated Security to True, you will need to ensure that the application pool service accounts have access to the database server in a later step.

Open in Notepad the connectionstrings.config file created in step 54 and copy in the following text; replacing the SQL Server Name and Database Name (highlighted in bold below) with values for your environment. Save changes.

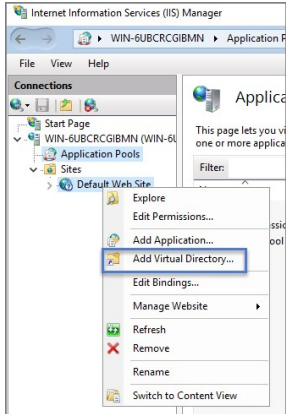
```
<connectionStrings>
<add name="ApplicationServerWorkflowInstanceStoreConnectionString"
connectionString="Data Source= SQLServerAddress;Initial Catalog= DatabaseName;Integrated Security=True;Application Name='Arellia Management Server - WF'" />
<add name="AmsConnectionString"
connectionString="Data Source= SQLServerAddress;Initial Catalog= DatabaseName;Integrated Security=True;Application Name='Arellia Management Server'" />
</connectionStrings>
```

Continue: Installing as a Virtual Directory

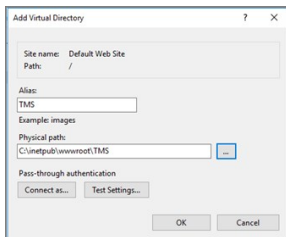
1. Open Internet Information Services Manager (inetmgr.exe).
2. Under your local server, right-click Application Pools and select **Add Application Pool..** Add three new application pools. Name one TMS, name another TMSAgent, and name the third TMSWorker.



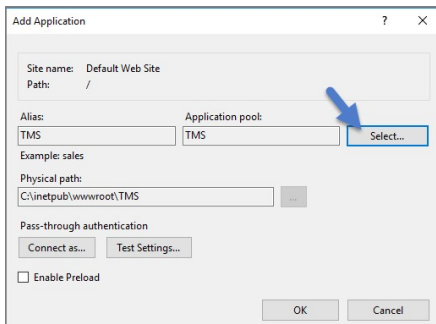
3. When creating your connection string, if you selected Integrated Security=True in step 6, change the Identity for your application pools to a service account that has DBOwner rights on the SQL database & make sure that the Identity for the three app pools have Modify rights to the folder that you put the Privilege Manager files into. To setup the service account correctly and set folder permissions and the Identities for these app pools, follow all of the steps in [Using a Service Account to run the IIS App pool](#) now.
4. Right-click Default Web Site in IIS and select Add Virtual Directory..



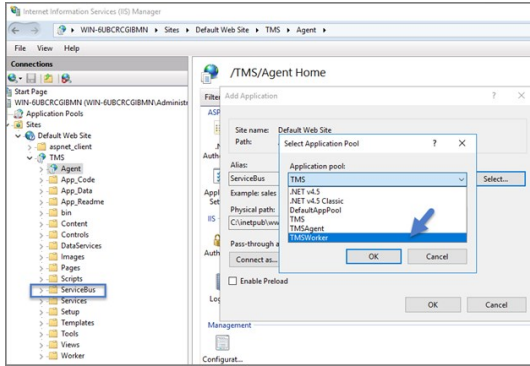
5. Select an alias for your Privilege Manager. The alias is what will be appended to the website. For instance, "TMS" in `http://myserver/TMS`.
6. Next, enter the physical directory where you unzipped Privilege Manager `C:\inetpub\wwwroot\TMS`.
7. Click **OK**.



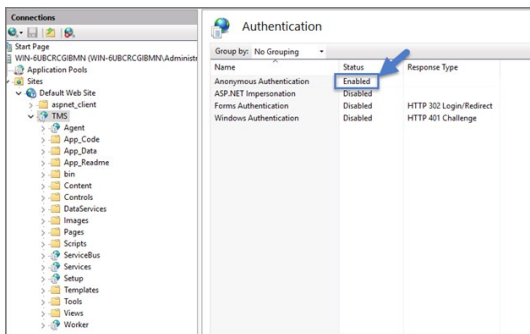
8. In the tree, right-click the new virtual directory and select **Convert to Application**.
9. Set the Application Pool to the one called TMS. Click **OK**.



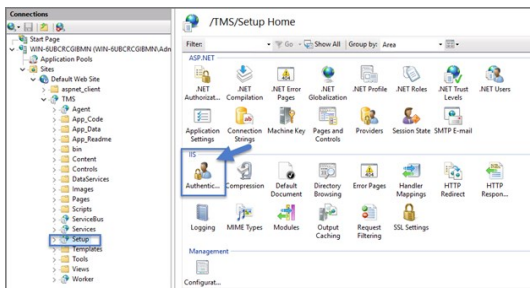
10. In the virtual directory expand the new TMS site, right click the Agent Subfolder and select **Convert to Application**.
11. Set the Application Pool to the one called TMSAgent and click **OK**.
12. Next, in the virtual directory navigate to the ServiceBus Subfolder. Right-click and select **Convert to Application**.
13. Set the Application Pool to the one called TMSWorker. Click **OK**.



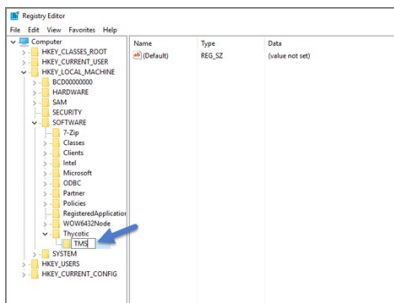
14. In the virtual directory select the Services Subfolder, right-click the new virtual directory and select **Convert to Application**. Ensure that the Application Pool is set to the one called TMS. Click **OK**
15. In the virtual directory select the Setup Subfolder, right-click the new virtual directory and select **Convert to Application**. Ensure that the Application Pool is set to the one called TMS. Click **OK**
16. In the virtual directory select the Worker Subfolder, right-click the new virtual directory and select **Convert to Application**. Set the Application Pool to the one called TMSWorker. Click **OK**
17. Select your TMS virtual directory, double click **Authentication** in the features pane and make sure that only *Anonymous Authentication* is set to **Enabled**. Everything else should be set to disabled.



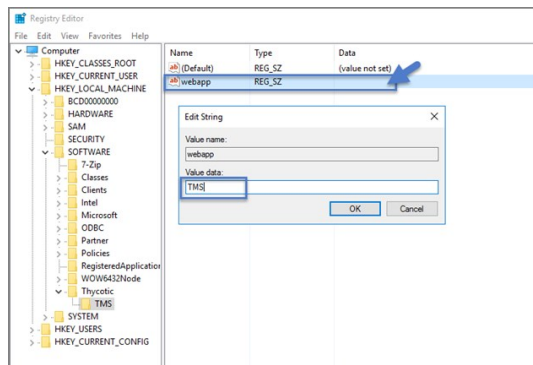
18. Select the Setup directory, double click **Authentication** in the features pane and make sure that Anonymous Authentication and Windows Authentication are both set to **Enabled** and everything else is disabled.



19. Select the Worker, double click **Authentication** in the features pane and make sure that Anonymous Authentication and Windows Authentication are both set to **Enabled** and everything else is disabled.
20. In **Regedit.exe**, create a new Registry key (HKEY_LOCAL_MACHINE) right-click on **Software | New | Key**, name the new key Thycotic. Next right-click on **Thycotic | New | Key**, name the new key TMS.



1. Create a new string value in the TMS folder right-click **TMS | New | String Value** with a name of webapp and a value of TMS (double click to assign value)



2. Create a 2nd new string value with a name of website and a value of the url to the root of the site you will be using (ex: "testlab" for a website of https://testlab/TMS)
 3. Create a new string value with a name of Webdir and a value of the path you put your Privilege Manager files in (i.e. C:\inetpub\wwwroot\TMS)
21. Ensure that the Privilege Manager folder has the proper permissions by checking that the account running the application pool in IIS has Modify permissions on the folder where Privilege Manager is installed. (i.e. C:\inetpub\wwwroot\ right-click **TMS | Properties | Security** tab, if the service account created in [Using a Service Account to run the IIS App pool](#) is not listed, Edit... | Add... | find account via Check Names | **OK**. Click on the account, check **Modify | Apply**.)
22. If your server does not have internet access you will need to ensure that your **solutionCenter** is configured for the directory that you deposited the nupkg files into.

1. Go to the directory where you have installed the TMS site (i.e. C:\inetpub\wwwroot\TMS)
2. Open the **web.config** file with Notepad and find the line
`<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com" /`
3. Replace the value with the directory from step 1 (usually c:\ProgramData\NuGetCache). Save changes.

```
<add key="almah.mvc.requiresauthentication" value="false" />
<add key="almah.mvc.allowedRoles" value="" />
<add key="almah.mvc.routes" value="almah" />
<!--
<add key="nuget:source:DevSolutionCentre" value="http://localhost/TesDevNuGet/NuGet/" />
<add key="nuget:source:SolutionCentre" value="http://nuget-dev.ds.arelila.com/NuGet/" />
key="nuget:source:SolutionCentre" value="C:\ProgramData\NuGetCache" />
-->
<add key="nuget:source:SolutionCentre" value="C:\ProgramData\NuGetCache" />
</appSettings>
<connectionStrings configSource="ConnectionStrings.config" />
<system.web>
```

Note: Make sure if using a local path to include the final slash.

Privilege Manager is now ready to be configured. Continue with [Completing Privilege Manager Installation from Website](#).

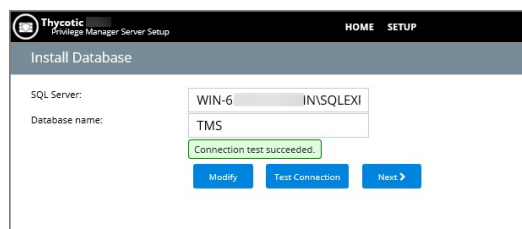
Installing as a Website

1. In IIS, right-click **Sites** and select **Add Website...**
2. Enter a Site name.
3. Click **Select...** and choose the application pool you created in the Manual Installation section from the drop-down menu. Click **OK**
4. Click the **...** beside the Physical path field and select the directory containing the unzipped Privilege Manager files (for example, C:\inetpub\wwwroot\TMS). Click **OK**
5. At the bottom of the Add Website window click **OK** to save your settings.

Completing Privilege Manager Installation from Website

Privilege Manager is now ready to complete installation. Open a browser and navigate to where your Privilege Manager Setup is located, for example: https://localhost/TMS/Setup. It will request windows credentials which must be the credentials for a local administrator on the web server.

The site will detect that it does not have the proper database configuration and walk you through installing the initial database objects.



After this initial step you will be presented with a list of Privilege Manager features you can choose to install.

1. Select **Add/Remove Product Features**
2. Select Application Control and Privilege Manager. This will automatically also select any prerequisites they require.
 Each feature is delivered as a NuGet Package, the package will unzip, add files to the Privilege Manger website, and update the database with its required objects. Installing the database and features may take several minutes.
3. Click **Show Install Log** to reveal installation progress.

Once all features have been installed Privilege Manager is ready to use! Refer to the [Getting Started](#) section for setup and configuration advice.

Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

With version 10.5 and up, encryption of items no longer requires app pool permissions on the machine's certificate store.

What this means for Privilege Manager

New installations of Privilege Manager will no longer require that the application pool user has to have permission to access the certificate stores. Previously this permission was required in order to encrypt and decrypt items in the database.

Existing installs of Privilege Manager (10.4 and earlier) should not remove this permission and should not remove old certificates as they will still need them to decrypt old items which predate this change. Both the web setup page and the installers will create a local **encryption.config** file in the TMS directory to hold the keys to the key stored in the database. This file is highly sensitive and should be regarded with caution.

Agents are required on endpoint machines to carry out policies created in Privilege Manager. This section offers direct downloads and descriptions for all available agents.

Thycotic Agents can be deployed in various ways, via:

- software management systems,
- GPO,
- cloned (gold) images, and
- manually.

Instructions and links for agent installers are provided in this article, grouped as follows:

- [Bundled Agent Installer - Windows](#)
- Individual Agent Installers for Privilege Manager:
 - [64-bit Windows Operating Systems](#)
 - [32-bit Windows Operating Systems](#)
- [macOS X Installer - 10.11 or Newer](#)

For details about Thycotic Agent System Requirements, see our [Agent System Requirements](#).

In version 10.5 and up, installation codes are required upon initial install to prove to the server that an agent install is authorized. Once an agent is installed, it deletes the install code and authenticates to the server via a certificate. See Agent Trust Revocation for certificate revocation.

The agent uses the install code to prove to the server that it is an authorized install. Once the agent is installed, the install code is deleted and the agent certificate is used to communicate with the server. The server needs either an install code or agent trust (a certificate) to accept communication from an agent. Multiple install codes can be created for bundling with different installers, if the last install code is revoked, a new one is generated automatically. Revoking an install code prevents new installations with that install code but does not affect previous installations since those agents now use their own certificates to authenticate.

1. Navigate to the agent settings under **Admin | Agents**.
2. On the Installation Codes tab you may Generate New codes, Refresh code information, Revoke, or Copy Codes to the clipboard to use in the installer.

Agents

IMPORTANT: Prior to installing agents, please ensure the necessary AV exclusions are in place [KB Article](#).

For agent setup instructions and specific installation files review this [KB article](#).

Summary Agent Reports Windows Agent Configuration MacOS Agent Configuration Installation Codes

Installation Codes

These install codes are used when an agent is installed and first registered with Privilege Manager. Revoking an install code will prevent new agent installations from connecting to the server for initial registration and can be useful if the install code is lost or stolen. Revocation will not affect existing installed agents. If you need to revoke an existing agent, use the [resource explorer](#) to browse agents and click the one you wish to revoke or search for the computer name and click the resource you wish to revoke. The individual item will contain a button to revoke agent trust of that specific resource. It will no longer be able to communicate with the server until it is installed with a valid install code.

Installation Codes

Generate New
Refresh

Code	Created	Action
10H7-12TF-7HVZ	Jan 23, 2019, 3:43:05 PM	Copy Revoke

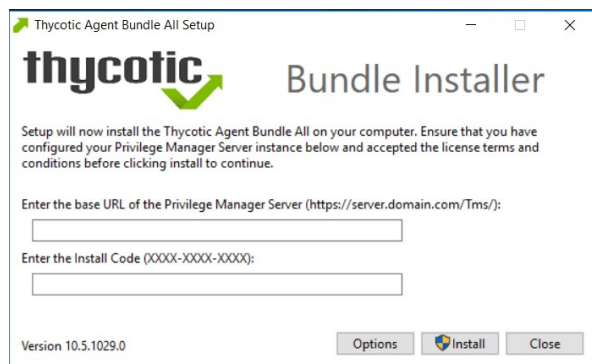
If deploying with msisexec, the following command shows an example for how to set the Install Code:

```
msiexec.exe /i ThycoticTmsSetup_x64.msi INSTALLCODE=1234XXXXABCD AMSURL=https://DOMAINName/
```

Where:

- ThycoticTmsSetup_x64 is the install file used.
- INSTALLCODE is argument taking the install code value.
- AMSURL is the argument taking the base URL to the TMS installation.

If installing via a bundled installer, the install code is placed in the **Enter the Install Code** field (dashes in the install code are for readability and are optional).



You can install the agent without an install code, but it will be unable to register with the server. To add an install code after the install, either run the bundled installer again or use the **SetAmsServer.ps1** script in `c:\program files\thycotic\powershell\arellia.agent`.

The **SetAmsServer.ps1** script will ask for the server and a valid install code.

If older agents are used, the **Prevent Legacy Agent Registration (10.4 and older)** option might be checked under ADMIN | Configuration and the Advanced tab, which prevents older agents without install code from registering.

If an agent was previously installed and never revoked, the endpoint will still have a valid certificate and a new agent can be installed with post-install registration.

For agents in an environment with a moderate policy configuration, the requirements for memory and disk space are as follows:

- Memory usage: 50Mb
- Disk usage:
 - Thycotic base agent: 10MB
 - Application Control Solution: 9MB
 - Local Security Solution: 3MB
 - Security Analysis Solution: 13 MB
- Average CPU over a week: 3%
- Impact to boot time: Negligible

Supported Windows Operating Systems (both 32- and 64-bit):

- Desktops: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10
- Servers: Windows Server 2008 R2 and newer
- Disable the GPO security option "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing."

Windows Management Framework download locations

Windows Management Framework 2.0 or newer

- Installed on Windows 7 and Windows Server 2008 R2 by default
- PowerShell 3.0 is installed on Windows 8 and Windows Server 2012 by default
- Older operating systems require installation

Windows XP	http://download.microsoft.com/download/E/C/E/ECE99583-2003-455D-B681-68DB610B44A4/WindowsXP-KB968930-x86-FNG.exe
Windows Server 2008 (x86)	http://download.microsoft.com/download/F/9/E/F9EF6ACB-2BA8-4845-9C10-85FC4A69B207/Windows6.0-KB968930-x86.msu
Windows Server 2008 (x64)	http://download.microsoft.com/download/2/8/6/28686477-3242-4E96-9009-30B16BED89AF/Windows6.0-KB968930-x64.msu

.NET 4.0 Framework or newer

Windows 8 and newer and Windows Server 2012 and newer have 4.5 installed by default.

To download it, go to <http://www.microsoft.com/en-us/download/details.aspx?id=24872>.

.NET 2.0 Framework SP1

The .Net 2.0 SP1 update is required only for Windows XP. To download, go to http://download.microsoft.com/download/c/6/e/c6e88215-0178-4c6c-b5f3-158ff77b1f38/NetFx20SP2_x86.exe.

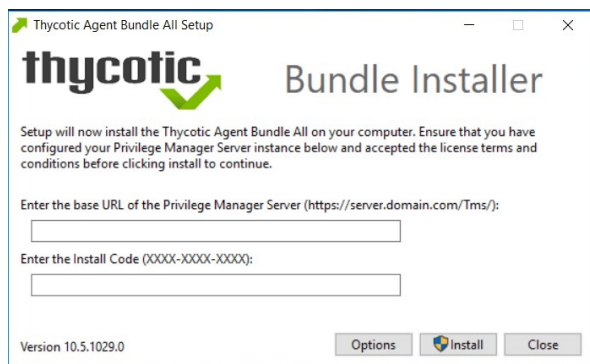
The bundled EXE installer is recommended when installing Privilege Manager on machines one at a time, for deployments through software delivery see the next section. This installer includes all Privilege Manager Agents for Windows machines (Core, ACS, LSS). You can use the bundled installer directly on individual endpoints for testing or for production environments in either 32-bit or 64-bit environments.

Important: To ensure you have installed all prerequisite software on your managed computers **before** you install the Thycotic agents, please see our [System Requirements for Privilege Manager](#)

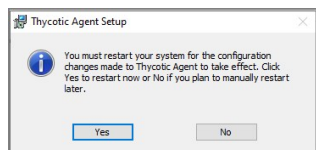
To install Thycotic agents **on a single testing machine**, follow these steps:

1. Download the [Bundled Agent Installer - Windows](#).
2. Run the Thycotic Bundled Installer on the computer you want to manage.
3. During the setup process, enter the Privilege Manager Server URL (or AZ Service Bus Queue URL) and the [Install Code](#) when prompted.

Note: The Install Code field can be left blank when using versions lower than 10.5.



4. After the installation you will be prompted to restart your endpoint.



Note: It may take 15-30 minutes for agents to receive new policies, to speed this up navigate to **Admin | Configuration | General** and click **Run Policy Targeting Update**, then open the Agent Utility on the endpoint and click the **Register** button.

Note: The bundled installer does require a restart in order to ensure the agent is completely ready to use.

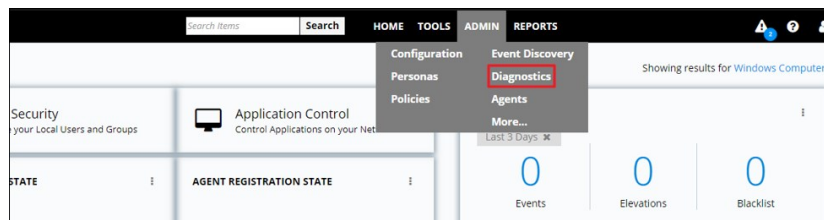
Rollout to Multiple Systems

To install Thycotic agents **on multiple machines**, we recommend the following:

1. Download the [Agent standalone.MSI](#) files based on specific systems.
2. Push them out through any software delivery system tool (e.g.: SCCM) using the recommended command lines.

Agent Diagnostics

Once your agents are installed, verify that they have registered in Privilege Manager. Navigate to the **ADMIN | Diagnostics** page from the Dashboard, or **ADMIN | Agents** to view your agent details.



After the initial policies are received, future updates will be based on the task schedules set in Update Applicable Policies and Scheduled Registration policies. Ensure to select the correct policies based on Windows or Mac operating systems. To edit these schedules, navigate to **Admin | Policies | General** tab, click the desired task, click the **Triggers** tab, and then **Edit**.

Diagnostics

This page shows you general diagnostics about your environment that can be used to troubleshoot issues or submit to Technical Support.

Managed Operating Systems

Windows Server 2012 R2 1

Key Configuration Settings

- Unconfigured - Warning Set Default User Credential
- Properly Configured Product Licenses Installed
- Unconfigured - Warning Configure Active Directory
- Properly Configured Install Agents
- Normal Upgrade Available
- Normal Server Activity Paused

Agent Registration State

Agent Policy State

System Health

- Normal Remote Task Status
- Normal Number of Old Computers
- Normal Unacknowledged Events
- Normal Pending Approvals Count
- Normal Number of Application Events
- Normal File Uploads Size

On the Diagnostics page you will see the quantity of agents registered and what operating system is running on registered endpoints. Registered endpoints can also be viewed in the report (run from the **REPORTS** menu selection) **Agent Installation Summary** or by navigating to the **Admin | Agents | Agent Reports** tab.

Reports

Select Report Options

Actions

- Application Control Event Summary
Lists Application Control Event Summaries
- Summary of Application Actions by Computer
- Summary of Application Actions by Operating System
- Summary of Application Actions by Product Version
- Application Control Event Summary Acknowledgements
Lists Application Control Event Summary Acknowledgements
- Summary of Application Actions by Mac Executable
- Summary of Application Actions by Product Name
- Summary of Application Actions by Win32 Executable

Agent

- Agent Installation Summary**
Lists computers with the Application Control Agent or File Inventory Agent installed, along with the version of the agent and client operating system and service pack level. The results can be filtered by the Agent Version or Operating System on the client computer.
- Agent Summary by OS
List of Operating Systems discovered with or without the agent installed.
- Managed Operating Systems
List of operating systems with the count of managed computers running them.
- Agent Installations
Lists computers and their installed agent information.
- Computers Without Agent Installations
Lists computers without the given agent or without the given agent version.

Approvals

- Pending Execute Application Approvals
- Summary of Application Approval Requests by Approver
Summary of Approvals

Resource Explorer > WIN-10-10-10-10-10-10

Summary

Known Data

Events

Associations

Name: WIN-10-10-10-10-10-10

Created: Jan 14, 2018 9:54:24 AM

Modified: Jun 20, 2018 8:38:17 AM

Monitor Resource

Health

- Normal Policy State
- Normal Registration State
- Managed Managed or Unmanaged State

Back Revoke Agent Trust Delete

Policies on Endpoint License Reservations Task History Computer Group Membership

Drag column here for grouping

POLICY NAME	HAS A VERSION OF THE POLICY	HAS CURRENT VERSION OF THE POLI...	POLICY LAST MODIFIED	POLICY APPLIED TO AGENT
Application Control Agent Configuration Policy (Windows)	True	True	6/20/18 8:37 AM	6/14/18 8:38 AM
Basic Inventory (Windows)	True	True	6/20/18 8:38 AM	6/14/18 8:38 AM

From the **Agent Installation Summary** report you can click into any of the **target machines** listed that have a Thycotic agent installed. Pictured above is a view from one of these resource pages where you can check the machine's System Health and configured policies.

Note: If you find that you've entered the wrong Privilege Manager Server address or want to change this settings, refer to the information under [Setting the Privilege Manager Server Address](#).

Use the links below to download the agent installation software for Windows based endpoints.

There are three agents available for Windows endpoints:

- **Thycotic Agent:** The core agent is responsible for all reporting and monitoring communication on the endpoint. It can be considered the managing agent, while the Application Control and Local Security Agents are the worker agents.
- **Application Control Agent (ACS):** This agent is responsible for monitoring processes executing the Privilege Manager Application Control Functions on the endpoint.
- **Local Security Agent (LSS):** This agent is responsible for monitoring and executing Local Security functions.

Individual Agent Installers for Privilege Manager

Hardened Agents

If agent hardening was applied to user endpoints, the hardened agents need to be deleted via the `sc delete (agent name)` commandline command. This needs to be done under the context of the domain user prior to running the msi-based agent installation commands. When the agent is deleted successfully, a success message will be returned, for example:

```
C:\>sc delete arelliaagent
[SC] DeleteService SUCCESS
C:\>sc delete arelliaacsvc
[SC] DeleteService SUCCESS
```

Note: If the hardened agents are being deleted via software delivery script, the script needs to be delivered under the context of the domain user.

64-bit Windows Operating Systems

Individual Windows agents are available in MSI format for easier bulk-rollout through software delivery tools. For installing individual agents, begin with the Core Thycotic Agent:

- **Core Thycotic Agent (x64):** https://tmsnuget.thycotic.com/software/Agents/ThycoticAgent_x64_10_7_2266.msi
- **Application Control Agent (x64):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_ApplicationControlAgent_x64_10_7_2257.msi
- **Local Security Solution Agent (x64):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_LocalSecurityAgent_x64_10_7_2219.msi

Installation Command Lines

Note: The Install Code field can be left blank when using versions lower than 10.5

- **Core Thycotic Agent**

```
msiexec.exe /i "ThycoticAgent_x64_10_7_2266.msi" /norestart AMSURL=https://SERVERNAME/TMS/ INSTALLCODE=XXXX1234ABCD REBOOT=ReallySuppress /qn
```

- **Application Control Agent**

```
msiexec.exe /i "Thycotic_ApplicationControlAgent_x64_10_7_2257.msi" /norestart REBOOT=ReallySuppress /qn
```

- **Local Security Agent**

```
msiexec.exe /i "Thycotic_LocalSecurityAgent_x64_10_7_2219.msi" /norestart REBOOT=ReallySuppress /qn
```

32-bit Windows Operating Systems

Individual Windows agents are available in MSI format for easier bulk-rollout through software delivery tools. For installing individual agents, begin with the Core Thycotic Agent:

- **Core Thycotic Agent (x86):** https://tmsnuget.thycotic.com/software/Agents/ThycoticAgent_x86_10_7_2266.msi
- **Application Control Agent (x86):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_ApplicationControlAgent_x86_10_7_2257.msi
- **Local Security Solution Agent (x86):** https://tmsnuget.thycotic.com/software/Agents/Thycotic_LocalSecurityAgent_x86_10_7_2219.msi

Installation Command Lines

Note: The Install Code field can be left blank when using versions lower than 10.5

- **Core Thycotic Agent**

```
msiexec.exe /i "ThycoticAgent_x86_10_7_2266.msi" /norestart AMSURL=https://SERVERNAME/TMS/ INSTALLCODE=XXXX1234ABCD REBOOT=ReallySuppress /qn
```

- **Application Control Agent**

```
msiexec.exe /i "Thycotic_ApplicationControlAgent_x86_10_7_2257.msi" /norestart REBOOT=ReallySuppress /qn
```

- **Local Security Agent**

```
msiexec.exe /i "Thycotic_LocalSecurityAgent_x86_10_7_2219.msi" /norestart REBOOT=ReallySuppress /qn
```

The Bundled Mac Agent DMG + PKG installer is available for macOS systems. You can use this installer directly on individual endpoints for testing or for production environments.

Installing macOS Agents

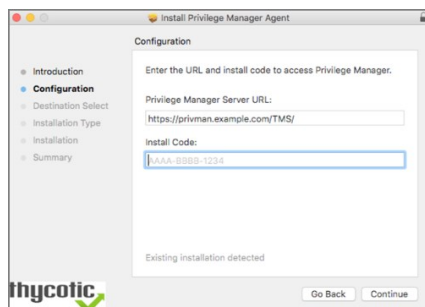
Note: If you enter the wrong install code or you need to update an install code for whatever reason, rerun the package installer to provide the correct/new install code. The Install Code field can be left blank when using versions lower than 10.5.

Directly

The Bundled macOS Agent is a DMG + PKG file. You can use this Mac agent installer directly on individual endpoints for testing or production environments.

To install the agent software on a single testing machine, follow these steps:

1. Go to [Agent Downloads](#) and download the Privilege Manager Mac Agent.
2. Run the Bundled Mac Agent DMG + PKG Installer on the computer you want to manage.
3. During the setup process,
 1. enter the base URL and
 2. the Install Code when prompted.



Note: The bundled installer does require a restart in order to ensure the agent is ready to use.

Using an Unattended Install Method

Begin by downloading the DMG + PKG package (See link for Privilege Manager Mac Agent listed above) on one of your Mac endpoints. Run the installer by double clicking the PKG file.

After installing this first agent, navigate to `/Library/Application Support/Thycotic/Agent/agentconfig.json`. The `agentconfig.json` file stores information such as your organization's URL and a few other custom settings like 'Task Polling Interval,' etc.

Open the file and add the "installCode" parameter after the "tmsBaseUrl" to that file as shown in the following code sample:

```
{
  "tmsBaseUrl": "https://servername/Tms",
  "installCode": "VALUEHERE"
}
```

There are two methods for deploying your remaining Mac agents in an unattended fashion:

- Network File Share
- Distribution Tool

Network File Share

If you want administrators to deploy agents onto individual macOS endpoints, save the PKG installer from the DMG side-by-side with the `agentconfig.json` file in a network share folder.

Due to new macOS security enhancements, users cannot run a PKG installer from a network share anymore. The administrator must then run the installer command-line tool from **Terminal.app** after mounting and cd'ing to the directory containing the PKG installer and `agentconfig.json` file:

```
cd /Volumes/<network share>/<path to PKG installers>
sudo installer -pkg ThycoticManagementAgent-10.7.30.pkg -target /
```

The PKG will first look for an `agentconfig.json` file located in the same folder. When it finds this file, it will copy `agentconfig.json` into the `/Library/Application Support/Thycotic/Agent` folder during the unattended install on the Mac endpoint where the installer is running.

Distribution Tool

Using a Deployment Tool like Jamf or SCCM, include both the PKG installer and the `agentconfig.json` files in the distribution package together, then deploy the package onto your endpoint Macs by running a script using a tool or remotely by using ssh to install the PKG, for example:

```
sudo installer -pkg ThycoticManagementAgent.10.7.30.pkg -target /
```

As in the example using a Network Share, the PKG will first look for an `agentconfig.json` file located in the same folder. When it finds this file, it will copy `agentconfig.json` into the `/Library/Application Support/Thycotic/Agent` folder during the unattended install on the endpoint Mac where the installer is running.

For more instructions on how to deploy in bulk using Microsoft Software System Center Configuration Manager (SCCM), Microsoft instructions for Macs are described [here](#).

After Initial Deployment

If the Mac already has an existing `agentconfig.json` file, it will NOT be overwritten because creating a file only occurs if the computer didn't already have an `agentconfig.json` installed. This means you can use the same distribution package for upgrades and new installs.

Note: It will take 15-30 minutes for newly installed agents to register in Privilege Manager. See the agent registration information in the [Terminal Commands](#) topic to speed the process up.

Uninstalling an Agent

When you need to uninstall the macOS Agent, use the **Uninstall.sh** shell command:

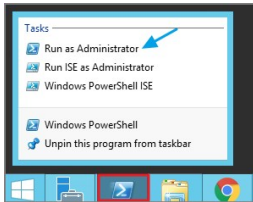
```
sudo /Volumes/ThycoticManagementAgent-10.7.30/Uninstall.sh
```

This topic explains how to uninstall the Agent through command line. If you're trying to uninstall an old agent in order to install a newer version of the agent, there is no need to do so. The installers will detect a previous version installed and uninstall the old version prior to installing the new agent.

Note: For hardened agents refer to information under [Windows Agents](#).

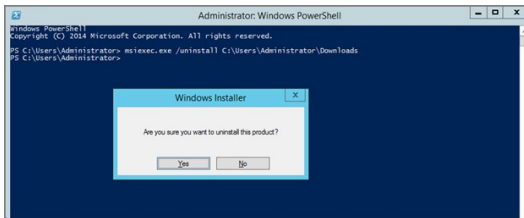
Manual Uninstall Steps

1. Navigate to the machine(s) where the agent is located.
2. Right-click on Windows Powershell and select **Run as Administrator**.



3. Run the following command:
`msiexec.exe /uninstall <path to the msi installer>\ThycoticAgent_x64_10_5_1029.msi`

4. Select **Yes** on the Windows Installer prompt.



Privilege Manager software updates are made available via NuGet server packages. The upgrade process can be performed via **Add/Upgrade Features** link in the Privilege Manager Setup page.

Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Setting up the NuGet Source

Once Privilege Manager is installed on a server, updates can be performed by pointing the web.config file to the product NuGet source.

1. Navigate to C:\inetpub\wwwroot\TMS\ and right-click the web.config file.
2. Select Edit from the drop-down.
3. Verify the following line with correct NuGet source is present:

```
<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" />
```

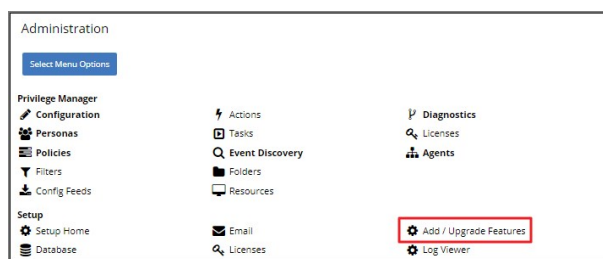
Updating Privilege Manager

Important: Always make a backup of the Privilege Manager Database in SQL and the TMS web files before performing upgrades in a production environment. The default location of the web files on the Privilege Manager Server C:\inetpub\wwwroot\TMS.

In environments with multiple Privilege Manager Server nodes, stop the TMS application pools on all secondary nodes before starting the upgrade. Restart the applications pools once the upgrade is completed.

Primary Node

1. Navigate to **Admin | More...** and select the **Add / Upgrade Features** link.



2. If you are not a local Administrator on the server, you might see a warning that adding or upgrading features requires administrative access. Based on your account role membership either click **Continue to Add / Upgrade Privilege Manager Features** or **Cancel** if your role permissions don't meet the requirement.
3. The Currently Installed Products page displays a table listing all the products by name in alphabetical order.

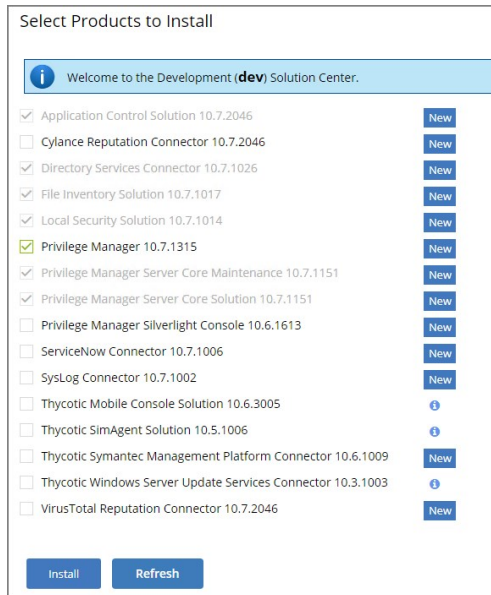
Product Name	Installed	Available	Published	
Application Control Solution	10.7.2045	10.7.2046 New	9/16/2019 12:01 PM	Upgrade
Cylance Reputation Connector	10.6.1093	10.7.2046 New	9/16/2019 12:01 PM	Upgrade
Directory Services Connector	10.7.1024	10.7.1026 New	9/16/2019 12:01 PM	Upgrade
File Inventory Solution	10.7.1016	10.7.1017 New	9/16/2019 12:01 PM	Upgrade
Local Security Solution	10.7.1013	10.7.1014 New	9/16/2019 12:01 PM	Upgrade
Privilege Manager	10.7.1313	10.7.1315 New	9/16/2019 12:01 PM	Upgrade
Privilege Manager Server Core Maintenance	10.7.1149	10.7.1151 New	9/16/2019 12:01 PM	Upgrade
Privilege Manager Server Core Solution	10.7.1149	10.7.1151 New	9/16/2019 12:01 PM	Upgrade
Privilege Manager Silverlight Console	10.6.1160	10.6.1613 New	8/21/2019 4:36 PM	Upgrade
ServiceNow Connector	10.6.1017	10.7.1006 New	8/21/2019 4:36 PM	Upgrade
SysLog Connector	10.6.1020	10.7.1002 New	8/21/2019 4:38 PM	Upgrade
System Center Configuration Manager Connector	10.6.1003	10.6.1003	5/31/2019 12:40 PM	Repair
Thycotic Symantec Management Platform Connector	10.6.1003	10.6.1009 New	8/21/2019 4:37 PM	Upgrade
VirusTotal Reputation Connector	10.6.1093	10.7.2046 New	9/16/2019 12:01 PM	Upgrade

[Install/Upgrade Products](#) [Refresh](#)

Activate Windows
 Go to Settings to activate W

Use either of the following ways to upgrade your environment to the latest Privilege Manager version:

1. Click Upgrade next to individual packages, this will require to come back to the Installed Products page after each separate upgrade for most of the packages, or
2. Click Install/Upgrade Products at the bottom of the page.
 1. Select the products you want to install/upgrade.

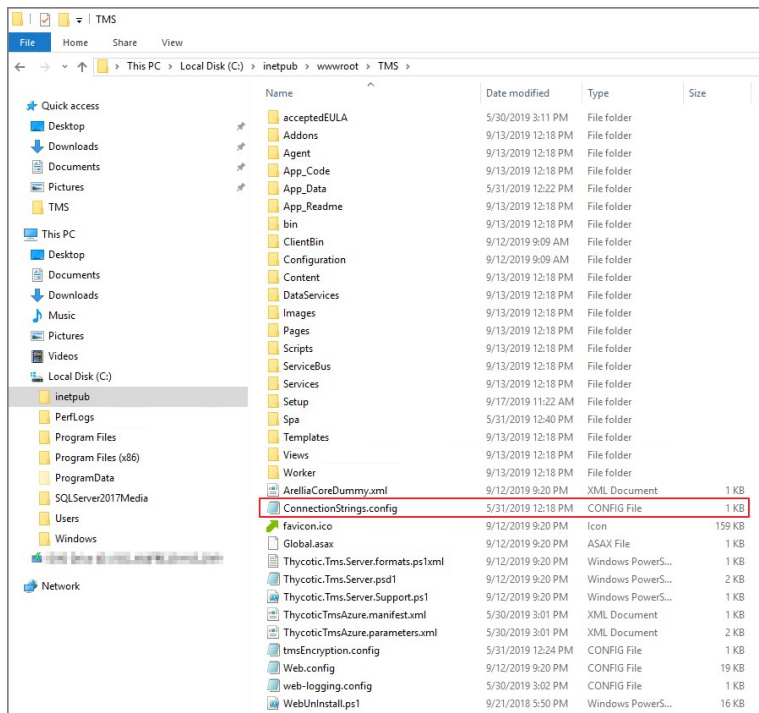


2. Select Install.

The installation/upgrade process starts and you can view the log while products are being installed.

Secondary Nodes

1. On the upgraded primary node navigate to TMS web files. The default location is: C:\inetpub\wwwroot\TMS.
2. Copy the TMS folder, except for the ConnectionStrings.config file.



3. On your secondary node navigate to the same folder location, most likely C:\inetpub\wwwroot\TMS and paste the copied files.
4. Repeat this the copy and paste for all other secondary Privilege Manager nodes in your environment.
5. Navigate to the IIS Manager and start all TMS Application pools on the secondary nodes.

Follow these steps to perform an offline upgrade for Privilege Manager. This article is ONLY applicable when upgrading from versions 10.2 and higher.

1. Go to <https://thycotic.force.com/support/s/download-onprem>
2. Download the Privilege Manager Application Files (not the Installer .exe); this will download a .zip, for example Version_10_7_000000.zip
3. Extract the zip file.
4. From the unzipped folder, copy the contents of the nugetCache folder to this location on the web server: C:\ProgramData\NugetCache
5. On the web server, go to the TMS folder (default install locations include C:\inetpub\wwwroot\TMS or C:\inetpub\wwwroot\SecretServer\TMS)
6. Open the web.config in your favorite file editing tool, for example Notepad.
7. Find the following line:

```
<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget" />
```

8. Edit this line to change the path to C:\ProgramData\NugetCache\

```
<add key="nuget:source:SolutionCentre" value="C:\ProgramData\NugetCache\" />
```

9. Save the web.config
10. Recycle the TMS app pools.
11. Navigate to **ADMIN | More...** and select **Add / Upgrade Privilege Manager Features**. This step will require windows authentication using an account that has local administrator permissions on the web server. The page should have a blue dialogue box stating:

"You are viewing a local (cached) repository of product options. For an up-to-date list of products available, switch to the online repository"

Also, the version numbers available should match the highest versions available in the C:\ProgramData\NugetCache\ folder on the web server.

Note: Do NOT select the link to "...switch to the online repository", unless you want to revert the changes made above. Selecting this will edit the web.config back to the original SolutionCentre web path.

An upgrade or repair to the product may rewrite the web.config with default settings. Always double-check that the web.config has the correct SolutionCentre path whenever you perform a manual upgrade.

Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Follow these steps to perform an offline upgrade for Privilege Manager and Secret Server. This article is ONLY applicable when upgrading from products that are versions 10.2 and higher.

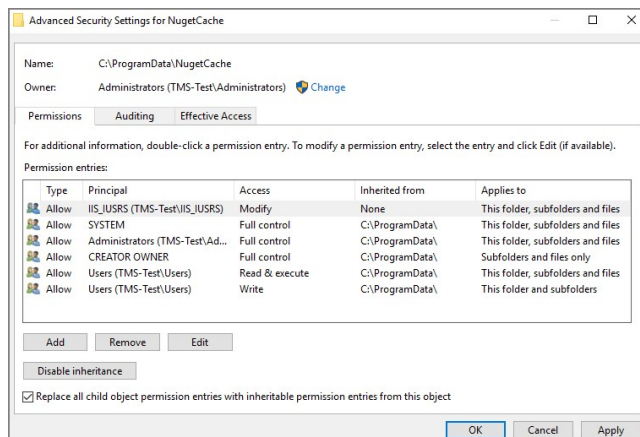
1. Download the zip files for your offline upgrade [here](#). Copy/paste this zip file on your Privilege Manager Web server
2. Make a backup of the Secret Server and TMS web folders (Default path is C:\inetpub\wwwroot> SecretServer + TMS folders, copy/paste these into a backup folder)
3. Make a backup of the Database (In Secret Server navigate to Admin | Backup | Backup Now button)
4. On the web server, navigate to C:\ProgramData\NuGetCache\ and delete all the files in the folder (*ProgramData folder may be hidden: View > check the Hidden items box to reveal)
5. Open Secret Server and navigate to: <https://<YourSecretServerURL>/Setup/Upgrade>
6. On the Secret Server Update page:

1. Select "Advanced (not required)" to open the advanced options
2. Select "Choose File" and navigate to the location of the Secret Server Update zip package
3. Select "Upload Upgrade File"
4. When the new version is available select "Upgrade"

Check <https://URL/TMS/Setup> to see if an install is already in progress (this is usually seen when the TMS Upgrade portion of SS shows successful)

7. Accept the License. Then allow the Secret Server upgrade to complete. Note: The Upgrade TMS step may say it was successful, or it may say it wasn't. Please ignore this message and continue to follow the steps below:
8. Open the C:\ProgramData\ folder:

1. Right click on the NuGetCache folder and select Properties
2. Click on the Security tab
3. Click the Advanced button
4. Check the Replace all child object permission entries with inheritable permission entries from this object checkbox



5. Click the OK button, and Yes.
9. Navigate to <https://<webserver>/TMS/Setup/ProductOptions/ShowProducts> Note: The TMS setup page requires authentication with a Windows account that is a Local Administrator of the Web Server
10. You may see a page that looks like the image below. If so, click the Use Local (Cached) Product Options Button
11. IMPORTANT: Do not ignore this step, even if you see the list of products:
 1. Open the web.config file in the TMS web folder (C:\inetpub\wwwroot\TMS\ "Web" or "Web.config"), right click and open with Notepad, Run as Administrator
 2. Delete the line that says: `<add key="nuget:source:SolutionCentre" value="http://tmsnuget.thycotic.com/nuget/" />`
 3. Replace with your offline nugetCache directory file path. (For example: `<add key="nuget:source:SolutionCentre" value="C:\ProgramData\NuGetCache\"`)
 4. Save the web.config file
12. Refresh the page at <https://<webserver>/TMS/Setup/ProductOptions/ShowProducts>
13. Click the Install/Upgrade Products button.
14. Select the products you wish to upgrade or install, and follow the steps to finish the installation.

Note: If one of the products fails to install, please repeat steps 11 and 12. You may encounter an issue with an error of "Version Store out of Memory" - this is transient and re-starting the upgrade will fix it.

If you encounter any additional errors or the error from step 13 persists, please contact Thycotic Technical support for assistance by submitting a case here.

Note: Thycotic recommends to create a back-up copy of the Privilege Manager web application folder after installation or upgrades.

Upgrading from our 8.2 version to Privilege Manager 10.4 and up can't be done from <https://servername/Ams/Setup/>. To upgrade, we recommend using the same database and removing the old application before installing the new version. This can be done automatically or manually.

Automatic Steps

1. Download http://tmsnuget.thycotic.com/Software/ThycoticTmsinstaller_10_0_1570.exe and run it on the web server where your existing Arellia Management Server 8.x version is installed.
2. Follow the prompts.
3. Once it completes, you'll access the server at <https://servername/Tms/> instead of <https://servername/Ams/>.
4. Go to <https://servername/Tms/Setup> to install the latest 10.x version.
5. Open **IIS Manager** and go to **Sites | Ams | Agent | Uploads**.
6. Click on the **BITS Uploads** and change the notification URL from <http://localhost/Ams/Services/BitsUpload.ashx> to <http://localhost/Tms/Services/BitsUpload.ashx>.
7. Download and install the latest agents. Please refer to the agent installation section [the latest agent installation](#).

Note: Old agents will continue to work because of the redirect created during the install that sends traffic from <https://servername/Ams/Agent> to <https://servername/Tms/Agent>. When upgrading the agents, we recommend that you set the **AMSURL** to the new <https://servername/Tms/> address.

Manual Steps

1. Remove the AMS website from the web server.
2. Download the latest bundled installer <http://thycotic.com/products/secret-server/resources/download-secret-server/>.
3. Follow the prompts to install Privilege Manager, setting the database connection to the existing database.
4. Download and deploy the latest agents that are [available here](#).

Note: Set the AMSURL to the new server address, <https://servername/Tms/>

Legacy System Extensions

In 2019, Apple announced the deprecation of kernel extensions (KEXTS) in a future OS upgrade and that System Extensions should be used instead. Beginning in macOS 10.15.4, the use of kernel extensions will trigger a notification that software using this type of extension includes a deprecated API and an alternative should be provided by the vendor.

You may see this popup:



Thycotic plans to support Endpoint Security via system extension in Privilege Manager version 10.8 to be delivered this summer. In the meantime, Privilege Manager will continue to function normally and no immediate action is required.

You can read more about legacy system extensions on [Apple's website](#).

Privilege Manager will continue to support kernel extensions for macOS versions that require them for the product to function.

Privilege Manager Agents

The [Privilege Manager Agents](#) are a critical component of Thycotic's application control and local security, giving you the ability to evaluate the health and status of endpoints in real time. Agents are required on endpoint machines to implement Privilege Manager policies.

Privilege Manager provides pre-configured and fully customizable reporting on the status of agents and endpoint operating systems. In the Privilege Manager reporting dashboard, you can drill into reports based on any dimension and easily export report data to other reporting applications or Excel.

Privilege Manager supports agents on:

- Windows
- macOS

endpoint operating systems.

For information about installing agents, refer to [Agent Installation](#) to review agent system requirements and the specific agent installation procedures. This section of our document is a general agent information section, containing details about how to use/interact with agents and to provide information about the agent processes.

To make sure that local Administrators do not tamper with Thycotic agents running on their system, Privilege Manager Administrators can define users that can start and stop the Privilege Manager services running on endpoints, such as the Thycotic Agent or Thycotic Application Control. Refer to [Agent Hardening](#).

When your agents are installed, you can verify the status of your Agents' health in terms of Registration State and Policy State from the Home page. You also can navigate to **Admin | Agents** for more information about installed agents.

The Agent Health dials describe how many Managed Operating Systems you have as well as your Agent(s) Registration State and Policy State. If you click on the Agent Registration State dial, you will see a report on a list of machines (the "MonitoredResource" column) where each registered agent is installed.

Clicking the Agent Policy State dial from the Home dashboard brings you to a report that links all of your agent-registered machines with the Number of Policies Missing from each agent. This page will become invaluable once you have multiple policies running over different computer groups in your network.

Navigate to the **ADMIN | Diagnostics** page to view more comprehensive agent details. The Diagnostics page also is the go-to stop for full system health. Go here to find Server Console Logs and other system level warnings or tips.

The agent traffic is secured via SSL/TLS.

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents **independent** of the endpoint operating system.

The following topics are available:

- [Setting the Privilege Manager Server Address](#)
- [Connecting Agents to the Privilege Manager Server](#)
- [Agent Trust Revocation](#)
- [Uninstalling an Agent with Script](#)
- [How to prevent Backwards Compatibility for Agents v10.4 and earlier](#)
- [Configuring for a Test Environment](#)
- [Agent Tasks](#)

Agents require a Privilege Manager Server to communicate with. The recommended way to set the URL address is during the [installation of the Thycotic Agent](#). If an Azure Service Bus or Reverse Proxy is used, the URL can point at the URL of those components.

The URL address can be changed post-install via the registry or PowerShell.

Setting the Privilege Manager Server (TMS) Address via PowerShell

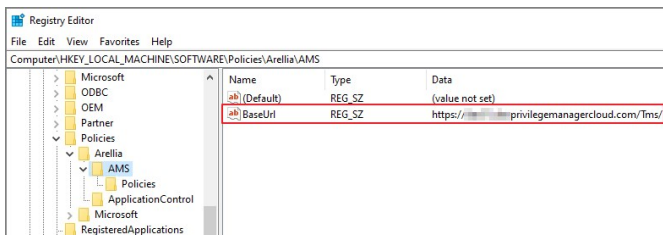
To set the Privilege Manager Server (TMS) address via PowerShell, run this command as Administrator:

```
C:\Program Files\Thycotic\Powershell\Arellia.Agent\SetAmsServer.ps1
```

The script will then ask you to type in the fully qualified domain name of the server.

Changing the Privilege Manager Server (TMS) Address via the Registry Editor

1. Open the Registry Editor (regedit)
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**
3. Right click BaseUrl and select Modify.

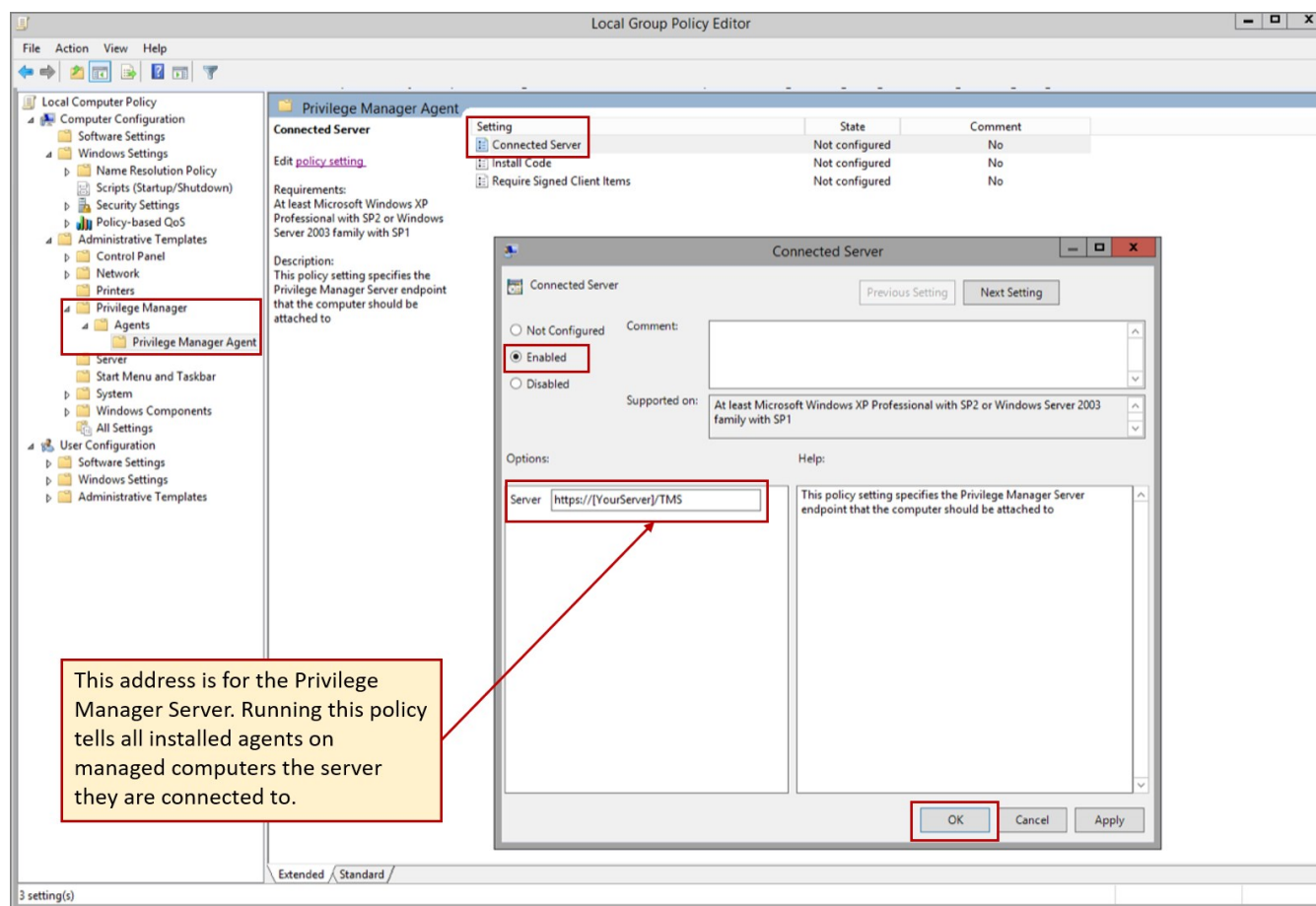


4. In the Edit String dialog box, change the BaseURL to your TMS Address.
5. Close the registry.
6. Restart the Agent service.

Regardless of how you installed agents or rolled agents out to your network, Privilege Manager has a method to link those agents with Servers. Privilege Manager has templates (files) that enable you to point agents back to the Privilege Manager Server.

To perform this task, do the following steps:

1. Download the attached [PrivilegeManagerAgent.admx](#) and [PrivilegeManagerAgent.adml](#) zip folders and extract the corresponding files (one file from each zip folder).
2. Install the downloaded and extracted custom Privilege Manager Group Policy files either on a single machine or on a domain controller.
 - o To install on a single machine:
 1. Copy PrivilegeManagerAgent.admx to %systemroot%\PolicyDefinitions
 2. Copy PrivilegeManagerAgent.adml to %systemroot%\PolicyDefinitions\en-US
 - o To install on a Domain Controller effectively making the custom GPO available to all Domain Administrators:
 1. Copy PrivilegeManagerAgent.admx to %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions
 2. Copy PrivilegeManagerAgent.adml to %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions\en-US
3. From the Group Policy Management Editor, navigate to Policies.
4. Go to Administrative Templates > Privilege Manager > Agents > Privilege Manager Agent and click Connected Server.



5. In the Connected Server window click **Enabled**.
6. In the Server field, **enter** the **URL** for your Privilege Manager Server, click **OK**.
7. Now you need to copy some data from Privilege Manager. In Privilege Manager, navigate to **Admin | Agents | Installation Codes** tab.

Thycotic Agents

For agent setup instructions and specific installation files review this [KB article](#).

Summary

Agent Reports

Windows Agent Configuration

MacOS Agent Configuration

Installation Codes

Installation Codes

These install codes are used when an agent is installed and *first* registered with Privilege Manager. Revoking an install code will prevent new agent installations from connecting to the server for initial registration and can be useful if the install code is lost or stolen. Revocation will not affect existing installed agents. If you need to revoke an existing agent, use the [resource explorer](#) to browse agents and click the one you wish to revoke or search for the computer name and click the resource you wish to revoke. The individual item will contain a button to revoke agent trust of that specific resource. It will no longer be able to communicate with the server until it is installed with a valid install code.

Installation Codes

Generate New

Refresh

Code

TVU0-VYGV-9CL2

Created

Aug 28, 2018, 4:34:46 PM

Action

Copy

Revoke

8. Copy the Code value found in the Installation Codes tab by clicking on Copy.

9. Switch back to the Group Policy Editor, in the Privilege Manager Agent window, click Install Code.

The code to be entered here should be copied from Privilege Manager:
Admin > Agents > "Installation Codes" tab

1. In the Install Code window, click Enabled.
2. In the Install Code field, paste the Code value you copied from Installation Codes tab in Privilege Manager.
3. Click OK.

10. Set the Client Item Signature Validation. By default, Privilege Manager validates only client items that have a signature present. If you want to require that all client items have a valid signature, then configure the group policy settings to enforce the **Require Signed Client Items** setting.

Un-Installing Old Templates

If you had previously downloaded and installed files which had the names "AMSAgent.admx" and "AMSAgent.adml", these should be removed. Do so as follows:

- To un-install from a single machine:
 1. Delete AMSAgent.admx from %systemroot%\PolicyDefinitions
 2. Delete AMSAgent.adml from %systemroot%\PolicyDefinitions\en-US
- To un-install from a Domain Controller:
 1. Delete AMSAgent.admx from %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions
 2. Delete AMSAgent.adml from %systemroot%\SYSVOL\domain\Policies\PolicyDefinitions\en-US

With Privilege Manager 10.5 and up, you can revoke an agent trust relationship.

1. Look up a computer in Resource explorer. Navigate to **ADMIN | More | Resources | expand Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
2. Click one listed; OR search by resource name.
3. Click **Revoke Agent Trust**.

Resource Explorer > DEVQA-AA-1000009

Summary

Name
Created
Modified
Monitor Resource

Health

- Normal Policy State
- Warning Unmanaged Local Administrators by Computer
- Warning Registration State
- Managed Managed or Unmanaged State

Back Delete **Revoke Agent Trust**

Policies on Endpoint License Reservations Task History Computer Group Membership

Drag column here for grouping

POLICY NAME	HAS A VERSION OF THE POLICY	HAS CURRENT VERSION OF THE ...	POLICY LAST MODIFIED	POLICY APPLIED TO AGENT	AGENT LAST RECEIVED POLICIES
-------------	-----------------------------	--------------------------------	----------------------	-------------------------	------------------------------

Note: You must confirm by clicking the button again on the next screen. The message below reads:

Revoking this agent's trust will disallow this computer from registering and receiving policies. This process cannot be undone. To later re-establish trust between this computer, you will need to re-install the agent with the proper install code.

This does not uninstall the agent from the computer, it simply denies it from contacting this server. This process also does not delete this agent nor its data from this server. Use the 'Delete' button from the Resource Explorer view to remove the computer and its data from this server.

HOME TOOLS ADMIN REPORTS

Upgrade Available - There are 1 updates for Privilege Manager available.

Resource Explorer > THY-01-0121-LT

Revoke Agent Trust

Computer: THY-01-0121-LT

Revoking this agent's trust will disallow this computer from registering and receiving policies. This process cannot be undone. To later re-establish trust between this computer, you will need to re-install the agent with the proper install code.

This does not uninstall the agent from the computer, it simply denies it from contacting this server. This process also does not delete this agent nor data from this server. Use the 'Delete' button from the Resource Explorer view to remove the computer and its data from this server.

To continue, click 'Revoke Agent Trust'.

Back **Revoke Agent Trust**

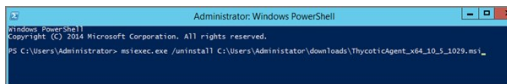
This topic covers uninstalling an agent when the endpoint is not going to be upgraded to a new version of Privilege Manager agents anymore.

If you're trying to uninstall an old agent in order to install a newer version of the agent, use the Upgrade Products/Feature link under the Setup page.

Using a PowerShell Script to Uninstall an Agent

1. Navigate to the machine(s) where the agent is located.
2. Right-click on **Windows Powershell** and **Run as administrator**.
3. Run the following command:

```
msiexec.exe /x ThycoticAgent_x64_VERSION.msi /qn
```



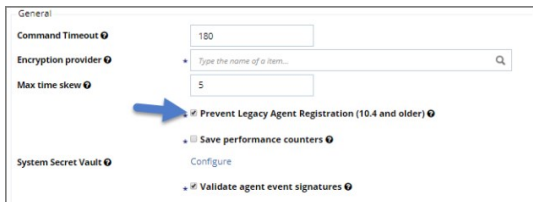
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> msiexec.exe /uninstall C:\Users\Administrator\downloads\ThycoticAgent_x64_10.5_1029.msi_
```

4. On the prompt, click **Yes**.

Starting in Privilege Manager version 10.5 and up, due to security updates you can now prevent services from using agents versions 10.4 and earlier from communicating with the Privilege Manager server.

Resolve

1. Launch Privilege Manager.
2. Navigate to **ADMIN | Configuration**.
3. Click the **Advanced** tab.
4. To enable this setting, click the **Edit** button at the bottom of this page.
5. Check the box next to **Prevent Legacy Agent Registration (10.4 and older)** under the General section.



The screenshot shows the 'General' configuration section in the Privilege Manager interface. It includes several settings: 'Command Timeout' set to 180, 'Encryption provider' with a search dropdown, 'Max time skew' set to 5, and 'System Secret Vault' with a 'Configure' link. The 'Prevent Legacy Agent Registration (10.4 and older)' checkbox is checked, and a blue arrow points to it. Other options include 'Save performance counters' and 'Validate agent event signatures'.

6. Click **Save**.

You need to set Privilege Manager Agent configuration options to readily test configuration changes in a test environment. The agent configurations outlined in this page allow for accelerated feedback when testing use cases.

1. Navigate to **ADMIN | Agents**.

2. Go to either the **Windows Agent Configuration** or **MacOS Configuration** tab.

3. Click **Edit**.

4. Under Intervals, adjust the values to receive quicker turnarounds on any tests run on a test instance.

1. Set Sent Application Action events every to 1 Minutes.
2. Set Send ActiveX events every 5 Minutes.
3. Set Refresh Client Items cache every 5 Minutes.


5. Keep the advanced settings as is (Thycotic recommends to only change the advanced settings after consulting via Professional Service engagement.)

Hide Advanced

Advanced

Policy Priority

Advanced Process Control

 Warning: These settings are only intended to be adjusted with the assistance of support personnel.

Expire file hashes every	<input type="text" value="1"/>	Week(s) ▾
Maximum wait for queue	<input type="text" value="10"/>	Second(s) ▾
Maximum wait in queue	<input type="text" value="30"/>	Second(s) ▾
Maximum pre-processing time	<input type="text" value="40"/>	Second(s) ▾
Maximum processing time	<input type="text" value="1"/>	Minute(s) ▾
Process monitoring interval	<input type="text" value="5"/>	Second(s) ▾

6. Click **Save**.

Certain Privilege Manager tasks are directly related to agent processes and their operational loads.

Server side tasks, also known as Remote Client Scheduled Commands do not require a policy. Agent tasks require a policy. These types of tasks are with the exception of one, by default enabled and run on a scheduled basis. Most are read-only system tasks, that can be copied, renamed, and then customized.

The majority will run for the first time after system initialization.

Windows Remote Client Scheduled Commands

Restrict Account Permissions on Agent Services (Windows)	Instructs computers to only allow the specified users to start and stop the Thycotic services.	n/a	No
Basic Inventory (Initial Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server.	daily	Yes
Basic Inventory (Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server.	daily	Yes
Cleanup Agent Inventory Transfers (Windows)	Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.	daily	Yes
Cleanup sent Privilege Manager Events (Windows)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.	daily	Yes
Configure Privilege Manager Remove Programs	Configure the Privilege Manager Remove Programs behavior.	daily	Yes
Default File Inventory Policy (Windows)	The purpose of this policy is to inventory software programs running on the managed computer.	weekly	Yes
Ensure UAC Override Setting (Windows)	Ensures that the UAC Override Registry Key is set.	daily	Yes
Local User Inventory Policy	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.	weekly	Yes
Perform Resource Discovery (Windows)	Schedule on which agents will check with server to determine if any local resources require discovery.	daily	Yes
Retry errored TMS Events (Windows)	Scan Agent queue for any events that require retransmission.	daily	Yes
Scheduled Check Pending Client Tasks - Internet Clients (Windows)	Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.	daily	Yes
Scheduled Registration - Internet Clients (Windows)	Initiate agent registration with server less frequently than internal clients.	daily	Yes
Scheduled Registration (Windows)	Initiate agent registration with server.	daily	Yes
Update Agent Commands (Windows)	Instructs Agent to update any agent commands if required.	daily	Yes
Update Applicable Policies - Internet Clients (Windows)	Instructs Agent to check with server for policy changes.	daily	Yes
Update Applicable Policies (Windows)	Instructs Agent to check with server for policy changes.	daily	Yes
Update Provisioned Resource Client Items (Windows)		daily	Yes
User Logon Inventory Policy	Updates user logon data on the given schedule.	weekly	Yes
Windows Service Inventory Policy	The purpose of this policy is to inventory Windows Services on the client.	weekly	Yes

MacOS Remote Client Scheduled Commands

Basic Inventory (Initial Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.	daily	Yes
Basic Inventory (Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.	daily	Yes
Cleanup sent Privilege Manager Events (Mac OS)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.	daily	Yes
Default File Inventory Policy (Mac OS)	The purpose of this policy is to inventory software programs running on the managed computer.	weekly	Yes
Local User Inventory Policy (Mac OS)	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.	weekly	Yes
Perform Resource Discovery (Mac OS)	Schedule on which agents will check with server to determine if any local resources require discovery.	daily	Yes
Retry errored TMS Events (Mac OS)	Scan Agent queue for any events that require retransmission.	daily	Yes
Scheduled Registration (Mac OS)	When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.	daily	Yes
Update Agent Commands (Mac OS)	When this policy is triggered the Agent will update agent command items.	daily	Yes
Update Applicable Policies (Mac OS)	When this policy is triggered the Agent will check the server for updated policies.	daily	Yes
Update Provisioned Resource Client Items (Mac OS)		daily	Yes

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents installed on Windows systems.

The following topics are available:

- [Agent Hardening 10.7.1 and up](#)
- [Pre-10.7.1 Agent Hardening](#)

Agent installations on endpoints can be secured, only allowing a specified user access to start or stop an agent service and denying any agent control access to a local Administrator or basic user account.

To make sure that local Administrators do not tamper with Thycotic agents running on their system, Privilege Manager Administrators can define users that can start and stop the Privilege Manager services running on endpoints, such as the Thycotic Agent or Thycotic Application Control.

A user or group needs to be available in Privilege Manager to be selected while setting up the task. This user or group will have rights to start and stop agent services running on endpoints once the **Restrict Account Permissions on Agent Services (Windows)** policy is enabled.

Note: If you implemented Agent Hardening prior to 10.7.1, **disable** and **delete** the following policies:

- Agent Service Start / Stop Control (Windows)
- Agent Service Clear Restrictions (Windows)

Editing the Restrict Account Permissions on Agent Services (Windows) Policy

1. Navigate to **ADMIN I Policies**.
2. Click on the **General** Tab.
3. In the Name field enter **Agent Services**.

The screenshot shows a 'Policies' management interface. At the top left is a blue 'Add New Policy' button. Below it are tabs for 'Windows', 'Mac OS', 'Client System Settings', 'ActiveX', 'Firewall', and 'General' (which is selected). The main area contains a form with an 'ENABLED' dropdown set to 'Any' and a 'NAME' field containing 'Agent Services'. Below the form, there is a 'Not Enabled' link and a blue link for 'Restrict Account Permissions on Agent Services (Windows)'.

4. Click on the **Restrict Account Permissions on Agent Services (Windows)** policy.

The screenshot shows the configuration page for the 'Restrict Account Permissions on Agent Services (Windows)' policy. At the top, it says 'Remote Scheduled Client Command > Restrict Account Permissions on Agent Services (Windows)'. Below that is a blue bar with an information icon and the text 'This item is read-only.'. There are tabs for 'General', 'Parameters', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment'. The 'General' tab is active. It shows an 'Enabled' checkbox which is unchecked. The 'Name' field contains 'Restrict Account Permissions on Agent Services (Windows)'. The 'Description' field contains 'This policy restricts access on the selected services to only the system and selected accounts. No other accounts (including Administrators) will be able to start/stop or modify the services.'. The 'Command' field contains 'Restrict Account Permissions on Services (Script) (Windows)'. At the bottom, there are buttons for 'Back', 'Edit', 'Create a Copy', 'View as XML', and 'Export'.

5. To customize the policy click **Create a Copy**.

1. Customize the name of the copied policy and click **Create**.

The screenshot shows the configuration page for a copied policy named 'DocTest - Restrict Account Permissions on Agent Services (Windows)'. The breadcrumb is 'Remote Scheduled Client Command > DocTest - Restrict Account Permissions on Agent Services (Windows)'. The tabs are the same as in the previous screenshot. The 'Enabled' checkbox is unchecked. The 'Name' field contains 'DocTest - Restrict Account Permissions on Agent Services (Windows)'. The 'Description' field contains 'This policy restricts access on the selected services to only the system and selected accounts. No other accounts (including Administrators) will be able to start/stop or modify the services.'. The 'Command' field contains 'Restrict Account Permissions on Services (Script) (Windows)'. At the bottom, there are buttons for 'Back', 'Edit', 'Create a Copy', 'Delete', 'View as XML', and 'Export'.

6. Click **Edit**.
7. Select **Enabled**.
8. Navigate to the **Parameters** tab.

Remote Scheduled Client Command > DocTest - Restrict Account Permissions on Agent Services (Windows)

General Parameters Triggers Targets Conditions Advanced Deployment

Enter default parameter values for this task.

Services * • ArelliaACSvc • ArelliaAgent

User Accounts * • Administrators

1. Under **Services** the Arellia Application Control Service and Arellia Agent Service are present by default. Add any services you might also want to protect by clicking **+**. Use the search field to find and specify other service names.
2. Under **User Accounts** click the **+** button and use the search field to find specific user accounts that have permissions to make changes to the specified services. Administrators are present by default, if you wish to limit to only a subset of users with administrative rights, create a group and update accordingly.

9. Click **Save**.

Note: If you wish to update a hardened agent, refer to information under the topic [Windows Agents](#).

Users on Privilege Manager 10.7.1 or up should use the new policy named **Restrict Account Permissions on Agent Services (Windows)**. Refer to [Agent Hardening 10.7.1 and up](#) for details on the policy used starting with Privilege Manager 10.7.1.

Editing the Agent Service Start / Stop Control (Windows) Policy

1. Navigate to **ADMIN | Policies**.
2. Click on the **General** Tab.
3. In the Name field enter **Agent Service Start / Stop Control**.

The screenshot shows the 'Policies' management interface. At the top left is a blue 'Add New Policy' button. Below it are navigation tabs for 'Windows', 'Mac OS', 'Client System Settings', 'ActiveX', 'Firewall', and 'General', with 'General' selected. A table lists policies with columns for 'ENABLED', 'NAME', and 'FOLDER'. One policy is shown: 'Agent Service Start / Stop Control (Windows)' with 'Enabled' checked and 'Windows' in the folder column. The page number '1 to 1 of' is in the top right.

4. Click on the **Agent Service Start / Stop Control (Windows)** policy.

The screenshot shows the configuration page for the 'Agent Service Start / Stop Control (Windows)' policy. The breadcrumb is 'Remote Scheduled Client Command > Agent Service Start / Stop Control (Windows)'. There are tabs for 'General', 'Parameters', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment', with 'General' selected. The 'Enabled' checkbox is checked. The 'Name' field contains 'Agent Service Start / Stop Control (Windows)'. The 'Description' is 'Instructs computers to only allow the specified users to start and stop the Thycotic services.' The 'Command' is 'Local Security Set Service Security Script with Account IDs'. At the bottom are buttons for 'Back', 'Edit', 'Create a Copy', 'Delete', and 'Export'.

5. To customize the Agent Hardening policy navigate to the **Parameters tab**.
6. Click **Edit**.

The screenshot shows the 'Parameters' tab of the policy configuration page. The breadcrumb is 'Remote Scheduled Client Command > Agent Service Start / Stop Control (Windows)'. The 'Parameters' tab is selected. The text says 'Enter default parameter values for this task.' There are two sections: 'Services' with a '+ Add' button and a list containing '• ArelliaACSvc' and '• ArelliaAgent'; and 'User Accounts' with a '+ Add' button and a list containing '• Administrators'. At the bottom are buttons for 'Save', 'Cancel', and 'Export'.

7. Under **User Services** click the **+** button and use the search field to select the Services to be targeted by the task
8. Under **User Accounts** click the **+** button and use the search field to find the specific user account that has permissions to make changes to the Agent services.
9. Click **Save**.

Note: If you require a rollback of the agent hardening due to upgrade issues, use the manual Restore Default Agent Permissions procedure following below.

Restore Default Agent Permissions

If you need to rollback agent hardening on your endpoints, follow these steps to restore the default agent permissions:

1. Navigate to **ADMIN | More...** and select **Config Feeds**.
2. Next to **Privilege Manager Product Configuration Feeds** click **Select Items**.
3. Next to **Thycotic Management Server Core** click **Select Items**.
4. Download the **Reset Agent Service Permissions** config feed.

Data Feeds > Thycotic Management Server Core

i The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	DOWNLOADED
Maintenance Resources	Contains maintenance gauges, tasks, etc. for optimal TMS performance	Nov 27, 2019, 12:58:05 PM	Download
Reset Agent Service Permissions	Contains a policy to restore the security descriptor on Thycotic Services	Jan 23, 2020, 4:13:21 PM	Download
SQL CPU Usage Gauge	Contains a gauge and report to monitor SQL CPU usage.	Jul 24, 2019, 5:23:54 PM	Download

[Back](#)

5. Once the config feed is installed, navigate to **ADMIN | Policies** and select the General tab.
6. Search for the agent service policies and select to edit.

Policies

[Add New Policy](#)

Windows Mac OS Client System Settings ActiveX Firewall General

1 to 2 of 2

ENABLED	NAME	FOLDER
Any	agent service	
Enabled	Agent Service Start / Stop Control (Windows)	Windows
Not Enabled	Agent Service Clear Restrictions (Windows)	Windows

7. Disable the **Agent Service Start / Stop Control (Windows)** policy.

1. Click **Edit**.
2. Deselect **Enabled**.

Remote Scheduled Client Command > Agent Service Start / Stop Control (Windows)

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name Agent Service Start / Stop Control (Windows)

Description Instructs computers to only allow the specified users to start and stop the Thycotic services.

Command Local Security Set Service Security Script with Account IDs

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [View as XML](#) [Export](#)

1. Click **Save**.

8. Enable the **Agent Service Clear Restrictions (Windows)** policy.

1. Click **Edit**.
2. Select **Enabled**.

Remote Scheduled Client Command > Agent Service Clear Restrictions (Windows)

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name Agent Service Clear Restrictions (Windows)

Description Sets the Security Descriptor back to Default on Thycotic services.

Command Local Security Clear Restrictive Service Security Script

Back Edit Create a Copy Delete View as XML Export

1. On the Targets tab specify the computers that need to be targeted by this policy.
2. On the Triggers tab specify when to run and/or what events will trigger the policy to run.

9. Click **Save**.

This section of the Privilege Manager documentation covers information and step procedures pertaining to Privilege Manager agents installed on macOS.

The following topics are available:

- [Modify Update Agent Commands \(MacOS\) Policy](#)
- [Terminal Commands](#)
- [Finding Logs for Troubleshooting](#)

Agents receive new policies on a schedule which can be modified.

To check or change the schedule, follow these steps:

1. Go to **Admin | Resources**
2. Select for this macOS machine named the **Update Agent Commands (Mac OS) Policy**.
3. Edit the schedule on the **Triggers** tab.

For troubleshooting your Mac agent, logs are found in the Console application. There are two places to check for logs in Console:

1. You can filter your machine's logs by clicking your machine's name under Devices and typing "Thycotic" into the top search bar.
2. Thycotic-specific logs are recorded in a Console folder that is titled thycotic (found in the left side bar: **Reports | /var/log | thycotic**).

In the Mac Terminal application you can perform the following commands directly to your Thycotic macOS agent.

Note: The sudo command may prompt for admin account password verification.

Find this list by entering the following into Terminal:

```
sudo /usr/local/thycotic/agent/agentUtil.sh
```

These are the commands returned for the utility:

```
runcschedule -scheduleId (id)
updateclientItems
clientItemsSummary
register
setmsserver -serverUri (https://servername.com/Tms/)
setmsserver -serverName (servername)
stop
start
restart
enableverboselogging
disableverboselogging
```

Command Usage

To perform a command, insert the name of the above command that you need to perform into this command string:

```
sudo /usr/local/thycotic/agent/agentUtil.sh [InsertCommandHere]
```

As one example, if you entered an incorrect server name path in the agent installer and Privilege Manager therefore cannot find and register your Mac agent, you can run the command:

```
sudo /usr/local/thycotic/agent/agentUtil.sh setmsserver -serverUri (https://servername.com/Tms/)
```

Which is using the correct server name URI to redirect your agent toward the correct server location.

Or, to register an agent immediately after updating the Privilege Manager server location, type:

```
sudo /usr/local/thycotic/agent/agentUtil.sh register
```

The complete command shell exchange looks like this:

```
macadmin-MacBook-Pro:~ madadmin$ sudo /usr/local/thycotic/agent/agentUtil.sh register
Password:
Initiated registration.
macadmin-MacBook-Pro:~ madadmin$
```


The Privilege Manager UI

The Privilege Manager user interface, also referred to as the console, is launched in a browser. The URL has the following form:

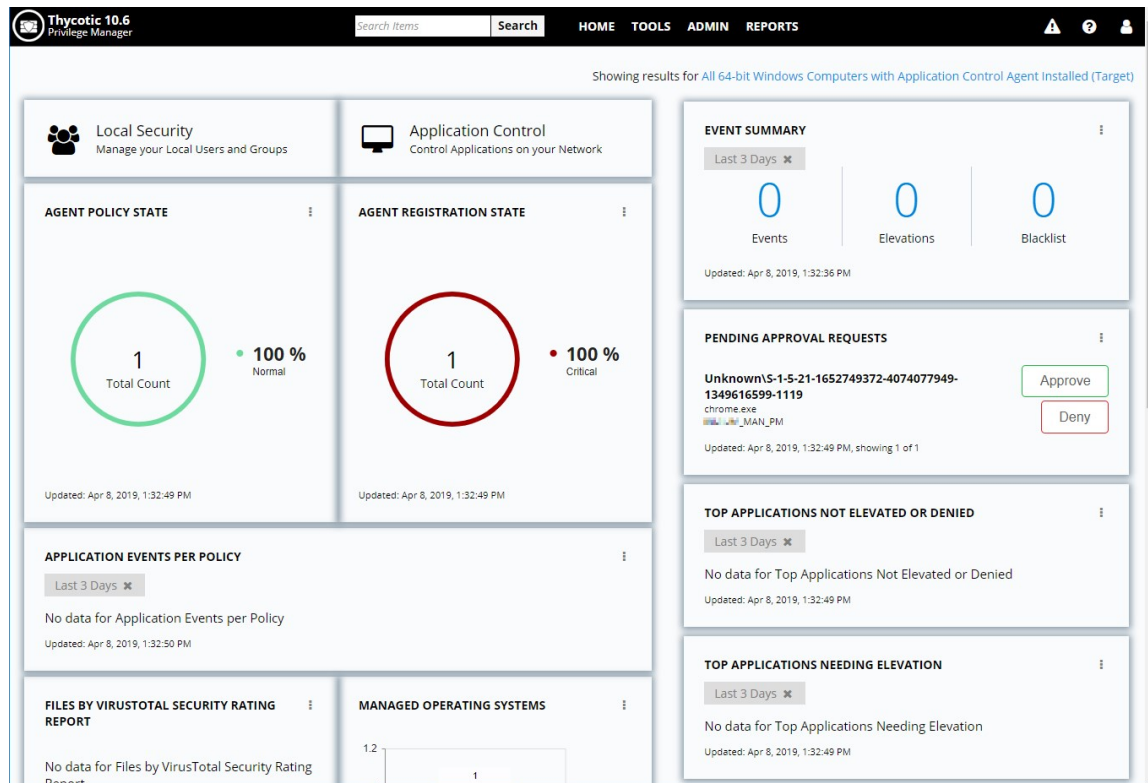
`https://[server-domain]/TMS/PrivilegeManager`

Where:

- `server-domain`, indicates the customer specific domain name, for example
 - <https://mydomain.com/TMS/PrivilegeManager> for On-premises installations and
 - <https://myassignedname.privilegemanagercloud.com/TMS> for Cloud instances.

The User Interface (UI) seen by all Privilege Manager roles is the same (whether Administrator or other). However, most of the interface is enabled only when you login in as a Privilege Manager Administrator; the other roles are able to perform very few activities.

The screenshot below shows the upper part of the Privilege Manager home page.



The home page includes actionable dashboard elements as well as the gateway to the two major components of Privilege Manager, Local Security and Application Control. These are available from their respective tiles.

Much of the text and other content on the page is clickable. The link under it will help you drill down to more detail. (Although some links, here and on other UI pages, are shown in blue, you should not assume that the absence of blue font implies there is no link. The best way to discover links is to hover over the content to find out if it is clickable.)

The set of three little vertical dots, in the upper right corner of each tile, provide options to manipulate the tile.

The ? seen near the right corner of the main menu bar, is used throughout the UI to provide help messages or other access to guidance.

Many aspects Privilege Manager can be customized. The gauges displayed on the home page of the Privilege Manager console and at many other pages can be removed and others can be added. The same with the Reports Options on the Reports page.

What is a Gauge?

Gauges are used in Privilege Manager to display the results of periodic configuration checks of the server and endpoints. Gauges allow reports and graphs to keep historical trend data, and speed up access in the console.

Reports and Gauges Currently Available

Privilege Manager currently has gauges published to track when an agent last communicated with the server, agents that have received all of their policies, agents that have a random password set, etc.

You can click gauges to drill down for more information.

Alerts can be accessed via the Alerts icon in the top right corner of the Privilege Manager console.



The Alert icon displays a number indicator for any alert received:

- Helpdesk: Manage Approval Requests
- Alert Notifications

To access Alert Notifications, click the icon and select Alert Notifications from the menu options.

Notifications are listed by alert categories such as Agents Online, Unacknowledged Events, Install Agents, etc.

NAME	DESCRIPTION	TYPE
Getting Started	Show Getting Started checklist	General
Agents Online	Total agent count is 1. This is the total number of agents that have registered with server and may be higher than the number of active agents you see available. Agents that haven't checked in with the server in the last 30 days are automatically removed from your computer groups. Groups to which computers belong will be updated periodically and can be updated immediately by choosing admin, configuration, and clicking the 'Run Policy Targeting Update' button on the General tab.	Agent Activity

Endpoint Specific Alerts

Alert Notifications can also be triggered for a specific endpoint agent, if the computer resource was configured for monitoring.

1. Navigate to **ADMIN | More...** and select Resources.
2. On the **Resources** tab, open the **Computers** folder.
3. Open the Resource Explorer for the endpoint you wish to monitor by clicking on its name in the list.
4. Select the **Monitor Resource** checkbox.

Resource Explorer > test computer

Summary	Name	test computer
Known Data	Created	Oct 24, 2019, 8:02:17 PM
Events	Modified	Oct 24, 2019, 8:02:17 PM
	Monitor Resource	<input checked="" type="checkbox"/>
	Health	

Once monitoring is enabled, alert notifications for the agent end point are available via the Alert Notification feature.

Alert Notifications

NAME	DESCRIPTION
Agents Online	Total agent count is 2. This is the total number of agents that have registered with server and may be higher than automatically removed from your computer groups. Groups to which computers belong will be updated periodically on the General tab.
Install Agents	Agents are required on endpoints to perform tasks and enforce policies. 3 in the unconfigured - warning state
Number of Old Computers	The number of old computers 1 in the warning state
Unacknowledged Events	The number of unacknowledged events 1 in the warning state
Monitor activity for a specific agent end point	<ul style="list-style-type: none"> October 25 2019, 4:45 AM Registration October 2 2019, 6:16 AM Resource Discovery October 25 2019, 4:45 AM Retrieved Updates November 4 2019, 11:54 AM Retrieved Updates

These type of alerts inform about the agent registration, resource discovery, and update retrieval times.

The Configuration area in Privilege Manager allows users with Privilege Manager Administrator roles to setup new or change existing configurations for areas like user credentials, foreign systems integrations, or authentication. It lets administrators specify settings that control Privilege Manager Server and Console behavior via the Advanced tab.

The Change History tab under Configuration provides users an overview of changes made to configuration items.

When clicking the ? to the top right, the Configuration page gives the user an overview of the Key Configuration settings and System Health.

The configuration page is tabulated and offers configuration or review options under the following tabs:

- [General](#)
- [Discovery](#)
- [Reputation](#)
- [Users - Visible in Privilege Manager Cloud only](#)
- [Credentials](#)
- [Foreign Systems](#)
- [Roles](#)
- [Advanced](#)
- [Authentication](#)
- [Change History](#)

Advanced Tab

The Advanced tab lets you configure settings:

- File Inventory Solution such as
 - [Collectors](#)
- Privilege Manager Server
 - [General](#)
 - [Monitor](#)
 - [Proxy](#)
 - [ServiceBus](#)

To edit any of the advanced settings, click **Edit** on the bottom of the page.

File Inventory Solution

Under the File Inventory Solution the file extensions used for inclusions and exclusions are specified.

- ISO contents filters with default extensions of .exe, .cat, and .zip.
- MSI contents filters with default extensions of .exe, and .cat.
- Package contents filters with default extensions of .exe, .iso, .msi, .cat, .vhd, .vmdk, and .zip.
- VHD contents filters with default extensions of .exe, .cat, and .zip.
- ZIP contents filters with default extensions of .exe, .cat, .msi, and .zip.

When you click Edit at the bottom of the page, you can change any of the listed file extensions.

File Inventory Solution	
Collectors	
ISO contents filter	*.exe;*.cat;*.zip
MSI contents filter	*.exe;*.cat
Package contents filter	*.exe;*.iso;*.msi;*.cat;*.vhd;*.vmdk;*.zip
VHD contents filter	*.exe;*.cat;*.zip
Zip contents filter	*.exe;*.cat;*.msi;*.zip

General System Settings

Under the Privilege Manager Server category, the first section is General settings.

Allow Agent Certificate Mismatch

This is a checkbox that when selected allows agents to communicate with the server even if there is a certificate mismatch.

Maximum Application Event Count

This settings specifies the Maximum number of application action events that will be kept in the database. The default setting is 1,000,000. Also refer to [Purge Maintenance - Application Control Events](#).

Command Timeout

This settings specifies the SQL command timeout. The default is 180 Seconds.

Encryption Provider

This setting specified the Encryption Provider used to encrypt sensitive data.

Inactivity Timeout

This settings specifies the maximum allowed time for inactivity when logged into the Privilege Manager console. The default is set to 30 Minutes. The session token remains active and does not need to be renegotiated when the inactivity timeout happens within the specified session timeout window.

Max Time Skew

This setting specifies the maximum time difference (in minutes) to allow client system clocks to be out of sync with the server.

Prevent Legacy Agent Registration (10.4 and older)

Enabling this setting prevents older agents (prior to 10.5) from registering, allowing only agents with valid agent Install Codes. Only enable this option if you are certain your managed computers have all been upgraded to 10.5 or newer agents.

Save Performance Counters

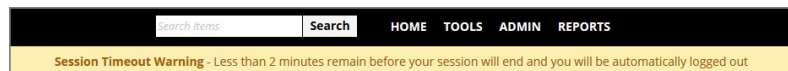
If this setting is selected, the performance counter data will be recorded in the database. Also refer to [Delete Old Performance Counter Events](#).

Session Timeout

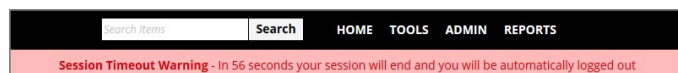
This setting specifies the maximum time in **minutes** for a login session to be active without having to negotiate another token. The default is set to 720 Minutes (12 Hours).

Session Timeout Warning

Two minutes before the set session timeout window expires, Privilege Manager displays a yellow warning with countdown timer to inform users about the pending session timeout.



One minute before the timeout, the color changes to red.



Once the session times out, the active user is logged out and returned to the Privilege Manager Server Setup Home page.

Thycotic 10.7
Privilege Manager Server

HOME PRODUCTS SETUP

Privilege Manager Server Setup Home

- Secret Server**
[Setup a Secret Server Foreign System](#)
- Privilege Manager**
[Add / Update Product Features ?](#)
[Privilege Manager ?](#)

System Secret Vault

This link lets you configure the foreign system used to store secrets.

Validate Agent Event Signatures

Enabling this setting will verify the signature contained within agent events that are sent to the server. Any events with invalid signatures are discarded.

Monitor Settings

Under the Privilege Manager Server category, the second section is Monitor settings. The Monitor setting is designed to monitor the Worker Role to ensure it is healthy and active. When enabled, the process checks the health at each Ping Interval and waits until the Timeout value before considering it unhealthy.

Monitor	
Base local address	<input type="text" value="https://localhost/"/>
Monitor Worker Role	<input checked="" type="checkbox"/> ⓘ
Ping interval	<input type="text" value="15"/>
Timeout	<input type="text" value="30"/>

Base Local Address

This setting specifies the base URL of the Monitor process.

Monitor Worker Role

When this setting is enabled the health of the monitor process will be polled.

Ping Interval

Specifies how often the server will attempt to contact the Monitor process to query its health. The default is set to 15 Seconds.

Timeout

Specifies how long the server process will wait to hear back from a ping request to the Monitor process. The default is set to 30 Seconds.

Proxy Settings

Under the Privilege Manager Server category, the third section is Proxy settings.

Proxy

Proxy server 

Proxy server credential  [Select resource...](#)

Port 

Use proxy server 

Proxy Server

This setting specifies the name or IP address of the proxy server.

Proxy Server Credential

This link lets you configure the credential used to authenticate with the proxy server.

Port

This setting specifies the port used for communications to the proxy server.

Use Proxy Server

If set, communications will be done via the proxy server specified.

ServiceBus Settings

Under the Privilege Manager Server category, the fourth section is ServiceBus settings.

ServiceBus	
Connectivity Mode	HTTPS ▾

Connectivity Mode

This setting specifies the connectivity mode for Service Bus. The default is HTTPS, which is also recommended.

Authentication Tab


The Authentication tab is used for setting up the Authentication Provider used with Privilege Manager. There can only be one provider at a time.

Configuration

General Discovery Reputation Users Credentials Foreign Systems Roles Advanced Authentication Change History

Authentication

i You may only use one authentication provider at a time.

Authentication Provider 

- Thycotic Dev Azure AD Domain
- DocTest Azure AD Domain
- New Azure AD Domain**
- Thycotic Dev Azure AD Domain
- Thycotic One

Note: If you are trying to change your Authentication Provider specifically to NTLM, Privilege Manager runs a verification to make sure the local build-in Administrators Group is in the Privilege Manager Administrator Role.

Credentials Tab

The Credentials tab lets you configure and add new credentials required for configured Foreign Systems.

Configuration

General Discovery Reputation **Credentials** Foreign Systems Roles Advanced Authentication Change History

Credentials

[Add New](#)

1 to 3 of 3

NAME ^	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED
<i>Filter</i>	<i>Filter</i>	<i>Filter</i>	<i>Filter</i>
Default Proxy Server User Credential	Proxy Server User Credential	Principal Self Well Known Group	Sep 13, 2019, 12:20:37 PM
Default User Credential	Default User Credential	Principal Self Well Known Group	Sep 13, 2019, 12:20:37 PM
PM -Test Admin	test admin account		Aug 22, 2019, 10:21:08 AM

User Credentials and Roles

As described for the Roles Tab, Privilege Manager comes with a set of default user roles. Those roles can be edited or new ones can be added to the system.

The role for the Privilege Manager Administrator gives permissions to manage all aspects of the Privilege Manager implementation. As a best practice, it is recommended to set-up roles that limit administrative access to tasks directly related with a users job role.

For integrations with Secret Server keep in mind that Privilege Manger has the ability to use Secret Server as its storage container for credentials. This includes credentials for connecting to integrated systems such as Service Now, as well as credentials for local accounts that are managed by Local Security in Privilege Manager. Customers can choose to integrate with Secret Server only (no Vault setup) or Secret Server and Vault. Either option requires Authentication Data setup for Foreign Systems in Privilege Manager. Refer to the [Setting up Integration between Privilege Manager and Secret Server](#) topic.

If you are integrating with Active Directory synchronization please refer to [Active Directory Synchronization](#).

Note: If you synced with Azure AD, and then added that user to the Privilege Manager Administrators Role, that Azure AD user has admin rights only, if Azure AD is used as the auth provider. If users login via Thycotic One, use Admin | Configuration | Users to create a new user and then add that new user to the Privilege Manager Administrators Role, refer to [How to Add Thycotic One Users Manually](#).

Create User during Installation

During the installation process the Create User page is where you enter information for the initial Privilege Manager Administrator user. Please remember these credentials as they are necessary to login to the web application after you complete the installation.

Discovery Tab

This tab is for resource discovery. After a resource is initially discovered by the server, the name is set to **New Loaded Resource...**. After discovery runs the names of those resources are updated.

Resource Discoverers are selectable under the advanced section. Resource Discoverers are categorized by Agent and Server Discoverers. Most are selected by default and can be disabled by removing the check from the selection box.

Configuration

General **Discovery** Reputation Users Credentials Foreign Systems Roles Advanced Authentication

Resource Discovery

i After a resource is initially discovered by the server, the name is set to 'New Loaded Resource...'. After the following discovery has run the names of those resources will be updated.

[Review Server Resource Discovery Schedule \(Run now\)](#)
[Review Endpoint Resource Discovery Schedule](#)

Default File Inventory Policy (Windows) ⓘ (Can be used to discover file resources)

Hide Advanced

Enable or Disable Resource Discoverers

Agent Discoverers

- App Bundle Agent Discoverer ⓘ
- COM Component Agent Discoverer ⓘ
- COM Application Agent Discoverer ⓘ
- DCOM Agent Discoverer ⓘ
- File Agent Discoverer ⓘ
- File Agent Discoverer (File Location) ⓘ
- File Agent Discoverer (Services) ⓘ
- File Discoverer from ACS Events ⓘ
- File Discoverer from Approval Events ⓘ
- Security Descriptor Agent Discoverer ⓘ














Server Discoverers

- Digital Certificate Server Resource Discoverer ⓘ
- Domain User Group Server Resource Discoverer ⓘ
- File Digital Signature Resource Discoverer ⓘ
- Security Descriptor Server Resource Discoverer ⓘ
- User Server Resource Discoverer ⓘ

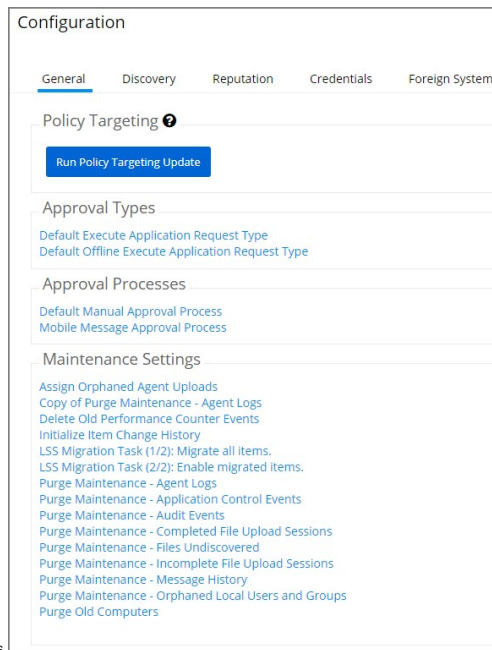
Foreign Systems Tab

Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least SMTP and either Active Directory or Azure AD.

In order to use Secret Server as the password vault please review [Setting up Integration between Privilege Manager and Secret Server](#)

Configuration								
General	Discovery	Reputation	Credentials	Foreign Systems	Roles	Advanced	Authentication	Change History
 Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least SMTP and either Active Directory or Azure AD.								
NAME		COUNT						
Active Directory Domains		0 						
Azure Active Directory Domains		0						
Azure Service Bus		0						
Privilege Manager Server		0						
Secret Server		1						
ServiceNow		0						
SMTP Server		0 						
Symantec Management Platform		0						
SysLog		0						
System Centre Configuration Manager		0						

General Tab



Configuration

General Discovery Reputation Credentials Foreign Systems

Policy Targeting ⓘ

Run Policy Targeting Update

Approval Types

Default Execute Application Request Type
Default Offline Execute Application Request Type

Approval Processes

Default Manual Approval Process
Mobile Message Approval Process

Maintenance Settings

Assign Orphaned Agent Uploads
Copy of Purge Maintenance - Agent Logs
Delete Old Performance Counter Events
Initialize Item Change History
LSS Migration Task (1/2): Migrate all items.
LSS Migration Task (2/2): Enable migrated items.
Purge Maintenance - Agent Logs
Purge Maintenance - Application Control Events
Purge Maintenance - Audit Events
Purge Maintenance - Completed File Upload Sessions
Purge Maintenance - Files Undiscovered
Purge Maintenance - Incomplete File Upload Sessions
Purge Maintenance - Message History
Purge Maintenance - Orphaned Local Users and Groups
Purge Old Computers

The General Tab provides a quick access to Privilege Manager Maintenance tasks and job settings.

Policy Targeting

The Policy Targeting Update automatically caches the list of policies applicable to each agent by updating the collections and resource targets.

Approval Types

For approval types can be specified as policy or file specific, a Security Rating System can be added, and a Process Handler can be entered. The following default approval types are available:

- Default Execute Application Request Type
- Default Offline Execute Application Request Type

Approval Processes

These are read-only items and by default Administrators are always allowed to approve any requests and an optionally activity can be started as part of the approval.

- Default Manual Approval Process
- Default Offline Approval Process
- Mobile Message Approval Process

Markdig.Syntax.Inlines.LinkInLine

- [Assign Orphaned Agent Uploads](#)
- [Delete Old Performance Counter Events](#)
- [Initialize Item Change History](#)
- [Purge Maintenance - Agent Logs](#)
- [Purge Maintenance - Application Events](#)
- [Purge Maintenance - Audit Events](#)
- [Purge Maintenance - Completed File Upload Sessions](#)
- [Purge Maintenance - Files Undiscovered](#)
- [Purge Maintenance - Incomplete File Upload Sessions](#)
- [Purge Maintenance - Message History](#)
- [Purge Old Computers](#)

History Tab

The Change History tab is accessible via:

- **Admin | Configuration** – listing all changes made to Advanced, Authentication Provider, Foreign Systems, Discovery, and Reputation item configuration settings.
- **Admin | Policies** – listing all changes made to policies.
- Admin | More and then (for the default menu, might differ if customized)
 - **Filters** – listing all changes made to a specific filter.
 - **Actions** – listing all changes made to a specific action.
 - **Resources** – listing all changes made to a specific user editable resource. Meaning resources that are not user editable, like a file extension, do not have a history change tab.
 - **Tasks** – listing all changes made to a specific task.

Once the tab is selected, it opens a two-column page. On the left all recorded changes are listed with the newest record on top. This left column data provides a summary of the changes:

- who made the change,
- what was changed,
- the type of change,
- item changed, and
- date/time of the change.

For any changes made to the Authentication Provider for Foreign Systems, like changing from NTLM to Azure Active Directory for example, the Change History provides details about the active and staged states with true and false indicators.

Looking at Details

The following image shows an example of the change history for a foreign system entry. The change shows that the foreign system was initially pointed at the local host URL, with a Credential and Client Secret pertaining to that localhost instance. An update was made to configure a real Secret Server instance URL with accompanying changes of Client Secret and Credential to be able to authenticate against that new URL.

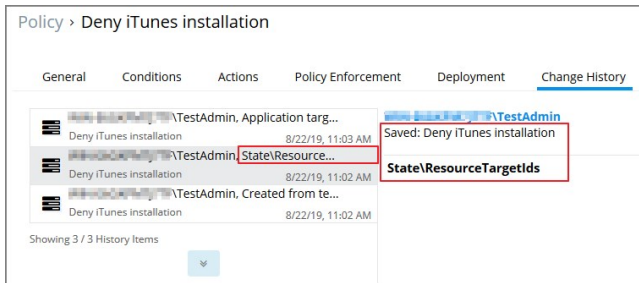
Drilling Down

To look at details of any given change, select one of the change entries in the left column. For the example we created a policy to deny the installation of iTunes on Windows endpoints.

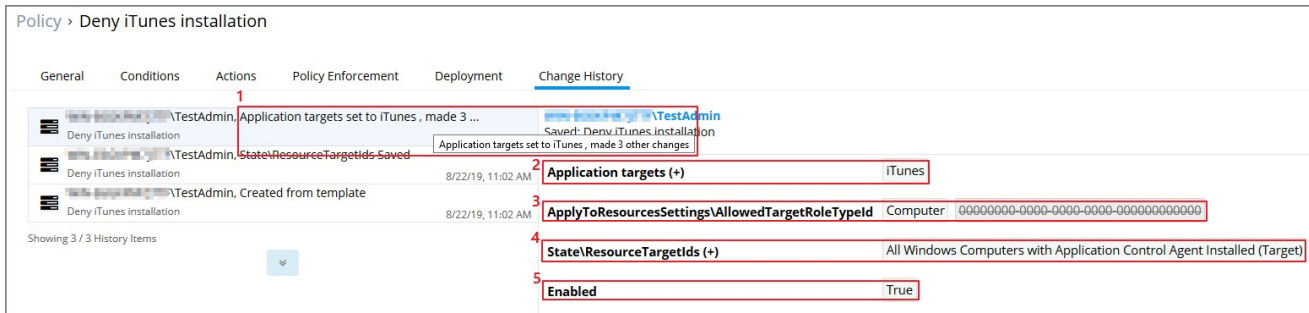
What we see:

1. Information about the system and user initiating the change, here WIN-...\TestAdmin and information about the type of change, here Created from template.
2. The name of the item that was created from template, the date and time when the change occurred.
3. Details on the summary information from the left, such as a link to view the user details and what change was done to which item.

The next screen shows a state change due to the policy being saved. The State\ResourceTargetIds are being saved for the first time for this policy.



The last entry in the Change History list provides all the details about the change to the policy after initial creation and save.



What we see:

1. The left-hand summary indicates that Application targets were set to iTunes and three other changes were made.
2. Application targets (+) iTunes indicates that iTunes was added as an Application target. A (-) would indicate a removal of an application target.
3. ApplyToResourcesSettings\AllowedTargetRoleTypeId indicated that the previous zero value Id was changed to a value of Computer.
4. The State\ResourceTargetIds field was populated with the value All Windows Computer with Application Control Agent Installed (Target).
5. The last change was setting the policy Enabled state to True.

Item Change History Report

The [Item Change History Report](#) is part of the **Diagnostic** group on the Reports page. You can also search for "change history" and the report will be listed on the search results page. Click the link to access the report.

The report lists the history of item changes.

Reports > Item Change History					
Filter Report Refresh CSV PDF Search					
Drag column here for grouping					
Name	Operation	User	Date	Correlation ID	
Test Catch-All Policy	Delete	testing.mydomain.com\ssadmin	11/25/19, 10:08 AM	bf423171-5bf6-4e7d-8	
Test Catch-All Policy	Save	testing.mydomain.com\ssadmin	11/25/19, 9:18 AM	3c54a183-3bb6-47d9-	
Test Catch-All Policy	CreateFromTemplate	testing.mydomain.com\ssadmin	11/25/19, 9:18 AM	bb47a321-139b-4f78-	
Application Entitlements	Save	testing.mydomain.com\ssadmin	11/22/19, 11:32 AM	2bd72239-38f4-4b18-	
Application Entitlements	Save	testing.mydomain.com\ssadmin	11/22/19, 11:02 AM	80952ee3-e7bb-46b3-	
Client Option - Elevate Changing ...	Save	testing.mydomain.com\ssadmin	11/22/19, 10:43 AM	d5d692b3-0009-4394-	
Client Option - Elevate Changing ...	Save	testing.mydomain.com\ssadmin	11/22/19, 10:42 AM	54dd704b-4c76-4b9d-	
New Active-X Group Policy Setting...	Delete	testing.mydomain.com\ssadmin	11/22/19, 8:43 AM	349a7f6f-a740-4eea-9	

For further investigation, you can access the item that was changed by clicking the entries in the Name column.

Reputation Tab

Here you select the Rating Provider from drop-down. Current options are Cylance and VirusTotal rating providers.

The configuration details required are different for the two rating providers as shown in the following sample images.

Cylance Rating Provider

Configuration

General Discovery **Reputation** Users Credentials Foreign Systems Roles Advanced Authentication

Select Rating Provider Cylance Rating Provider

Cylance administrators should add the Thycotic agent to the Cylance safe list. Review [Privilege Manager's documentation](#) on antivirus exclusions.

Credentials

Application Secret Show

Application ID Show

Settings

Tenant ID

Region North America

Edit

VirusTotal Rating Provider

Configuration

General Discovery **Reputation** Users Credentials Foreign Systems Roles

Select Rating Provider VirusTotal Rating Provider

VirusTotal API Key ***** Show API Key Change

Details

Name VirusTotal Rating Provider

Description Application Control VirusTotal based provider for resource security ratings.

Classify as 'Suspect'

When or more positive indicators are found by leading scan engines

When the total number of positive indicators reaches or more across all contributors

Classify as 'Bad'

When or more positive indicators are found by leading scan engines

When the total number of positive indicators reaches or more across all contributors

Back Edit

Roles Tab

The following Privilege Manager roles are available by default and it is possible to add to or remove members from these roles. Privilege Manager also allows the creation of new roles, if a customer environment requires more role support.

NAME	DESCRIPTION
Privilege Manager Administrators	Privilege Manager Administrators
Privilege Manager Field Engineering	
Privilege Manager Helpdesk Users	Privilege Manager Helpdesk Users
Privilege Manager MacOS Administrators	Privilege Manager MacOS Administrator
Privilege Manager Users	Privilege Manager Users
Privilege Manager Windows Administrators	Privilege Manager Windows Administrators

Privilege Manager's Roles logic prevents the removal of a user account with an Administrator Role, if that user account is the last with those Administrator Role privileges. Privilege Manager does not allow current users to delete their own account.

Note: Privilege Manager manages the roles of users accessing the console, unless Privilege Manager is connected to Secret Server. When connected to Secret Server, role membership is controlled by Secret Server.

Also refer to the following topic: [User Credentials and Roles](#).

All these roles are considered application role permissions.

Privilege Manager Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console.

Privilege Manager Field Engineering

This role is reserved for future use.

Privilege Manager Helpdesk Users

This role allows the user to have approve or deny escalation requests access. The helpdesk role can also disclose passwords.

Privilege Manager MacOS Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to macOS systems. This role can view but not edit Windows policies.

Privilege Manager Users

This role allows the user to have read permissions to most items, but no rights to modify security permissions. This role can disclose passwords.

Privilege Manager Windows Administrators

This role allows the Privilege Manager Administrator to have full administrative access to the Privilege Manager Server Console to administer local security and application control items pertaining to Windows systems. This role can view but not edit macOS policies.

Application Roles

The following table provides an overview of Privilege Manager Application Roles:

Privilege Manager Administrators	Can do anything.	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Privilege Manager Field Engineering	Cannot do anything out of box. Reserved for future use.										
Privilege Manager Helpdesk Users	This role is the least permissions and can disclose passwords and do approvals.			yes		yes					
Privilege Manager MacOS Administrators	Can do anything an administrator can, but only for Mac policies and resource targets.	yes	yes	yes		yes	yes	yes (macOS)	yes	yes	yes
Privilege Manager Users	This is a read only role that can view all items, disclose passwords, and do approvals.	yes		yes		yes			yes		
Privilege Manager Windows Administrators	Can do anything an administrator can, but only for Windows policies and resource targets.	yes	yes	yes		yes	yes	yes (Win)	yes	yes	yes

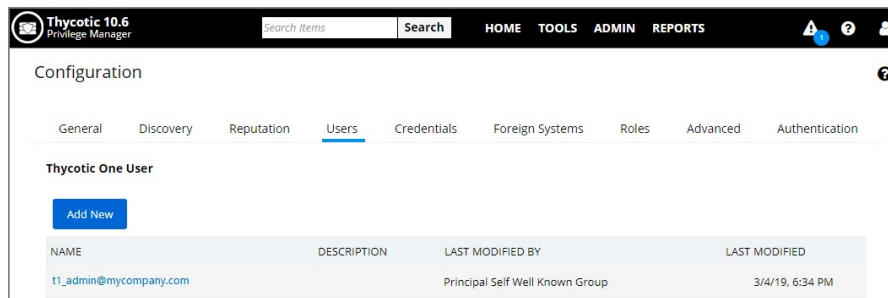
Users Tab - Cloud Only

On the cloud only Users tab new users can be added to Privilege Manager. These users are specified as Thycotic One users.

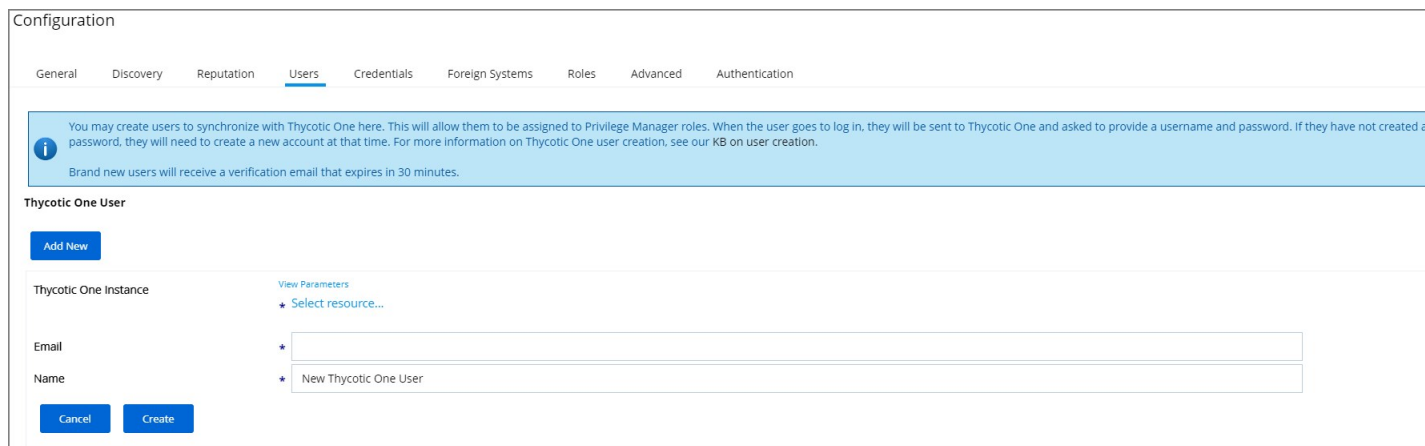
How to Add Thycotic One Users Manually

To manually add users to your Privilege Manager cloud instance, follow these steps:

1. Navigate to **Admin I Configuration** and click the **Users** tab.

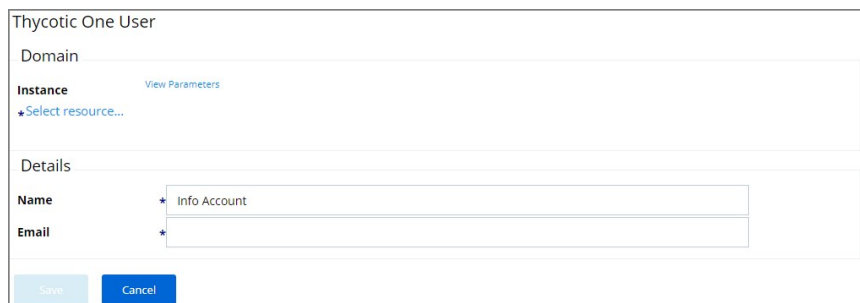


2. Click **Add New**.



3. Enter the new username in the Name field and click Create.

4. Click the Edit button.



5. Click the Select resource link to select the Instance for this user.



6. Click the + button to select the resource.

7. Under **Details** in the Email field enter the accounts email address.

Domain

[View Parameters](#)

Instance

★ Thycotic One

Details

Name ★ Info Account

Email ★ info@mycompany.com

8. Click **Save**.


Navigate to the **ADMIN | Diagnostics** page to view more comprehensive agent details. The Diagnostics page is also the go-to stop for full system health. Go there to find Server Console Logs and other system level warnings or tips.

Diagnostics


This page shows you general diagnostics about your environment that can be used to troubleshoot issues or submit to Technical Support.

[Back](#) [Clear Descriptive Item Cache](#) [Clear Local Storage Cache](#) [Import Items](#) [Console Logs](#)


Managed Operating Systems



Agent Registration State



Agent Policy State



Key Configuration Settings

- Properly Configured** Product Licenses Installed
- Normal** Server Activity Paused
- Normal** Upgrade Available
- Properly Configured** Configure Active Directory
- Properly Configured** Set Default User Credential
- Properly Configured** Install Agents

Licensing

- Normal** Client License Expiration
- Normal** Server License Expiration

System Health

- Normal** Remote Task Status
- Normal** Number of Old Computers
- Normal** Unacknowledged Events
- Normal** Pending Approvals Count
- Normal** Number of Application Events
- Normal** File Uploads Size
- Normal** Background Message Queue Size
- Normal** Background Message Queue Older than 1 Week

This best practices section pertains to all macOS versions from **El Capitan** to (and including) **Catalina**.

Thycotic supports elevation without having to enter admin credentials for these preference panes:

- Date & Time
- Energy Saver
- Network

Other preference panes should not be used in elevation policies based on the nature of their function within the system. They can be elevated, but for certain actions, admin credentials may still be required. Changing those preference panes' settings should really be done by administrators only and not standard users, as designed by Apple®.

All macOS preference panes can be used in deny policies.

This section contains macOS specific user interface topics.

- [Best Practices System Preferences](#)
- [Best Practices Printer Installs](#)
- [Date & Time Preference Pane](#)
- [Energy Saver Preference Pane](#)
- [Network Preference Pane](#)
- [Preference Pane macOS](#)

On macOS systems, users (Admin and Standard) can customize the System Preferences based on their macOS role scope. Details about macOS based customizations via the system preferences can be found at <https://support.apple.com/guide/mac-help/change-system-preferences-mh15217/mac>.

With Privilege Manager you can implement policies that provide application control to deny execution of all preference panes. Run as root policies are only supported and recommended for management of the following preference panes:

- [Date & Time](#)
- [Energy Saver](#)
- [Network](#)

The following rules apply for policy managed preference panes:

- If we have no policy for a given preference pane, the authorization for it is left to its system default.
- A preference pane's default authorization is restored when a policy for it is disabled/deleted.
- Managed preference pane defaults are restored on an uninstall.

Note: For preference panes that display the padlock icon, if you click the padlock to close it, you are required to enter admin credentials to unlock it again. Due to the way macOS caches preference pane authorizations, if a standard user has clicked the padlock icon, they will have to close and reopen System Preferences for the policy evaluation to be performed again.

Error Behavior of Preference Panes

When a particular preference pane is opened in the System Preferences application, XPC bundles for that particular preference pane are opened. These XPC bundles remain open until the System Preferences application is completely closed.

This behavior can result in apparent failed policy evaluations. Opening a preference pane that has previously been opened and evaluated without closing the System Preferences application following the initial opening, results in the policy evaluation not triggering again for that particular preference pane due to the XPC bundle remaining open.

For example, if you have a policy that requires approval of Date & Time preference pane changes and our notification dialog is cancelled and then Date & Time is opened again, our notification dialog is not presented to the user again. Instead, a sheet dialog indicates that the preference pane can't be loaded. In order to trigger policy evaluation again, System Preferences must be closed and then reopened.

User Based Behavior of Preference Panes

Standard User

Without an active policy, preference panes appear locked and standard users are not able to make changes. The exception is the Date & Time preference pane. Standard users are allowed to edit the clock appearance. Any changes here are specific to the user's session and can be modified without clicking the locked padlock icon despite what the text next to the icon says.

With an active policy, depending on its action, the following happens for:

- **Deny Execute | Deny Execute Message | Application Denied** - The user is presented with a dialog indicating they are denied running the preference pane. Depending on the usage of Deny Execute Message versus Application Denied Message and the version of macOS, each one may appear twice.
- **Application Justification** - The user is presented with the justification dialog. Once the user enters a justification and clicks Continue, all controls on the pane are enabled. Any changes made are saved. When the user clicks Cancel, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane.
- **Application Warning** - The user is presented with the warning dialog. When the user clicks Cancel, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane. When the user clicks Continue, all controls on the pane are enabled and any changes made are saved.
- **Application Approval Request** - The user should be presented with the approval dialog. When the user clicks Cancel, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane. Once the user enters a reason and clicks Continue, the dialog for waiting for approval is displayed. If the user clicks Cancel in the waiting dialog, macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane. Depending on the Approval action (Allow or Deny), the following takes place:
 - **Allow** - All controls on the pane are enabled. Any changes made are saved.
 - **Deny** - macOS will display an error sheet in System Preferences indicating there was an error loading the preference pane.

The following preference panes require admin credentials to make changes and should not be managed with a run as root policy that triggers a user dialog for justification or approvals:

- Parental Controls,
- [Printers & Scanners](#),
- Security & Privacy,
- Sharing,
- Time Machine, and
- Users & Groups

Admin User

Local admin users should not be managed by any policies requiring user interaction when the policy is triggered. For macOS endpoints the only type of policy would be to demote administrative rights for a particular preference pane by simply denying access.

To install and manage printers via the Printers and Scanners preference pane, standard users on macOS should be added as members of the **lpadmin** group. You can use Privilege Manager's [LSS user and group management features](#) to assist with this.

On macOS, adding a printer can happen in three ways. Two of those can be allowed through an elevation policy enabling a user to add a printer via

- an .app installation file directly or
- a .pkg driver installation directly.

The third option is where the Printers and Scanners preference pane is used to manually add a printer based on existing printer drivers. Refer to the link below for more information.

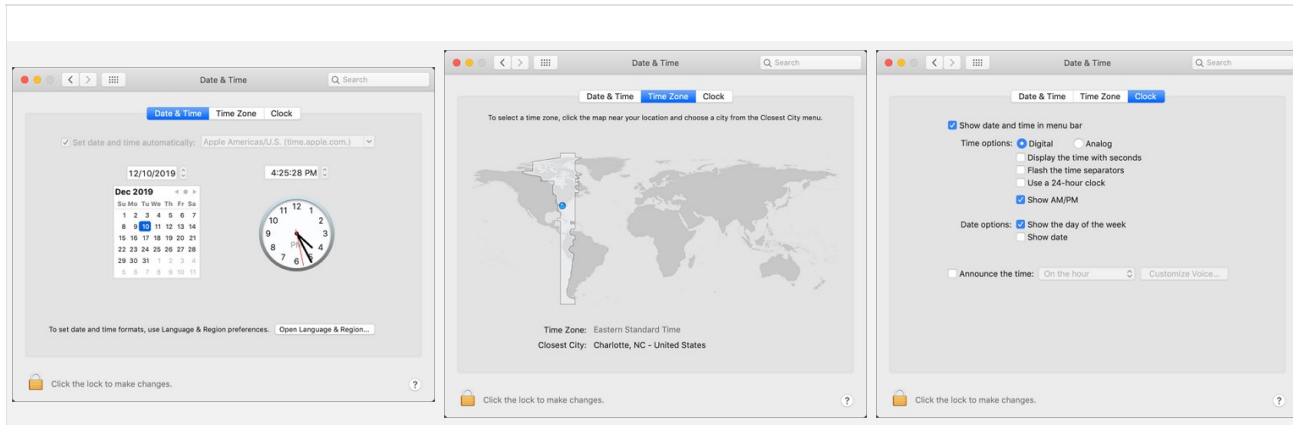
Under the first scenario, the application that is performing the install and configuration of the printer may prompt for admin credentials. If this is the case, you may need a policy that allows the application or applications provider by the printer vendor.

Refer to <https://support.apple.com/guide/mac-help/add-a-printer-on-mac-mh14004/10.15/mac/10.15> for the latest printer setup information from Apple.

Standard User - System Defaults

For standard users when Date & Time is not managed by a policy,

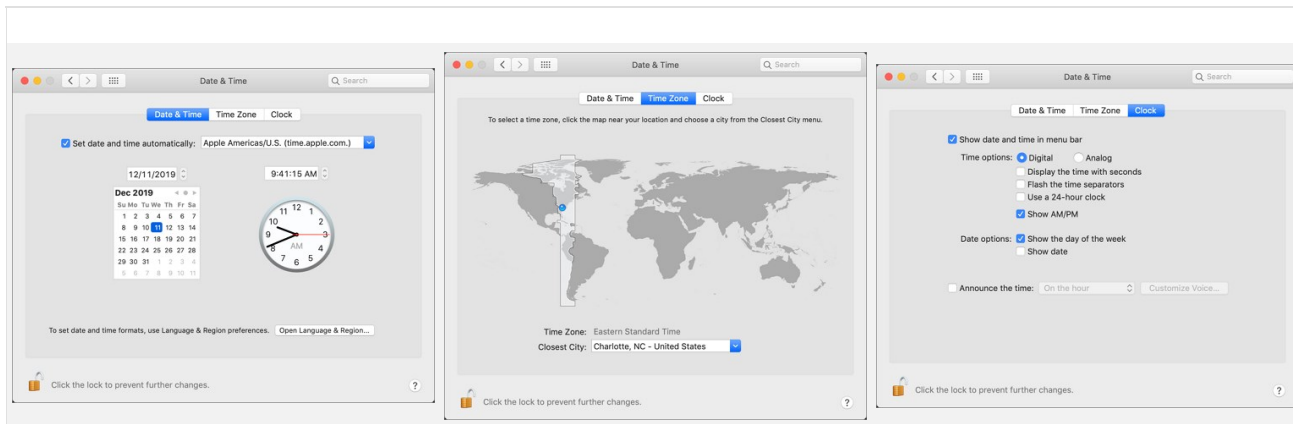
- all controls on the Date & Time tab are disabled and the padlock icon is closed.
- all controls on the Time Zone tab are disabled and the padlock icon is closed.
- all controls on the Clock tab are enabled and changeable by the user. These are user specific settings.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Standard User - Managed by Policy

For standard users when Date & Time is managed by a policy to run as root,

- all controls on the Date & Time tab are enabled and changes are saved.
- all controls on the Time Zone tab are enabled and changes are saved.
- all controls on the Clock tab are enabled and changeable by the user. These are user specific settings.
- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

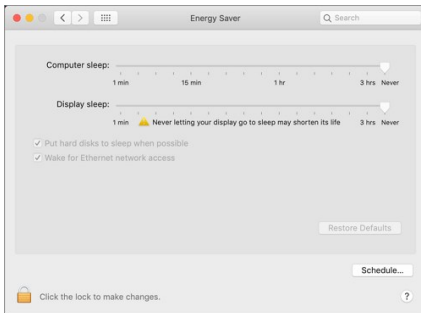
For local admin users, the padlock icon appears locked, by clicking on it a prompt is triggered to enter admin credentials. Once those admin credentials are entered, the padlock icon is unlocked and changes can be made.

Using a policy to run as root is not necessary for local admin users.

Standard User - System Defaults

For standard users when Energy Saver is not managed by a policy,

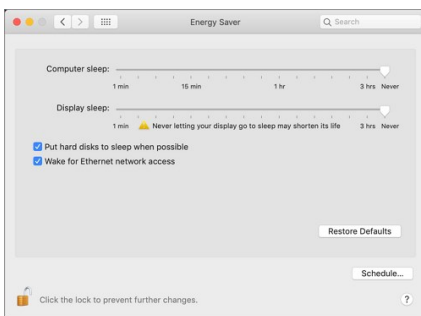
- all controls are disabled and the padlock icon is closed.
- Clicking the Schedule... button shows a panel with disabled controls.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Standard User - Managed by Policy

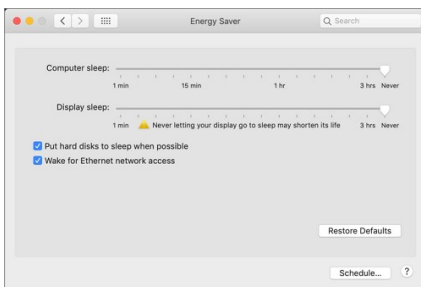
For standard users when Energy Saver is managed by a policy to run as root,

- all controls are enabled and changes are saved.
- Clicking the Schedule... button shows a panel with enabled controls. Any changes are saved.
- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

For local admin users, the Energy Saver pane does not have a padlock and all controls are enabled and changeable. Any changes are saved.

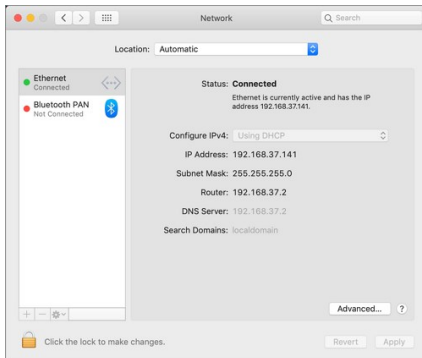


Using a policy to run as root is not necessary for local admin users.

Standard User - System Defaults

For standard users when Network is not managed by a policy,

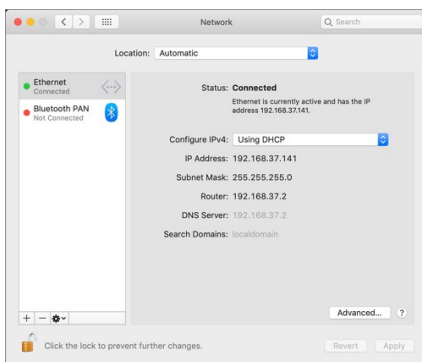
- all controls except for Location and Advanced are disabled and the padlock icon is closed.
- Clicking the Advanced... button opens a sheet depending on the network interface selected. Based on the selected interface, some elements may be enabled.
- Clicking on the padlock icon results in a prompt, asking for administrator credentials.



Standard User - Managed by Policy

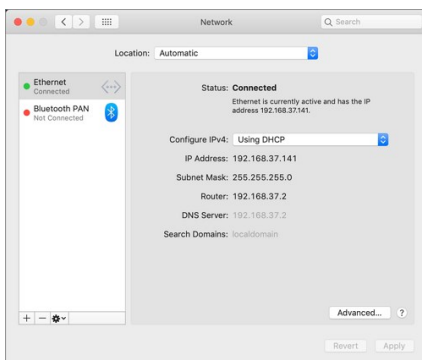
For standard users when Network is managed by a policy to run as root,

- all controls are enabled and changes are saved.
- Clicking the Advanced... button opens a sheet depending on the network interface selected. Based on the selected interface, elements are enabled.
- The padlock icon is unlocked.



Local Administrator User - Not Managed by a Policy

For local admin users, the Network pane does not have a padlock and all controls are enabled and changeable. Any changes are saved.



Using a policy to run as root is not necessary for local admin users.

A Preference Pane (abbreviated as prefpane) is a dynamically loaded plugin in Mac OS X. Introduced in Mac OS X v10.0, the purpose of a Preference Pane is to allow the user to set preferences for a specific application or the system by means of a graphical user interface.

Targeting Preference Panes

How do you target Preference Panes on macOS endpoints? On versions of Privilege Manager (10.3 and lower), you need to specify Preference Pane actions via filepath or file name. A chart is listed below for reference to some of the most common Preference Pane targets:

App Store	com.apple.preferences.appstore.remoteservice	/System/Library/PreferencePanes/AppStore.prefPane/Contents/XPCServices/com.apple.preferences.appstore.remoteservice.xpc/Contents/MacOS/
Date & Time	com.apple.preference.datetime.remoteservice	/System/Library/PreferencePanes/DateAndTime.prefPane/Contents/XPCServices/com.apple.preference.datetime.remoteservice.xpc/Contents/MacOS/
Energy Saver	com.apple.preference.energysaver.remoteservice	/System/Library/PreferencePanes/EnergySaver.prefPane/Contents/XPCServices/com.apple.preference.energysaver.remoteservice.xpc/Contents/MacOS/
Network	com.apple.preference.network.remoteservice	/System/Library/PreferencePanes/Network.prefPane/Contents/XPCServices/com.apple.preference.network.remoteservice.xpc/Contents/MacOS/
Parental Controls	com.apple.preferences.parentalcontrols.remoteservice	/System/Library/PreferencePanes/ParentalControls.prefPane/Contents/XPCServices/com.apple.preferences.parentalcontrols.remoteservice.xpc/Contents/MacOS/
Printers and Scanners	com.apple.preference.printfax.remoteservice	/System/Library/PreferencePanes/PrintAndScan.prefPane/Contents/XPCServices/com.apple.preference.printfax.remoteservice.xpc/Contents/MacOS/
Security & Privacy	com.apple.preference.security.remoteservice	/System/Library/PreferencePanes/Security.prefPane/Contents/XPCServices/com.apple.preference.security.remoteservice.xpc/Contents/MacOS/
Sharing	com.apple.preferences.sharing.remoteservice	/System/Library/PreferencePanes/SharingPref.prefPane/Contents/XPCServices/com.apple.preferences.sharing.remoteservice.xpc/Contents/MacOS/
Time Machine	com.apple.prefs.backup.remoteservice	/System/Library/PreferencePanes/TimeMachine.prefPane/Contents/XPCServices/com.apple.prefs.backup.remoteservice.xpc/Contents/MacOS/
User & Groups	com.apple.preferences.users.remoteservice	/System/Library/PreferencePanes/Accounts.prefPane/Contents/XPCServices/com.apple.preferences.users.remoteservice.xpc/Contents/MacOS/

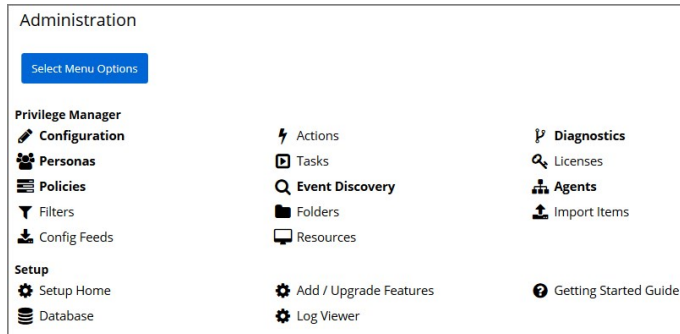
Catalina Preference Pane Behavior

Refer to [Best Practices System Preferences](#) for details.

The Privilege Manager console allows the customization of the quick access menu items. These are the product areas that are available when navigating to the Admin menu. The default options for quick access are Configuration, Personas, Policies, Event Discovery, Diagnostics, and Agents.

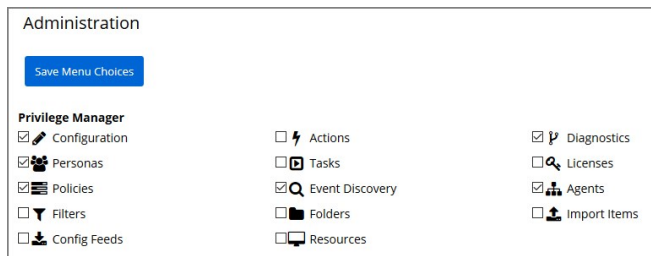
To change the default quick access menu options, follow these steps:

1. Navigate to **Admin | More**.



Active quick access options are indicated as bold on this page.

2. Click **Select Menu Options** to customize the quick access menu.



3. Select or deselect any of the checkboxes for the quick access menu items.

4. Click **Save Menu Choices**.

The menu options are immediately available for quick access under the Admin menu list. The following image shows the Admin menu after Filters and Folders have been selected.



The Resource Explorer provides information about any type of resource item in Privilege Manager.

The Resource Explorer provides:

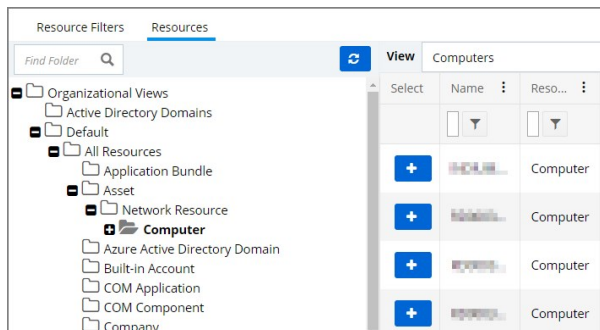
- **Summary**, which contains general information, such as name, description, and modified date for any resource accessed.
- **Known Data**, such as any data known that relates to the resource. This data is different from resource type to resource type. For example, a domain has Global Domain Details and no account details, and a file will have all sorts of information pertaining to the file.
- **Events** are log-style data entries that are directly related to the resource. For example for discovered files, those are the events that are reported from an endpoint.
- **Associations**, are any associated/related items.

Resources can be deleted from the Resource Explorer page.

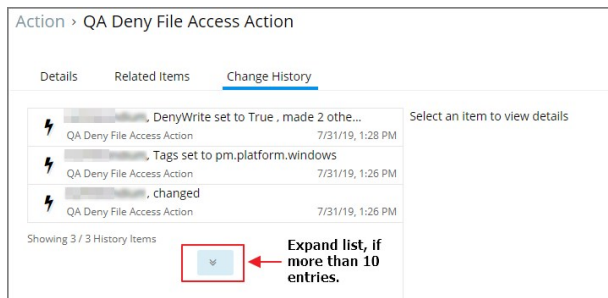
Note: Only use Delete when you are absolutely sure that you want to delete that resource. Clicking on Delete will delete the current resource record you are viewing.

The Resource Explorer is accessible by either navigating to

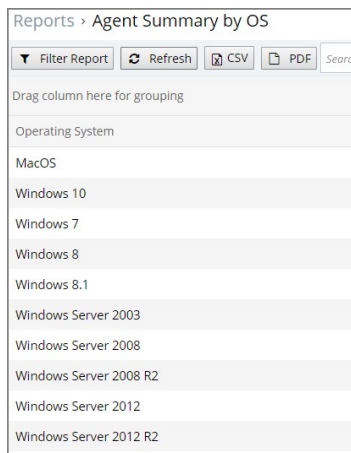
- **Admin | More**, selecting the **Resources** link and expanding the Resources tree drilling down to a named resource to further explore and/or edit.



- **Change History** tab of a named resource.



- any named item, such as a report, in the Privilege Manager console and selecting a named resource.



Example for Discovered Files

You enter the Resource Explorer for discovered file through **Admin | Event Discovery** and then the **Files** tile. On the Events page, click any of the discovered file links to drill down to the files resources.

The following image shows all discovered information about the chrome.exe file, such as:

- File Name
- Original File Name

- Product Name
- Version
- Internal Name
- Company Name
- Copyright information
- File Hashes
- View Reputation, if a reputation provider is integrated with your Privilege Manager instance.

Resource Explorer > chrome.exe

Summary

Known Data

Events

Associations

File Name chrome.exe

Original File Name chrome.exe

Product Name Google Chrome

Version 76.0.3809.132

Internal Name chrome_exe

Company Name Google LLC

Copyright Copyright 2019 Google LLC. All rights reserved.

File Hashes md5: 94e4f3e52bae1a934889aaeb7238dccc
sha1: f6af6cd298f660ff5bb4f89398d1d3edac020a7d
Authenticode: 78758f2f8aeb5396e72db8e5a4678bdfc477d888

View Reputation [VirusTotal.com](#)

Back View as XML Add New Filter Add To Policy Delete

Computer Locations Policy Events Similar Files Report

Drag column here for grouping

COMPUTER NAME	DOMAIN	OS NAME	FILE PATH
TMSTest	Testbed.local	Microsoft Windows Server 2016 Datacenter	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

Showing 1 - 1

Export to CSV | PDF

In the bottom section of the explorer page you can look at further details on the **Computer Locations**, **Policy Events**, and **Similar Files Report** tabs.

The **Computer Locations** tab provides details about the discovery locations where the file was discovered.

The **Policy Events** tab provides details about the policy events that triggered by the file if executed.

The **Similar Files Report** tab provides a list of and links to similar files that have been discovered by Privilege Manager.

Resource Explorer > chrome.exe

Summary

Known Data

Events

Associations

File Name chrome.exe

Original File Name chrome.exe

Product Name Google Chrome

Version 76.0.3809.132

Internal Name chrome_exe

Company Name Google LLC

Copyright Copyright 2019 Google LLC. All rights reserved.

File Hashes md5: 94e4f3e52bae1a934889aaeb7238dccc
sha1: f6af6cd298f660ff5bb4f89398d1d3edac020a7d
Authenticode: 78758f2f8aeb5396e72db8e5a4678bdfc477d888

View Reputation [VirusTotal.com](#)

Back View as XML Add New Filter Add To Policy Delete

Computer Locations Policy Events Similar Files Report

Drag column here for grouping

PRODUCT NAME	WIN32 EXECUTABLE	INTERNAL NAME	COMPANY NAME	PRODUCT VERSION	FILE VERSION
Google Chrome	elevation_service.exe	elevation_service_exe	Google LLC	75.0.3770.100	75.0.3770.100
Google Chrome	chrome.exe	chrome_exe	Google LLC	75.0.3770.100	75.0.3770.100
Google Chrome	chrome.exe	chrome_exe	Google LLC	75.0.3770.142	75.0.3770.142
Google Chrome	elevation_service.exe	elevation_service_exe	Google LLC	75.0.3770.142	75.0.3770.142
Google Chrome	chrome.exe	chrome_exe	Google LLC	76.0.3809.87	76.0.3809.87
Google Chrome	elevation_service.exe	elevation_service_exe	Google LLC	76.0.3809.100	76.0.3809.100
Google Chrome	chrome_proxy.exe	chrome_proxy	Google LLC	76.0.3809.100	76.0.3809.100
Google Chrome	chrome.exe	chrome_exe	Google LLC	76.0.3809.100	76.0.3809.100
Google Chrome	chrome_proxy.exe	chrome_proxy	Google LLC	76.0.3809.132	76.0.3809.132

The Known Data for a discovered file includes details like the

- File Inventory, which provides COFF Header and File Digital Signature data in raw form.

Resource Explorer > chrome.exe

Summary

Known Data ▲

- File Inventory ▲
- COFF Header**
- File Digital Signature Raw
- Software Management ▼
- File Details
- File Digital Signature
- Hash
- Events** ▼
- Associations**

View Default Viewer ▾

NAME	VALUE
Characteristics	34
Checksum	1683213
Machine	34404
Magic	523
MajorImageVersion	0
MajorOperatingSystemVersion	5
MajorSubsystemVersion	5
MinorImageVersion	0
MinorOperatingSystemVersion	2
MinorSubsystemVersion	2
NumberOfSections	10
NumberOfSymbols	0
Subsystem	2
TimeDateStamp	2019-08-23T05:00:00+00:00
Win32VersionValue	0

Back View as XML Add New Filter Add To Policy Delete

- Software Management, which provides the files Manifest, Version Info in raw form, and Win32 Executables details.

Resource Explorer > chrome.exe

Summary

Known Data ▲

- File Inventory ▲
- COFF Header
- File Digital Signature Raw
- Software Management** ▲
- Manifest
- Version Info Raw
- Win32 Executable**
- File Details
- File Digital Signature
- Hash
- Events** ▼
- Associations**

View Default Viewer ▾

NAME	VALUE
CompanyName	Google LLC
Copyright	Copyright 2019 Google LLC. All rights reserved.
FileSubType	0
FileType	1
FileVersion	76.0.3809.132
InternalName	chrome_exe
Language	English (United States)
OriginalFileName	chrome.exe
ProductName	Google Chrome
ProductVersion	76.0.3809.132

Back View as XML Add New Filter Add To Policy Delete

- File Details, such as name, file extension, file size, and if protected or not.
- File Digital Signature, which provided information on the Signer, Countersigner if available, and the signature date/time stamp.
- Hash, provides details on the name, the hash, and hex hash.

Under Events, Infrastructure offers a view into the Resource Discovery events that discovered the file, in this example the File Agent Discoverer and File Agent Discoverer (File Location) events.

Resource Explorer > chrome.exe

Summary

Known Data

- File Inventory
- COFF Header
- File Digital Signature Raw
- Software Management
- Manifest
- Version Info Raw
- Win32 Executable
- File Details
- File Digital Signature
- Hash

Events

Infrastructure

Resource Discovery

Associations

View: Default Viewer

RESOURCE\DISCOVERERID ^	AGENT\DISCOVERERRESOURCEID	DISCOVERED
File Agent Discoverer	TMSTest	2019-09-03T16:00:31+00:00
File Agent Discoverer (File Location)	TMSTest	2019-09-03T16:00:31+00:00

Back
View as XML
Add New Filter
Add To Policy
Delete

This discovered file resource has no related items associated and thus the Associations area of the Resource Explorer is empty.

Example for User Resource

When you are looking at change history for any item and click the view user link, you access the **Resource Explorer** for that specific user resource. The Summary information for that specific user resources shows:

- Name – this is the user account that made the change.
- Created – indicates when the item was created.
- Modified – indicates when the item was last modified.

The resource explorer is providing information about the current state of that user resource.

Resource Explorer > WIN-GGGRPMQ7TF\TestAdmin

Summary

Known Data

Events

Associations

Name WIN-GGGRPMQ7TF\TestAdmin

Created Aug 22, 2019, 10:36:13 AM

Modified Aug 22, 2019, 10:36:13 AM

Back
View as XML
Delete

Under **Known Data** we can explore the information for **Security Management | Global Account Details**.

Resource Explorer > WIN-GGGRPMQ7TF\TestAdmin

Summary

Known Data

- Security Management
- Global Account Details
- Global Windows Users

Events

Associations

View: Default Viewer

NAME	VALUE
AccountDomain	WIN-GGGRPMQ7TF
Description	
IsBuiltin	false
Name	TESTADMIN
Rid	1002
SID	U+502-40202-660202-10-10-8000-4020-1002

Back
View as XML
Delete

Users can select the View from the drop-down and see information on the type of the resource. User resources provide details about:

- AccountDomain – identifies the domain for the user account.
- Description
- IsBuiltin – can be true false to indicate if the account is built-in or not.
- Name – Name associated with the user account.
- Rid
- SID

Selecting the Global Windows Users information shows Name, Domain, and UserId.

Under **Events**, you can view **Infrastructure | Resource Discovery** information:

Resource Explorer > [www.delinea.com](#) \TestAdmin

Summary

Known Data ▲

- Security Management ▲
- Global Account Details
- Global Windows Users

Events ▲

- Infrastructure ▲
- Resource Discovery**

Associations

View Default Viewer ▾

NAME	VALUE
AgentDiscovererResourceid	
Discovered	2019-08-22T10:36:34-04:00
ResourceDiscovererid	User Server Resource Discoverer

[Back](#) [View as XML](#) [Delete](#)

Under **Associations** you can see related items, such as **Group Membership**, which is based on the users credentials.

Error Message after Deleting a User Resource

In case a resource was deleted, an error message like the following will be shown the next time the resource view link is accessed.

InvalidItemidException
The server could not find an item required for this request. Please check the server logs for additional information.
The specified Guid '9c0f4d76-5557-4aab-941d-3d13bc30cf81' is not a valid item.

The Tools menu in Privilege Managers offers access to

- [Password Disclosure](#)
- [File Upload](#)
- [Manage Approvals](#)
- [Offline Approval](#)
- Secret Server, if integrated.

The File Upload options allows existing file uploads via the standard Choose File dialog.

Upload a file

Application File: No file chosen

Notice: Files uploaded to the server will be stored temporarily during the inventory process without the ability to be executed. The file is then deleted once the process completes.

The file upload functionality is available during imports of items, for diagnostics, and for inventory purposes.

The Password Disclosure tool lets users based on role permissions disclose passwords and look a password rotation history.

The password rotation history is helpful when systems are being restored to a time prior to the current password.

Using the Disclose Password Tool

1. Navigate to **TOOLS | Disclose Password** or **TOOLS** and select the **Manage Password** link.
2. The Computer page opens.

Computer

Parameters

Computer name * %

Computer domain [All]

OS name [All]

Search

Computer Name	Computer Domain	OS Name	IP Address	Count
test computer	WORKGROUP	Microsoft Windows Server 2016 Standard	::1	1

10 Items per page 1 - 1 of 1 items

Cancel Select

Select a computer from the list.

3. The Password Disclosure page opens, it list the managed users and also provides links to view the current password and to password history.

Password Disclosure

Computer test computer

Managed Users 1 to 1 of 1

USER NAME	COMPUTER	DOMAIN	PASSWORD LAST CHANGED
test computer\Test Disclosure	test computer	WORKGROUP	Nov 4, 2019, 3:28:01 PM

View Password View Historical Password

4. Click on View Password to view the current password.

WIN-E6GKPM7J7TF\Test Disclosure's Password

Password

MG98jR&%!F%4

Phonetic

MIKE GOLF NINE EIGHT juliet ROMEO & % ! FOXTROT % FOUR

Close

5. Click on View Password History to view the password history.

Historical Passwords	
CHANGED	
November 4, 2019 at 3:32:01 PM GMT-5	View Password
November 4, 2019 at 3:31:01 PM GMT-5	View Password
November 4, 2019 at 3:30:01 PM GMT-5	View Password
November 4, 2019 at 3:29:01 PM GMT-5	View Password
November 4, 2019 at 3:28:01 PM GMT-5	View Password
November 4, 2019 at 3:27:01 PM GMT-5	View Password
November 4, 2019 at 3:26:01 PM GMT-5	View Password

[Close](#)

Select a link on the password history modal to view any of the rotated passwords.

WIN-E6GKPM7J7TF\Test Disclosure's Password

Password at November 4, 2019 at 3:32:01 PM GMT-5

wNUw~bLwXYC1

Phonetic

whiskey NOVEMBER UNIFORM whiskey ~ bravo LIMA
whiskey X-RAY YANKEE CHARLIE ONE

[Close](#)

[Close](#)

Note: Any password disclosure is audited and can be viewed in the **Password Disclosure History** report (requires Administrator role membership).

Local Security

Local Security in Privilege Manager allows customers to

- discover all local accounts and groups that exist on endpoints.
- provide membership control of those accounts on endpoints.
- allows to take complete ownership of the local credentials by enforcing password rotation for all accounts on those endpoints.
- use best practices when it comes to locking down the network from malicious endpoint attacks that exploit unsecured administrative access.

Local Security is made up of

- Computer Groups
- Local Groups
- Local Users

Under Reports various Local Security reports and summaries are available.

These so called resource targets (as configured in Application Control) are specified sets of computers that meet certain criteria, that are targeted by certain policies and scheduled tasks.

Each computer group contains all local groups and local users on endpoints with a local security agent installed. When the agent registers, Local Security automatically discovers the local groups that exist on each machine.

Each local group has a list of local users that exist in that specific local group. From that list you can see

- how many groups each user account is a member of.
- whether the user account is built-in or user-defined.
- whether or not the account itself is managed.

Setting up a local user account with password rotation means that the account is a managed account within Privilege Manager.

From Privilege Manager's Home page, click the left-hand section called Local Security to enter the Local Security Home. From Local Security's navigation panel you can click into existing Computer Groups to view all local groups and user accounts across these endpoint. The Local Security Home dashboard will give you a bird's eye view of the Computer Groups that already exist in your system.

Thycotic 10.6 Privilege Manager

Search Items Search HOME TOOLS ADMIN REPORTS

Getting Started - Show Getting Started checklist

LOCAL SECURITY HOME

COMPUTER GROUPS

MacOS Computers 0

Windows Computers 1

Local Security Home

Show All Computer Groups

Create Computer Group

1 to 2 of 2

NAME	COMPUTERS	USER GROUPS	USERS
Windows Computers	1	25	3
MacOS Computers	0	0	0

Computer Groups

If you have agents already installed and registered, you will see numbers automatically listed in Local Security Home, divided by Privilege Manager's two out-of-the-box computer groups that are listed as:

- Windows Computers and
- MacOS Computers

For example, in the screenshot above only one agent is registered with Privilege Manager. Local Security tells us that the agent is installed on a Windows computer (thus categorized in the Windows Computers group), that there are 25 local User Groups, and 3 local Users on the machine. Local Security automatically discovers this information upon every agent's registration with Privilege Manager.

If you have Computer Groups (also called Resource Targets) already configured for Application Control in Privilege Manager, keep in mind that those groups can also appear as Computer Groups in your Local Security navigation pane after selecting the "Show All Computer Groups" check box. Select the first column of any row to use the target endpoints as a Computer Group and display it in the left navigation panel.

To add new computer groups tailored to your organization's environment, click the Create Computer Group button from the Local Security Home screen. Enter a Name for your new group, a Description, and from the drop-down list select the Operating System (Windows vs macOS) used by these computers.

New Computer Group

Computer Group Name

Description

Show in left menu

Operating System

To select the machines you want to include within this group, you must create a Filter that will target the appropriate machines on your organization's network.

The default filter will begin with a rule that targets computers within the main OS Computer Group that was selected when you created the group, meaning it will target either all Windows or all Mac computers with registered agents.

To narrow your group, click **Add Rule** then in the List Type column select from the following options:

- Computer List
- Collection
- OU (Organizational Unit)
- Security Group

COMPUTER GROUPS		U	M	P	U	T	E	R	T	O	T	A	L
Copy of Windows Computers	1												6
Groups	27												
Users	10												
Windows Computers	1												
*nix Computers	0												
testingLSS	0												
MacOS Computers	0												

Start with **all computers**

1) THEN Only Keep Computers in All Windows Computers

2) THEN Only Keep Computers in All Managed Computers

Multiple rules can be added per computer group. To change already established Computer Groups use the Edit button to add more rules or change the resources targeted.

Computer List

1) THEN 0

Click any specific computers from the provided list of registered machines, then click Save. You may collapse the computer list view by clicking the button that says Select Computers under the Selected Items column.

Filter Rules Results Related Policies

Filter Rules Filters Applied: 2

RULE #	OPERATION	LIST TYPE	SELECTED ITEMS	RUNNING COMPUTER TOTAL				
Start with all computers				1				
1) THEN	Include Computers in	Computer List	WIN- - Select Computers	1				
View Parameters								
	NAME	RESOU...	SYSTE...	DOMAIN	MANU...	MODEL	IPADD...	CREAT...
	<input checked="" type="checkbox"/>	WIN- Computer	x64-based PC	WORKGRO...	Microsoft Corporation	Virtual Machine	:::1	2019-05- 31T09:24:.. 07:00
10 Items per page Showing 1 - 1								
2) THEN	Only Keep Computers in	Collection	Type the name of a filter...	0				

Add Rule Remove All Rules Calculate Rules

Save Cancel

Collection

1) THEN Only Keep Computers in Collection All Windows Computers 1

Enter a collection name, for examples collections can be "All Windows Computers" or "All Managed Computers".

OU (Organization Unit)

1) THEN Only Keep Computers in OU

Active Directory Domains
testing.mydomain.com

Select the OU from the populated domain tree.

Security Group

1) THEN Only Keep Computers in Security Group Type the name of a filter... 0

Search for and select a security group filter.

Local Groups

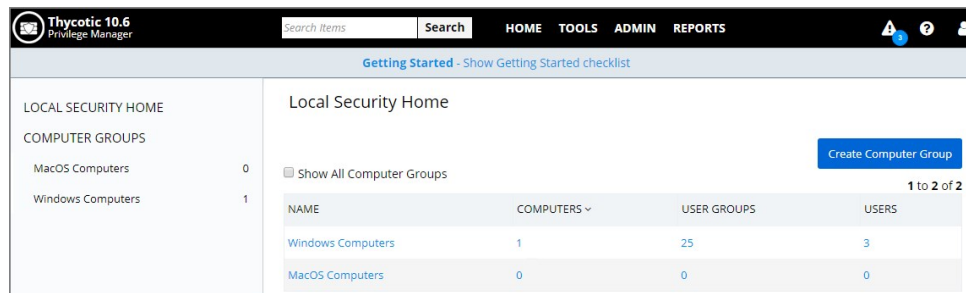
Every Computer Group is divided into Groups and Users. Both **Groups** and **Users** in this context refer to local accounts on the machines that are included in the Computer Group.

To see more details about the Windows Computers Group, either click on Windows Computers in the Local Security Home screen or in the left-hand navigation pane.

The Computer Group page gives you pointers on what can be done with the users and local groups within this set of computers, and provide a high-level overview of the selected computer group based on Local Users, Local Groups, and the number of computers in the group.

Remember: when an agent registers, Local Security will automatically discover the local groups that exist on each machine.

To create a new Group, select the Groups line item listed under the name of the intended Computer Group. At the right side of the page, click the Create Group button.



Enter a Group Name, click **Add Group**.

New Managed Group

Group Name

The new group page opens on the Details tab. Here you can add a description and use Add Members to this group.

Add Members

Select which member(s) to add to this group. Once in the members grid, choose what action is taken on the account by selecting from the options in the "Operation" column.

Type

- Select Type to Add
- Domain User
- Domain Group
- Local User

You can add members to the group by clicking the Add Member button. Choose the type to add from the drop-down (Domain User, Domain Group, Local User) and then select the available options from the local user account list or search for a Domain User Name or Domain Group Name. To finish click Add Member, then Save Changes.

Managing a local group means that you determine which accounts are in that group from the Local Security dashboard. In other words, if a group is being managed, the group membership will remain static and will no longer be able to be updated directly on the endpoint.

If a local group is not managed the Manage Group checkbox is not selected. To Manage the group, click Edit from the Details tab and then check the Manage Group box. Click Save Changes, and Yes to Confirm Navigation. Changes to these settings may take up to 15 minutes to update on your endpoints.

Details Statistics Audit

Group Details Edit

Manage this group by selecting edit. Fill in the following group details and choose which account(s) must be members of this group. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. Additionally, group membership will remain static and will no longer be able to be updated directly on the endpoint.

Manage Group

Group Name doc-test

Members No members

When managing a group, existing members and any that have been added to the policy will appear in the Members table. From the drop-down choose which operation to perform if an account (user) is found on the endpoint. The following options can be selected:

- Ignore if found
- Add if missing
- Remove if found

Group Details

Manage this group by selecting edit. Fill in the following group details and choose which account(s) must be members of this group. Users will be added, removed, or ignored based on the configured membership and will be consistently applied across all endpoints in this computer group target. Additionally, group membership will remain static and will no longer be able to be updated directly on the endpoint.

Manage Group Note: Changes to the local group will not be applied until Manage Group is checked.

Group Name Guests

Description

Members Add Member

MEMBER	TYPE	COUNT	OPERATION	
Guest	Local User	1	Ignore if found	1 to 1 of 1
All Other Users and Groups 0			<div style="border: 1px solid #ccc; padding: 2px;"> Ignore if found Ignore if found Add if missing Remove if found </div>	

The last row defines what action to take on all other users and groups. This ensures exact membership can be defined and any other users or groups can be automatically removed.

Using **Remove if found** for **All Other Users and Groups** instates exact group membership and **Ignore if found** cannot be used on individual accounts that are part of that group. If exact group membership is used, an account that is initially listed as **Ignore if found** switches to **Remove if found** as part of the group membership. Individually specified accounts can be set to Add if missing in those groups.

Note: Once saved, group membership is permanently defined. Updates made directly on the endpoint that break this policy will be immediately reverted.

The **Statistics** tab for a local group highlights some quick visual statistics and links you to relevant reports based on key factors like how many computers from your network are included in this group and whether there have been changes made to the Group's Membership within the specified period. Click on these graphs to drill down into more details.

Note: The reports in the "Related Reports" sections are scoped to only include endpoints in the current computer group. To view reports across all computers, go to the Reports section of the product.



The **Audit** tab is where you will find an audit record of all membership additions and deletions that have been made to your local groups.

Local Users

The Users page listed under your Computer Group shows a list of local users that exist within this Computer Group. The information highlighted by this table includes

1. how many groups each user account is a member of,
2. whether the user account was built-in or user-defined, and
3. whether or not the account itself is managed.

Managing local users in Local Security means that you are setting a password for the account and can rotate the password as desired.

COMPUTER GROUPS				Create User
MacOS Computers	0			1 to 3 of 3
Windows Computers	1			
Groups	25			
Users	3			

USER NAME ^	GROUP COUNT	BUILT-IN	MANAGED
Administrator	1	Built-In	Not Managed
DefaultAccount	1	Built-In	Not Managed
Guest	1	Built-In	Not Managed

To create a new local user, click the Create User button on the Users page, then give your user a name. Click Add User. This will take you to the Details tab for your new user account. To create a user through Local Security, it must be a managed user.

New Managed User

User Name

In Local Security, the most important thing to know about your user accounts is whether or not each is being managed. Managing a local user account means that you are able to rotate the account's password from Local Security's console in Privilege Manager.

To begin managing a user, select Edit in the Account Details box under the Details tab. Click the box next to User Managed to begin. While editing a user you can change the account User Name, add details like the full name of the user or details, you may disable the account or update the schedule that pushes out modifications to endpoints.

The most important part of managing a user is setting a one-time password for the account. This will mean that any user of this account will no longer be able to access this account with their former password, effectively locking a user out of the account unless they contact the Privilege Manager Local Security Helpdesk.

Account Details

Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manger.

User Managed

User Name

Full Name

Description

Account is Disabled

Initial Password

Confirm Password

[Show Advanced](#)

To set a password for this account, enter a new password twice to confirm, then click Save Password. For advanced options, click Show Advanced. To save your changes click Save Changes.

Note: The following settings are all specific to Windows endpoints and will not be displayed for macOS based Computer Groups:

- Account is Disabled
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires

The second box under the User Details tab is called **Password Details**. This option is generally used for privileged accounts that you want fully managed by Privilege Manager. To manage your password this way, select Edit in the Password Details box, then check the Password Management box and edit password length and strength rules. The password on this account will be rotated based on the Update Schedule details (click on the details in blue to edit). Save Changes when complete. The password for the account on each endpoint in the Computer Group will be unique.

Password Details

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.

Password Management

Characters Uppercase
 Numbers
 Lowercase
 Symbols

Password Length characters

Log Password Before Change

Update Schedule Every 30 days at 8:00:00 AM starting Wed Jul 03 2019

If the password is being managed, the Update Schedule will determine when the new password will be applied. Note, the Account Details of the user do NOT need to be managed in order to manage the password on a local account.

The **Groups tab** for a Local Account tells you how many groups and computers the account is on. Clicking on a Group Name from this page will direct you back to the Details tab for that local group.

The **Statistics tab** for a local user account highlights some quick visual statistics and links you to relevant reports based on key factors like how many computers from your network have this user account and whether there have been changes made to the User's Membership within the specified period. Click on the graphs to drill down into more details.

Shared Folder Inventory

To inventory shared folders on computers that have the local security agent installed, enable the shared folder inventory policy. This is an out-of-the-box policy; you do not need to make any configuration changes to this policy.

1. Navigate to **ADMIN | Policies**.
2. Click on the **General** tab.
3. In the Filter name section enter **Shared Folder Inventory Policy**.

The screenshot shows the 'Policies' management interface. At the top left is an 'Add New Policy' button. Below it are navigation tabs for 'Windows', 'Mac OS', 'Client System Settings', 'ActiveX', 'Firewall', and 'General' (which is selected). A table below the tabs has columns for 'ENABLED', 'NAME', and 'FOLDER'. The 'ENABLED' column has a dropdown menu set to 'Any'. The 'NAME' column contains the text 'shared'. The 'FOLDER' column is empty. Below the table, there is a row with 'Not Enabled' in the 'ENABLED' column, 'Shared Folder Inventory Policy' in the 'NAME' column, and 'Windows' in the 'FOLDER' column.

4. Click on **Shared Folder Inventory Policy**.
5. Under the **General** tab select the **Enabled** check box.
6. Click **Save**.

The screenshot shows the configuration page for the 'Shared Folder Inventory Policy'. The title is 'Remote Scheduled Client Command > Shared Folder Inventory Policy'. There are tabs for 'General', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment', with 'General' selected. The 'Enabled' checkbox is checked. The 'Name' field contains 'Shared Folder Inventory Policy'. The 'Description' field contains 'The purpose of this policy is to inventory shared folders on the client.' The 'Command' field contains 'Local Security Shared Folder Inventory Command'. At the bottom are 'Save', 'Cancel', and 'Export' buttons.

Disable Local Guest Accounts

To disable the guest account on computers that have the Local Security Agent installed, enable the **Disable Local Guest Accounts** remote scheduled client command. This is an out-of-the-box policy; you do not need to make any configuration changes to this policy.

To enable the policy:

1. Navigate to **ADMIN | Policies** and select the **General** tab.
2. Type **Disable** into the name column filter and select **Disable Local Guest Accounts** from the list.

Remote Scheduled Client Command > Disable Local Guest Accounts

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name Disable Local Guest Accounts

Description Provisioning policy to disable local Guest accounts on Windows computers.

Command Local Security Provision Command

Back Edit Create a Copy Delete View as XML Export

3. Click **Edit**.
4. Select the **Enabled** checkbox.
5. Click **Save**.

If you wish to customize any aspects of the default behavior, create a copy and edit the copied policy.

The **Disable Local Guest Accounts** policy uses the Local Security task **Disable Guest Accounts**. If you wish to run the task on demand follow these steps:

1. Navigate to **ADMIN | More...** and select **Tasks**.
2. On the **Tasks** tab open the folder tree to **Client Tasks | Local Security**.
3. Select the **Disable Guest Account** task.

Tasks Automation

Find Folder Search

Jobs and Tasks

- Client Tasks
 - Client Item Updates
 - Directory Services
 - Event Maintenance
 - File Inventory
 - Local Security**
 - HelpDesk Tasks
- Infrastructure Scheduled Activities
- Server Tasks

Add New Export

NAME

COM Inventory Task

Collect Windows Logon Events Client Task

Disable Guest Account

Name Disable Guest Account

Run View Edit History

4. Click **Run**.

Logon User Tracking

The Thycotic Local Security Agent collects logon and logoff events from Windows on a schedule configured via the User Logon Inventory policy. The Agent collects logon and logoff events and reports them as inventory data. The **Update Primary User for Collection** task calculates the primary user and the primary user and associated inventory data can then be viewed in the Resource Explorer.

The User Logon Inventory Policy is by default enabled.

Policies

[Add New Policy](#)

Windows Mac OS Client System Settings ActiveX Firewall General

1 to 5 of 5

ENABLED	NAME	FOLDER
Any	user	
Enabled	User Account Policy for 'LSSAdmin' in 'Windows Computers' - v. 1	Managed Users and Groups
Enabled	Password Management Policy for user 'LSSAdmin' on computers in 'Windows Computers'	Managed Users and Groups
Enabled	Local User Inventory Policy	Windows
Enabled	User Logon Inventory Policy	Windows
Enabled	Local User Inventory Policy (MacOS)	Windows

If you wish to customize the schedule or any other policy specification, create a copy of the default policy and edit the settings.

Remote Scheduled Client Command > User Logon Inventory Policy

General Triggers Targets Conditions Advanced Deployment

Enabled

Name User Logon Inventory Policy

Description Updates user logon data on the given schedule.

Command Windows Logon Event Processor

[Back](#) [Edit](#) [Create a Copy](#) [Export](#)

The default update primary user for collection task calculates the primary user on a schedule from inventory data.

1. Navigate to **ADMIN | More...** and select **Tasks**.
2. In the folder tree open Server Tasks | Local Security and search for **Update Primary User for Collection**.

Tasks

Tasks Automation

Find Folder Search

- Jobs and Tasks
 - Client Tasks
 - Client Item Updates
 - Directory Services
 - Event Maintenance
 - File Inventory
 - Local Security
 - HelpDesk Tasks
 - Infrastructure Scheduled Activities
 - Server Tasks
 - Application Control
 - Dev-QA Tasks
 - Directory Services
 - E-mail Tasks
 - File Inventory
 - Foreign Systems
 - Local Security**
 - Security

Export

NAME

Update Primary User

Update Primary User for Collection

Name Update Primary User for Collection

Description Updates the primary user for each computer in the given collection.

[Run](#) [View](#) [Edit](#) [History](#)

3. Customize the settings and schedule by editing the task.
4. Click **Save**.

You can run the **Update Primary User for Collection** task at any time to immediately recalculate the primary user for all computers in the selected collection.

Task > Update Primary User for Collection

General Parameters Schedules

Collection

Days to evaluate 90

Include local logons

Include remote desktop logons

Back Edit Run Task History Create a Copy Export

The Windows Logon Session events can be viewed by opening the Local User/Group Summary report and selecting a computer resource from the list.

Resource Explorer > computer

Summary

Known Data

Events

- Agent Logs
- Application Control
- Local Security
- Windows Logon Sessions

Associations

Name computer

Created Nov 8, 2019, 2:43:22 PM

Modified Nov 8, 2019, 2:43:22 PM

Monitor Resource

Health

- Normal** Policy State
- Warning** Unmanaged Local Administrators by Computer
- Normal** Registration State
- Managed** Managed or Unmanaged State

Back Revoke Agent Trust Delete

Selecting Events | Local Security | Windows Logon Sessions.

Resource Explorer > computer

Summary

Known Data

Events

- Agent Logs
- Application Control
- Local Security
- Windows Logon Sessions

Associations

View Windows Logon Sessions Data Class Report CSV PDF

User	Logon ...	Logoff ...	Minutes	Type
yoururl.co...	11/8/19, 11:30 AM		Incomplete	Remote Interactive

macOS Secure Token

Secure Token is a macOS High Sierra or later account attribute, that is required to be added to a user account before that account can be enabled for FileVault on an encrypted Apple File System (APFS) volume. To help make sure that at least one account has a Secure Token attribute associated with it, a Secure Token attribute is automatically added to the first account to log into the OS login window on a particular Mac. Once an account has a Secure Token associated with it, it can create other accounts which will in turn automatically be granted their own Secure Token.

In order for Privilege Manager to support Secure Token during account creation and for password management, a local account with Secure Token enabled must be created on each macOS endpoint. The credentials for this account must be set as the Secure Token Management Credential.

When the Secure Token Management Credential is configured in the MacOS Agent Configuration, Privilege Manager will use this credential to create a local account on each macOS endpoint. The resulting managed local account will be used during account provisioning and password management to ensure that managed accounts are Secure Token enabled.

If the Secure Token Management Credential is removed in the MacOS Agent Configuration, the agent will use the non-Secure Token enabled method of password management and any new users created/managed will not be Secure Token enabled. Any existing users that are Secure Token enabled will fail to have their password managed because without a Secure Token Management Credential macOS will not allow the agent to manage the password of a Secure Token enabled user.

Note: The agent will ignore attempts to manage the service account. This includes provisioning and password management of the service account via LSS. You should not modify the service account, this includes changing its local password. Doing so may invalidate its configuration and cause the agent to fail password management.

To use the secure token with macOS Agents, the user credential needs to be established and linked to the macOS Agent configuration.

1. Navigate to **ADMIN | Configuration**, select the **Credentials** tab.
2. Click **Add New**.

New User Credential

Credential Change History

Details

Name * macOS User Credential

Description macOS User Credential used for secure token

Settings

Account Name

Password

Confirm Password

Save Cancel Export

3. Under Details enter a Name and Description.
4. Under Settings enter the **Account Name** and **Password** for the macOS user account with Secure Token access.
5. Click **Save**.
6. Navigate to **Admin | Agents**.
7. Select the **MacOS Agents Configuration** tab.
8. Click **Edit**.

Summary Agent Reports Windows Agent Configuration **MacOS Agent Configuration** Installation Codes

MacOS Agent Configuration

These settings control how the Agent is configured on computers running MacOS.

General

Self-Elevation

Allow users to request privilege elevation of applications.

Menu text

Intervals

Send Application Action events every Minute(s)

Task Execution Polling Interval Minute(s)

Application Action Defaults

Quarantine Path

Secure Token Enabled Management Credential

9. In the **Secure Token Enabled Management Credential** field enter the macOS user credential you created in **step 4**.

10. Click **Save**.

Password Management

Local Security allows administrators to manage users and also to manage passwords and password rotation. Managing users, passwords, and rotation scheduled often go hand-in-hand, but not every managed user account also requires password rotation. For example, service accounts are managed, but usually do not have password rotation setup.

Password rotation can also be setup for existing users without having to provision user accounts. The documentation procedure guides you through

- provisioning a local user account to be managed and
- randomizing local user account passwords (password rotation).

Not all steps are required if you just wish to provision a managed account or you already have provisioned users and wish to enable password rotation only.

Note: Password rotation is an option that is not required for all accounts, especially not for service accounts.

1. Navigate to **HOME | Local Security**.
2. From the left navigation frame select **Windows Computers**.
3. Select **Users**.
4. Click **Create User**.
5. Enter a **User Name** and click **Add User**.

Windows Computers > Users > Test Password Disclosure

Details Groups Statistics

Account Details [Edit](#)

Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manger.

User Managed No

Password Details [Edit](#)

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.

Password Management Not Managed

6. For Account Details click **Edit**.
7. Select the **User Managed** checkbox to set the user to be managed.

Windows Computers > Users > Test Password Disclosure

Details Groups Statistics

Account Details

Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manger.

User Managed

User Name Test Password Disclosure

Full Name Test Password Disclosure

Description

Account is Disabled

Initial Password *No password is set [Set Password](#)

[Show Advanced](#)

[Save Changes](#) [Cancel](#)

8. Verify information populated in the User Name and Full Name text fields.
9. Click the **Set Password** button to setup the initial password.

Initial Password *

Confirm Password *

Save Password Cancel

- Enter the **Initial Password**.
- Confirm the Password.
- Click **Save Password**.
- Click **Save Changes**.
- For Password Details click **Edit**.

Password Details

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.

Password Management

Save Changes Cancel

- Select the checkbox for Password Management.

Confirm Manage Password

Please confirm that this account's password will now be managed by Privilege Manager. This means that the password for this user account on all computers in "Windows Computers" will be a unique random password.

Cancel Confirm Manage Password

- Confirm that you want to enable password management for the user.

Password Details

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.

Password Management

Characters

- Uppercase
- Numbers
- Lowercase
- Symbols

Password Length characters

Log Password Before Change

Update Schedule [Every 30 days at 8:00:00 AM starting Tue Nov 05 2019](#)

Save Changes Cancel

- Specify the details for the password management and/or establish a password rotation schedule.

Update Schedule

Begin **On a schedule**

Once
 Daily
 Weekly
 Monthly

Hide Advanced

Delay task for up to (random delay) 0 minute(s)
 Repeat every 0 minute(s) for a duration of 0 minute(s)
 Stop all running tasks at end of repetition duration
 Expire month/day/year hour:minute:second UTC

Starting * 11/4/2019 08:00:00 UTC
Recur every * 1 day(s)

Cancel Save

18. Click Save Changes.

The managed user and password management is now setup.

Details Groups Statistics

Account Details

Editing the account details will apply these details across all computers in this computer group. This action will make the account a "Managed Account" in Privilege Manger.

User Managed ⓘ	Yes
User Name	Test Password Disclosure
Full Name	Test Password Disclosure
Description	
Account is Disabled ⓘ	No
Initial Password	***** Password is managed. View password below.

[Show Advanced](#)

Password Details

Managing the password of this account means that Privilege Manager will be setting and controlling the password on each computer in this computer group.

Password Management	Randomized Passwords View Passwords
Characters	Uppercase, Lowercase, Numbers, Symbols
Password Length	12 characters
Log Password Before Change	Yes
Update Schedule ⓘ	Every 30 days at 8:00:00 AM starting Tue Nov 05 2019

- **All Computers with Managed Passwords:** Lists all computers that have at least one local user with a managed password.
- **Password Disclosure History:** Lists all local and provisioned user's passwords that have been disclosed in a given time frame.
- **Disclosure Summary (Local User):** Lists all local users whose managed password has been disclosed in the given time frame.

Active Directory Synchronization

The following procedures show the steps necessary to set-up Active Directory synchronization in Privilege Manager.

If you already configured the AD Default User Credential skip to the Foreign Systems set-up procedure.

1. Select **Admin I Configuration**.
2. Select the **User Credentials** tab.
3. Edit the Default User Credential or use Add New to create a new user. Set a domain credential with an Account Name and Password that has Administrative access of the Active Directory domain(s).

Details

Details

Name Default User Credential

Description Default User Credential

Settings

Account Name admin

Password *****

[Back](#) [Edit](#)

4. Click **Save** and continue with step 2 in the Foreign Systems set-up procedure.

1. Select **Admin I Configuration**.
2. Select the **Foreign Systems** tab.
3. Select Active Directory Domains.

Configuration

General Discovery Reputation Users Credentials **Foreign Systems** Roles Advanced Authentication

i Foreign Systems can be configured to allow for integration with other environments. It is recommended to configure at least SMTP and either Active Directory or Azure AD. In order to use Secret Server as the password vault please review configuring the Password Vault

NAME	COUNT
Active Directory Domains	0

4. Select the **Add New** button at the top.
5. Enter a fully qualified domain name and a friendly name. Click the **Create** button.

Active Directory Domains

[Add New](#)

Fully Qualified Domain Name * yourdomain.fullyqualified.com

Friendly Name * New Active Directory Domain

[Cancel](#) [Create](#)

NAME	DESCRIPTION	LAST MODIFIED BY	LAST MODIFIED
No Active Directory Domains exist, please create one			

[Back](#)

6. Select the newly created Active Directory Domain entry.
7. On the General tab click **Edit**

Active Directory > TESTPARENT

General Synchronization

Details

Name TESTPARENT

Description

Settings

Credential

URL testparent.thycotic.com

Use LDAPS

Back Edit Create a Copy Delete

8. Verify the **URL** is correct.

Active Directory > TESTPARENT

General Synchronization

Details

Name TESTPARENT

Description

Settings

Credential

URL testparent.thycotic.com

Use LDAPS

Save Cancel

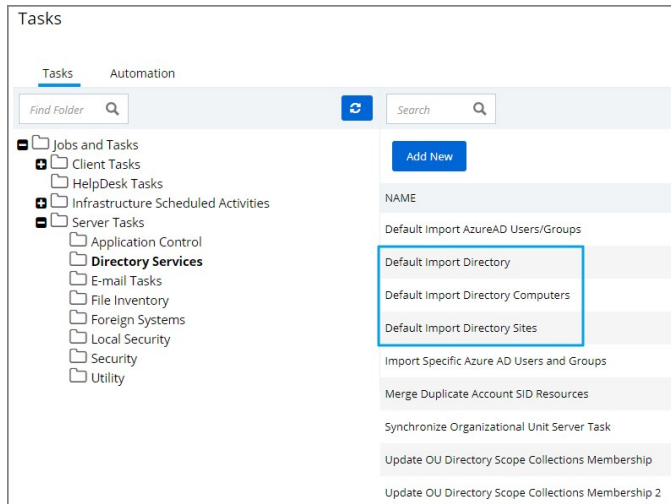
9. Type the name of the user credential to access the domain in the **Credential** field. If the domain uses LDAPS, select the checkbox to

enable. 10. Click **Save**. 11. Once Active Directory is configured a Directory Synchronization task needs to run to import the appropriate data. Select the **Synchronization** tab. 12. From the drop-down select the task you want to perform: * Default Import Directory * Default Import Directory Computers * Default Import Directory Sites 13. Click **Synchronize Active Directory** for each task you select.

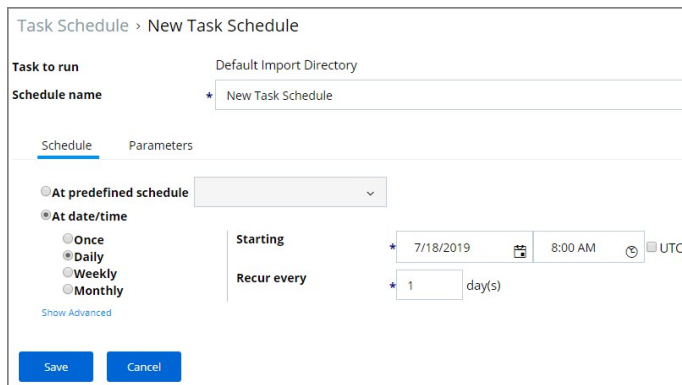
Note: This is a one-time manually triggered synchronization task only.

These tasks can be scheduled and synchronization can be coordinated through one or multiple tasks as needed by each specific environment. As an example, one task may synchronize users once a week, another task could synchronize computers daily, and perhaps a third could synchronize a specific LDAP query for a specific group from Active Directory.

1. Select **Admin | More**.
2. Select the **Tasks** link.
3. Navigate the Jobs and Tasks tree and open **Server Tasks | Directory Services**.
4. Use the following three templates to run a task on demand and to customize schedules based on your company needs:
 - o Default Import Directory
 - o Default Import Directory Computers
 - o Default Import Directory Sites



5. Click **View** on the template task.
6. Click **Create a Copy** and give it a name, click **Create**.
7. Click **Edit** on the newly created task.
 - o On the **General** tab, you can change the task name and customize the Description.
 - o On the **Parameters** tab,
 1. Click **Select Resource** to specify the Directory Id and Directory partner ID.
 2. You may provide a Full sync Query and specify Search Configuration.
 - o On the **Schedules** tab,
 1. Click New Schedule to set-up a customized synchronization schedule.



- o Click **Save**.
8. You may manually run the task now or wait for the schedule to kick in.

You may verify and browse the users and groups that are expected to be imported from Active Directory.

1. In Privilege Manager, navigate to **Admin | Resources**.
2. Expand **Organizational Views**.
3. Expand **Default**.
4. Expand **All Resources**.
5. Expand **Security Principal**.
6. Select **Domain Users**. You should see a list that contains imported Active Directory users.
7. Select **User Group**. You should see a list that contains imported Active Directory groups (other groups may exist in the list as well).

Migrate Local Security Policies

The migration path to the latest Local Security implementation provides an analysis report of issues like missing account credentials, or accounts that are not unique across targets, which can then be remediated before the migration.

Note: Thycotic recommends to use a Professional Services engagement when migrating local security to Privilege Manager 10.7 or newer.

Before any migration is performed, make sure to backup your Privilege Manager database.

Starting with Privilege Manager 10.7 the LLS Migration Readiness Report is available. The report is generated after an upgrade to 10.7 or higher from any previous Privilege Manager version.

To access the LSS Migration Readiness Report, follow these steps:

1. From anywhere in the Privilege Manager console search for LSS Migration.

The screenshot shows a search interface with the following results:

- Number of Results:** 5000
- Role Type Name (2):** Powershell Task (2)
- Report (2):** LSS Migration Task (1/2): Migrate all items. (10/7/19, 2:09 PM - Powershell Task) and LSS Migration Task (2/2): Enable migrated items. (10/7/19, 2:09 PM - Powershell Task)
- Advanced:** Search all items
- Results:**
 - LSS Migration Readiness Report - Drilldown (10/7/19, 2:08 PM - Report) - Displays all daemons running as a domain-based user account
 - LSS Migration Readiness Report (10/7/19, 2:08 PM - Report) - Displays all daemons running as a domain-based user account

The search does show all LSS Migration labeled results found in Privilege Manager. As the image shows, there are two related reports and tasks.

2. Select **LSS Migration Readiness Report**.
3. The report shows a table containing Policy IDs, their Name, and the current migration status.

Reports > LSS Migration Readiness Report

Refresh CSV PDF Search

Drag column here for grouping

Policyid	Policy Name	State
13cf661e-cdd5-4adf-be74-eb4a1d27c665	Disable Local Guest Accounts	Ready for migration.
3d8cb09b-119b-45c3-a4ac-c34e95b291c5	Randomize Administrator Password	Ready for migration.
e72aa7c6-6419-4b6d-a28a-e3d07f45e8db	Cleanup sent Privilege Manager Events (Windows)	Skipped: Is not using a Local Security Command.
26f84672-dcf4-48d5-b8e8-9943486ba68c	Retry errored TMS Events (Windows)	Skipped: Is not using a Local Security Command.
70e817f1-b865-4061-a0fb-84331ad176c2	Perform Resource Discovery (Windows)	Skipped: Is not using a Local Security Command.
eb885e5a-53db-4142-a974-6022482d8078	Update Agent Commands (Windows)	Skipped: Is not using a Local Security Command.
f0d0abc9-6858-45a8-9eee-0cff0590eac1	Basic Inventory (Windows)	Skipped: Is not using a Local Security Command.

Reports > LSS Migration Readiness Report

Refresh CSV PDF Search

Drag column here for grouping

Policyid	Policy Name	State
c72e8356-81f6-47fd-bcb3-788e64fb0dff	User Logon Inventory Policy	Skipped: Is not using a Local Security Command.
3374a6d9-8664-48d4-93fe-af3109671e50	WSUS Client Update Inventory Policy	Skipped: Is not using a Local Security Command.
135f8447-afc7-4b34-b75d-8c7678e11f3e	WSUS Client Update History Events Policy	Skipped: Is not using a Local Security Command.
9e333e6f-ae8f-4fdb-8478-7c65e706f04b	WSUS Agent Inventory Policy	Skipped: Is not using a Local Security Command.
c9e7f6f0-9b08-441d-ab82-5bfea05c6749	Password Management Policy for user 'testdb' on computer...	Skipped: Task has already being migrated.
3a4cc58f-81cb-492c-8750-6c57ab36c703	User Account Policy for 'test26s' in 'Windows Computers' - v...	Skipped: Task has already being migrated.
fb482cea-4098-4646-a9d3-e84cfd30a5ff	User Account Policy for 'testdb' in 'Windows Computers' - v. 1	Skipped: Task has already being migrated.

The migration state can be:

- o Ready for migration.
- o Skipped: Is not using a Local Security Command.
- o Skipped: Task has already been migrated.

4. To learn more about items that are listed as *Ready for migration* click on the item in the table. This opens up the **LSS Migration Readiness Report - Drilldown** report.

Reports > LSS Migration Readiness Report - Drilldown

Parameter Values

Policy Id

[Update](#) [Close Parameters](#)

Filter Report Refresh CSV PDF Search

Drag column here for grouping

Action	Resource Type	Resource Name	Resource RID	For Computer Group	From Resource Id
Will Create	User	Administrator	500	All Windows Computers wi...	00000000-0000-0000-0000...
Will Create	Password Randomization ...	Password Management Po...	N/A	All Windows Computers wi...	3d8c0b9b-119b-45c3-a4ac...

10 items per page 1 - 2 of 2 items

The drilldown report shows the Action to be performed for that particular item during the migration.

For example: The data shown in the image above indicates that two items will be created in Privilege Manager's Local Security. One item is a *User* the other a *Password Randomization* entry. For the user the item is created with **Resource Name** of *Administrator* and the **Resource RID** will be *500*. It further shows that the action will be done **For Computer Group** and **From ResourceID** as indicated.

During the report creating, Privilege Manager will find and resolve conflicts that might be caused by many policies targeting the same computer group with the same user/group, or multiple password rotation policies for the same user. The LSS migration script resolves these conflicts in a way that respects the logic of the initial policy set-up, and comply with the new model for the data.

5. If there aren't any conflicts and all items found can be migrated, use the LSS Migration tasks to migrate and then enable to items pertaining to Local Security. This is a two step process, first migrate then enable.

1. Search for LSS Migration Task (1/2): Migrate all items.

Task > LSS Migration Task (1/2): Migrate all items.

General Parameters Schedules

Name LSS Migration Task (1/2): Migrate all items.

Description

Command LSS Migration Script (1/2): Migrate all items.

[Back](#) [Edit](#) [Run Task](#) [History](#) [Create a Copy](#) [Delete](#) [View as XML](#)

2. After all items are migrated, run the LSS Migration Task (2/2): Enable migrated items.

Task > LSS Migration Task (2/2): Enable migrated items.

General Parameters Schedules

Name LSS Migration Task (2/2): Enable migrated items.

Description

Command LSS Migration Script (2/2): Enable the migrated items.

[Back](#) [Edit](#) [Run Task](#) [History](#) [Create a Copy](#) [Delete](#) [View as XML](#)

Either of these tasks can be edited, to have parameters or schedules defined.

Personas

In Privilege Manager, Personas are collections of privileges for specific roles at an organization. You can assign Personas to users on a specific Computer Group to elevate their identity to perform specific tasks.

For example: A "SQL Administrator" Persona might be created that assigns rights to launch Certificate Manager and SQL Server Configuration Manager. Only users under this Persona would be allowed to execute these applications on your network.

Note: It is recommended to setup Active Directory Synchronization first and run the synchronization task to then easily assign Personas to domain user groups.

To see all your Personas navigate to **Admin | Personas**. From the Windows Privilege Personas page, you can create new Personas and manage existing Personas.

To create a Persona, click Add New Persona from the Personas page. You will be presented with a dropdown list of Persona Templates to choose from.

[Getting Started](#) - [Show Getting Started checklist](#)

Persona Help

When certain users access certain servers they expect to have a certain set of privileges to perform a specific type of task.

For example:

- Web administrators access a web server to perform web server administration tasks such as restarting IIS and recycling App pools.
- SQL Administrators access a server to do common tasks such as ODBC configuration or SQL Server Configuration.

A Persona is an easy way to define which group of privileges specific users have on which computers.

Several Persona templates are available to get started quickly and each Persona can be customized with different behaviors and targets after being created. Once a Persona has been created that Persona will be distributed to the appropriate Managed Computers on a schedule. After it has been deployed the Agent will start applying that Persona for the targeted users.

[Read more about Personas](#)

Windows Privilege Personas

i Personas are a defined set of privileges for a specific role. Users are assigned a persona on a specific resource target or computer that will elevate their identity to perform specific tasks.

[Add New Persona](#)

There are currently no Windows Privilege Personas defined, select "Add New Persona" to create one.

Custom Persona	An empty Persona template for the users to customize based on their needs.
Network Administrators Persona	Automatically elevates applications that are commonly needed to manage network configurations. Elevate DHCP, DNS, and NLB Configuration
Security Administrators Persona	Automatically elevates applications that are commonly needed to manage local users and security settings. Elevate Local User and Groups and Group Policy Object Editor
SQL Administrators Persona	Automatically elevates applications that are commonly needed to manage SQL servers. Elevate Certificate Manager, ODBC Configuration, and SQL Server Configuration Manager
Storage Administrators Persona	Automatically elevates applications that are commonly needed to manage file storage settings. Elevate Disk Defragmentation, Disk Management, iSCSI Connection Configuration, Quota Management, Shared Folders, and Windows Backup
Web Administrators Persona	Automatically elevates applications that are commonly needed to manage web servers. Elevate App Pool Recycling, Certificate Manager, IISReset, and adding TCP Firewall Rules

Select a Persona Template and then provide a Name and Description. Once you are ready to proceed, click Create. If you selected any Persona Template other than Custom Persona then you will have pre-populated Behaviors that you can choose to delete or keep. Otherwise, you will start with a blank Persona.

Windows Privilege Personas

i Personas are a defined set of privileges for a specific role. Users are assigned a persona on a specific resource target or computer that will elevate their identity to perform specific tasks.

[Add New Persona](#)

Add New Persona

Template * -- select a policy template --

-- select a policy template --

Custom Persona

Network Administrators Persona

Security Administrators Persona

SQL Administrators Persona

Storage Administrators Persona

Web Administrators Persona

[Create](#) [Cancel](#)

There are currently no Windows Privilege Personas defined, select "Add New Persona" to create one.

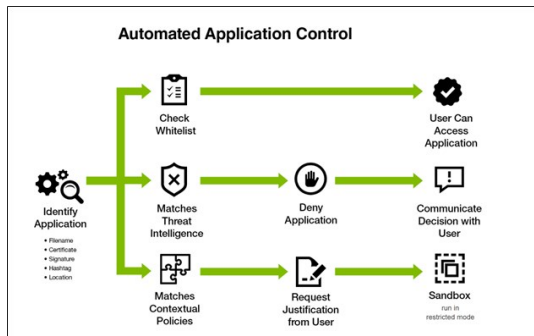
For Persona Settings, you can change the name, description, and whether the Persona will be enabled. For Persona Behaviors, you can click Add Behavior and choose which privilege(s) you want to allow for this Persona. Finally, for Persona

Targets you can choose which Active Directory Domain User Groups this Persona will affect and on which Active Directory Organizational Units this Persona will apply.
Check the Enabled box and click Save to finish creating your Persona.

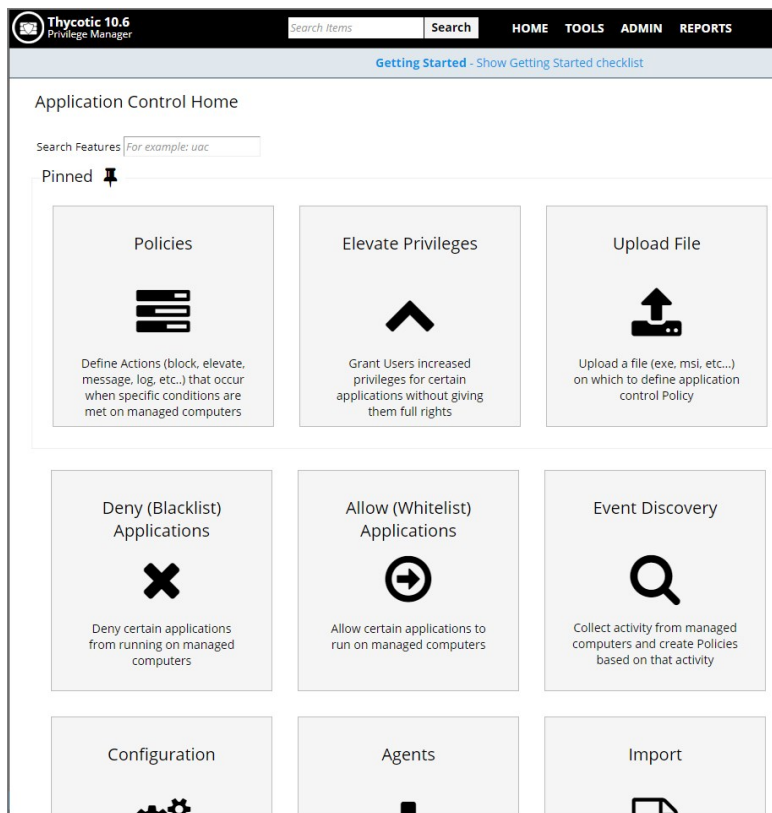
Application Control

Application Control in Privilege Manager allows administrators to manage all application activity on endpoints. Applications requiring admin rights or root access can be automatically elevated if trusted, allowed applications can be whitelisted, and malicious applications can be blocked.

In other words, the key to keeping your organization's employees working both securely and effectively without notable disruptions to their work is by tailoring a robust, role-based Application Control system. On the other hand, managing local administrator and root accounts through Local Security is the fastest way to lock down your network from malicious endpoint attacks that exploit administrator access.



From Privilege Manager's Home click the right-hand Application Control tile to enter your Application Control Dashboard. Tiles provide shortcuts to the different components housed within Application Control. You can pin tiles to the top of your screen to enhance navigation:



In Application Control, layered Policies create the backbone or parameters, that dictate precisely how privileges are accessed across your network. They define what a user can run, and where. A policy is made up of customizable filters that apply an action to specific Computer Groups. In other words, each policy is defined by:

- Filters - What criteria needs to be met to apply this policy?
- Targets - Where should this policy be applied?
- Actions - What should happen to the applications this policy applies to? (i.e. blocked, allowed, etc.)

During the creation of a Policy you will specify Actions and Targets, but Filters are created separately and then assigned to Policies.

Using Policy Templates

Privilege Manager ships with most commonly used policy templates. These can be created new based on a selected template or copied and then customized. These policies are quickly accessed via **Admin | Policies**.

Thycotic also provides templates that do not ship with the product, but that can be downloaded via **Config Feeds** from within the Privilege Manager Console. Once downloaded and installed, customers can access those policy templates via **Admin | More** and clicking on the Folders link. Here a new policy can be created based on a template from a drop-down list. This policy will have associated targets, filters, and actions set, which can be further customized to cover an organization's specific needs. Also refer to [Configuration Feeds](#).

Overview of the Configuration Process

While there are many different types of policies, the setup process must follow these basic steps:

1. Collect File Data - This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed in the Event Discovery | Files page.
2. Create Filters - This step sorts important file data (Events) according to different criteria.
3. Create Policies - This step defines what 1) Actions to perform on applications and the 2) Targets (Locations) for those actions.
4. Assign Filters to Policies - This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be Enabled, or activated.
5. Order your Policies based on priority level - Once your policies are created, the order they execute across your network matters. See the Policy Priority section in this guide for more details.

Collecting File Data

Before Privilege Manager can do anything else for Application Control, it must be able to recognize files or file types in your environment like applications or executables that run. File data can be collected in several ways:

- Event Discovery - Discover active applications on your network by setting up Learning Mode Policies
- File Upload - Directly upload a specific file that you want to target
- Remote File Inventory Task (Windows/macOS) - Scans endpoints directly and imports all file data (both active and inactive files) that exist on the targeted machine(s).

Points to Consider

If you configure Privilege Manager policies incorrectly they could prevent services or programs from starting or running with the proper rights.

Policies are evaluated in order based on the Policy Priority value on the Policy. If a blacklist policy that denies applications is too broad and is set with too high a priority that can prevent other applications from running or letting the user request approval to run.

You can avoid conflicts resulting from incorrectly configured Privilege Manager policies by using the following best practices:

- Always test policies on machines which mirror the production environment before rolling out to production.
- Assign policies that allow processes a lower policy priority number than policies that deny processes.
- Make sure your other policy enforcement settings check boxes are selected or cleared, depending on the aims of your policy.
- Policies that deny processes always exclude the following Application filters:
 - LocalSystem and Service
 - Signed Security Catalog
- You should (almost) never use wildcards in deny policies—they should be considered only after performing extensive testing.

After setting up your first policies, keep in mind that even after you enable them, new policies are not immediately sent to target endpoints. Instead, policies are updated on endpoints via the schedule defined by the Update Applicable Policies task.

1. Go to **Admin | Policies | General Tab** and search for the Update Applicable Policies task from your list of Scheduled tasks:

The screenshot shows the 'Policies' management interface. At the top, there is a blue 'Add New Policy' button. Below it are navigation tabs for 'Windows', 'Mac OS', 'Client System Settings', 'ActiveX', 'Firewall', and 'General' (which is selected). A table lists policies with columns for 'ENABLED', 'NAME', and 'FOLDER'. The first row shows 'Any' in the 'ENABLED' column, 'update applicable' in the 'NAME' column, and an empty 'FOLDER' column. Below this, three rows show 'Update Applicable Policies - Internet Clients (Windows)', 'Update Applicable Policies (Mac OS)', and 'Update Applicable Policies (Windows)', all with 'Enabled' in the 'ENABLED' column and their respective folder names in the 'FOLDER' column.

2. To edit the time scheduled that sets off this task, click the Trigger tab.

The screenshot shows the 'Triggers' tab of the policy configuration. It has tabs for 'General', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment'. Under the 'TRIGGERS (WHEN TO RUN)' section, there is a radio button selected for 'Default: Daily at 12:00:00 AM starting Mon Oct 01 2018 (repeating every 30 minutes for a duration of 24 hours)'. Below this is an 'Add Trigger' button. At the bottom, there are 'Save' and 'Cancel' buttons.

3. Clicking on the existing schedule link in edit mode, allows modifications.

The screenshot shows the 'Triggers' tab in edit mode. It has tabs for 'General', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment'. Under the 'TRIGGERS (WHEN TO RUN)' section, there is a radio button selected for 'Default: Daily at 12:00:00 AM starting Mon Oct 01 2018 (repeating every 30 minutes for a duration of 24 hours)'. Below this is a dropdown menu for 'Begin' set to 'On a schedule'. Under 'On a schedule', there are radio buttons for 'Once', 'Daily' (selected), 'Weekly', and 'Monthly'. The 'Starting' time is set to '10/1/2018 00:00:00' with a UTC checkbox. The 'Recur every' is set to '1 day(s)'. There are checkboxes for 'Delay task for up to (random delay) 30 minute(s)', 'Repeat every 30 minute(s) for a duration of 1 day(s)', and 'Expire'. At the bottom, there are 'Add' and 'Cancel' buttons.

In production environments having a delayed deployment schedule prevents performance issues when adjusting policies and rolling them out across a large number of agents on your network. However, when setting up new policies you may want to immediately activate them on testing endpoints and verify your configurations are working correctly.

Remember to Save any changes you make to activate this schedule.

View Deployment Status

Within a Policy's Detail View, Navigate to the Deployment tab. This will tell you how many computers the policy is already deployed on:

The screenshot shows the 'Deployment' tab of the policy configuration. It has tabs for 'General', 'Triggers', 'Targets', 'Conditions', 'Advanced', and 'Deployment'. Under the 'Policy Deployment' section, there is a description: 'Policies are automatically deployed to targeted managed computers on a schedule. Use the Policy Deployment tab to understand the status of a particular Policy in relation to the end points.' Below this are two buttons: 'Refresh Status' and 'Run Policy Targeting Update'. At the bottom, there are three rows of status information: 'Policy Modified' with a timestamp 'Oct 10, 2019, 8:23:08 AM', 'Total Resources Targeted' with the value '1', and 'Resources with Latest Version' with the value '1'.

Update Policies on an Endpoint using Powershell (prior version 10.7)

On Privilege Manager version prior to 10.7, the fastest way to deploy or update your policies on a specific testing endpoint is by running a simple Powershell script directly on your test machine where a Thycotic Agent is installed.

1. On your endpoint machine, right-click on the Windows Powershell application and select Run as Administrator.
2. Navigate to the Agent directory by entering the following command and then enter:

```
cd "C:\Program Files\Thycotic\Powershell\Arellia.Agent"
```
3. Next type

```
UpdateClientItems.ps1
```
4. Hit enter.

Note: If your policies are not immediately updated, wait a few minutes and try running the script again.

After you've updated your test endpoints, you can try running applications that are targeted by your policies to make sure the policies are configured correctly. You will also see the policy's Deployment tab updated if refreshed.

Agent Event Log Viewer

Another helpful place to look when setting up new policies is your Agent's Event Log Viewer. On your endpoint machine,

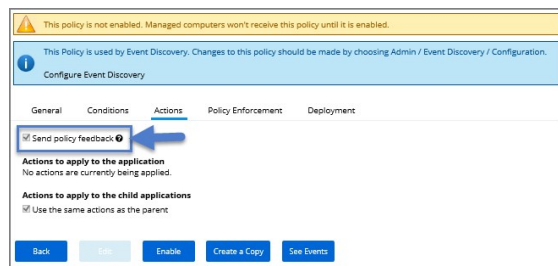
1. Navigate to your Thycotic Agent files. This is usually located in C:\Program Files\Thycotic\Powershell\Arellia.Agent.
2. Right-click on **AgentLogViewer** and select the Log Viewer button. This opens your Agent Event Log Viewer, which shows updates in real time as the agent communicates with the Privilege Manager server. For remote access, Agent logs are also viewable through the Windows Event Viewer.
3. Scroll all the way to the top of the page to see the most recent activity from your Thycotic Agent.
4. Uncheck the Information box on the upper right-hand corner to narrow search results for any Errors and Warning messages that may be occurring. You can also double-click any line item for more detailed information about each event.

Now that you know how to update your endpoints and check to make sure your policies are working, it's time to start building new policies!

At the most basic level, a Learning Mode Policy is a policy that takes no action, it exists only to gather data and you can use the data it gathers for audits or for assigning actions to application events retrospectively. For trials and Proof of Concept (PoC) environments these can be pointed at specific endpoints in order to learn about events that are already happening, or in order to test-run specific applications that you want to quickly introduce into Privilege Manager.

Any Learning Mode Policy will have the Send Policy Feedback check-box checked under the Policy's Actions tab.

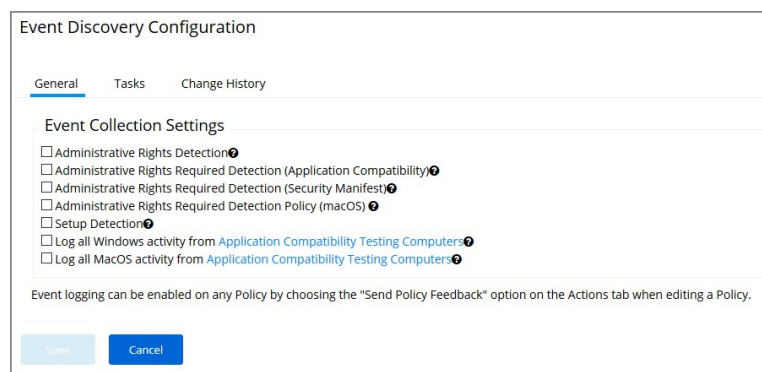
Note: Send Policy Feedback is generally disabled in production environments outside of specific auditing or data-collecting initiatives due to the large amount of data these policies can gather.



Discover Applications that Require Administrator Rights

The most influential applications are those that require administrator credentials to run. For setting up endpoints that are organized by Least Privilege, you can use a Learning Mode Policy to discover all events requiring Administrator rights.

1. From Application Control's Dashboard, navigate to Event Discovery.
2. Click on the Configuration tile.
3. Here, you see a list of pre-configured policies:



4. Click **Edit** and check the boxes of the Collection Settings: **Administrative Rights Detection**, **Administrative Rights Required Detection** (Application Compatibility), **Administrative Rights Required Detection** (Security Manifest), and **Setup Detection**.
5. Click the "?" icons beside these options for explanations of each setting. Each Collection Setting listed here is a Policy that flags any event on endpoints that required a User Account Control (UAC) prompt.

macOS specific Support 10.7 and up

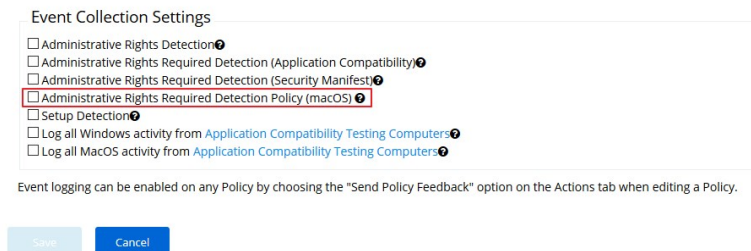
In Privilege Manager versions prior to 10.7, in order to discover applications requiring root access on macOS endpoints, Privilege Manager requires the creating of a policy using 2 filters:

- Executables Declared as Privileged Filter
- Codesign Entitled Elevated Application Filter

In 10.7 this policy is created by default with a single check box on the Discovery Configuration page to enable or disable the policy.

To enable this feature in 10.7 and up:

1. Navigate to **Admin | Event Discovery** and open the **Configuration** tile.
2. Select the checkbox for **Administrative Rights Required Detection Policy (macOS)**.



Discover All Events on Test Endpoints

Another type of Learning Mode Policy will discover all events on targeted machines regardless of whether the application requires Administrator Rights. This policy is used in test environments to quickly target policies at untrusted/unwanted

applications, but is not recommended for production settings.

1. From the **Event Discovery | Configuration** screen select **Edit**.
2. Select the checkboxes for Log all Windows/MacOS activity from Application Compatibility Testing Computers.
3. Simply checking these boxes will not activate this policy. To begin collecting data you must first specify target computers. To do so, click the text **Application Compatibility Testing Computers**.
4. Under the Filter Definition tab, click **Edit**, then **Edit Resources to Include**.
5. Here you can add specific **Resource Filters**, or target machines that your new policies should run on.



6. When target computers are selected, click **Close**, then **Save**.

View Policy Results

To view all feedback, or event, sent from your existing policies with the Send Policy Feedback activity checked, navigate from Dashboard to **Event Discovery | Policy Activity**. Events will be listed in the main section and on the left sidebar you can scope results for certain policies, computers, time frame, etc. You can use this view to assign any events to policies by clicking Assign to Policy under the event listing.

Events

Search Search Events

Type 1 to 10 of 26

Policy Activity ✕

Number of Results 2000

Last Change Date Last 30 Days

Acknowledged 0

Event Type (2)

- Application Action (25) WerFault.exe(Oct 10, 2019, 2:35:03 AM)
- Application Justification (1) Application Action from Event Discovery Audit Elevated Privileges Policy
- Policy (5) Pending Count: 1 | Total Count: 1
- Event Discovery Audit Assign to Policy | Create Filter | View Policy | Acknowledge Pending
- Elevated Privileges Policy (12) cleanmgr.exe(Oct 10, 2019, 2:35:03 AM)
- jing Deny Application Application Action from Event Discovery Audit Elevated Privileges Policy
- Execution Policy (9) Pending Count: 1 | Total Count: 1
- Assign to Policy | Create Filter | View Policy | Acknowledge Pending
- putty.exe(Oct 9, 2019, 6:39:54 PM)
- Application Action from elevate clean Applications - VirusTotal Rating Policy
- Pending Count: 14 | Total Count: 14
- Assign to Policy | Create Filter | View Policy | Acknowledge Pending

View Files

You can also quickly glean any new files found by Privilege Manager in the **Event Discovery | Files Screen**. Distinct from the Policy Events screen view, the Files page only shows files rather than displaying all events attached to current policies.

Events

Search Search Events

Type 1 to 10 of 174

Files ✕

Number of Results 2000

Discovery Date Last 30 Days

Computer (1) This Server (174)

OsName (1) Not Discovered (174)

FileName (167)

- New Loaded Resource WerFault.exe
- 10/9/2019 4:37:13 PM (5) Microsoft® Windows® Operating System by Microsoft Corporation version 6.3.9600.19306
- firefox.exe (3) Assign to Policy | Create Filter
- msiexec.exe (2) taskhost.exe
- WerFault.exe (1) Microsoft® Windows® Operating System by Microsoft Corporation version 6.3.9600.17415
- taskhost.exe (1) Assign to Policy | Create Filter
- Show More (all) cleanmgr.exe
- Microsoft® Windows® Operating System by Microsoft Corporation version 6.3.9600.17415
- Assign to Policy | Create Filter
- notepad++.exe
- Notepad++ by Don HO don.h@free.fr version 7.7.1.0
- Assign to Policy | Create Filter
- gXPEx020iv/ZugsuiBk5d55nng=
- Assign to Policy | Create Filter
- New Loaded Resource 10/9/2019 5:04:55 PM
- Specific details about this resource have not yet been received.
- Assign to Policy | Create Filter
- Agent Utility.exe
- Privilege Manager Agent Utility by Thycotic Software, LLC version 10.6.1080.0
- Assign to Policy | Create Filter
- msiexec (2)

New Loaded Resource

At the beginning of your policy creation process you will see many new events labeled as **New Loaded Resource**. This is because importing files in Privilege Manager is not the same thing as discovering information about the files. Discovery of file details is done by scheduled tasks by default, but if you want to discover file details immediately, do the following:

1. Navigate to **Event Discovery | Files**.

2. Select New Loaded Resource.

Events

Search Search Events

Type	1 to 5 of 5
Files Number of Results 2000	New Loaded Resource 10/9/2019 4:37:13 PM Specific details about this resource have not yet been received. Assign to Policy Create Filter
Discovery Date Last 30 Days	New Loaded Resource 10/9/2019 4:37:13 PM Specific details about this resource have not yet been received. Assign to Policy Create Filter
Computer (1) This Server (5)	New Loaded Resource 10/9/2019 4:37:13 PM Specific details about this resource have not yet been received. Assign to Policy Create Filter
OsName (1) Not Discovered (5)	New Loaded Resource 10/9/2019 4:37:13 PM Specific details about this resource have not yet been received. Assign to Policy Create Filter
FileName (1) New Loaded Resource 10/9/2019 4:37:13 PM (5)	New Loaded Resource 10/9/2019 4:37:13 PM Specific details about this resource have not yet been received. Assign to Policy Create Filter
InternalName (1) Not Discovered (5)	New Loaded Resource 10/9/2019 4:37:13 PM Specific details about this resource have not yet been received. Assign to Policy Create Filter
ProductName (1) Not Discovered (5)	1 to 5 of 5

3. Click one of your New Loaded Resource files.

4. Click Discover Now. This process may take a few minutes. If the file is not discovered, check to make sure your endpoint target resource is running.

Resource Explorer > New Loaded Resource 10/9/2019 4:37:13 PM

Summary	File Name New Loaded Resource 10/9/2019 4:37:13 PM
Known Data	File Hashes sha1: b14a04e9d040c7257181613a4c3f71770da12419
Events	View Reputation VirusTotal.com
Associations	Discovery Status Assigned to agent: ██████████

Back
Discover Now
Delete

[Computer Locations](#) [Policy Events](#) [Similar Files Report](#)

No results.

Note: Files may not be discovered if they have already been deleted in your system.

This topic is about the maximum number of application control events to be stored in Privilege Manager. It explains what causes these events to be stored, how they can be purged from storage, the default setting for maximum number of events to be stored, and how that setting can be modified.

Events

Application control events (which going forward are referred to as "events") are created if you choose to have one or more policies send feedback (from the endpoint to the server) each time the policy is triggered.

To view or set the option to request this policy feedback,

1. Navigate to **Admin | Policies | [policy name in list of policies]**.
2. Click **Edit**.
3. Select the **Actions** tab.

Policy > Blacklist per VirusTotal Rating

General Conditions **Actions** Policy Enforcement Deployment

Send policy feedback ⓘ

Actions to apply to the application

TYPE	ACTION NAME
+ Add Action	

Actions to apply to the child applications

Policy Feedback ×

Enabling send policy feedback means that any time this policy is triggered an event will be sent to the server.

No Action will be applied to child processes

+ Add Action	
--------------	--

Save Cancel

The help tip (shown in the blue message box in the screenshot) for the "Send policy feedback" option explains how events are generated to be stored: "Enabling send policy feedback means that any time this policy is triggered an event will be sent to the server."

4. Select the **Send Policy Feedback** checkbox.
5. Click **Save**.

Storage and Manual Purging of Events

In Privilege Manager versions prior to 10.6, all events continued to be stored unless manually purged. Event storage uses database space and can impact performance of dashboard queries so it is sometimes desirable to purge the stored events.

Manually Purge Events

1. Navigate to **Admin | Configuration** and select the **General** tab

Configuration

General Discovery Reputation Credentials

Policy Targeting ⓘ

Run Policy Targeting Update

Approval Types

Default Execute Application Request Type
Default Offline Execute Application Request Type

Approval Processes

Default Manual Approval Process

Maintenance Settings

- Assign Orphaned Agent Uploads
- Copy of Purge Maintenance - Agent Logs
- Delete Old Performance Counter Events
- Initialize Item Change History
- LSS Migration Task (1/2): Migrate all items.
- LSS Migration Task (2/2): Enable migrated items.
- Purge Maintenance - Agent Logs
- Purge Maintenance - Application Control Events**
- Purge Maintenance - Audit Events
- Purge Maintenance - Completed File Upload Sessions
- Purge Maintenance - Files Undiscovered
- Purge Maintenance - Incomplete File Upload Sessions
- Purge Maintenance - Message History
- Purge Old Computers

1. In the "Maintenance Settings" section of this page, click on "Purge Maintenance - Application Control Events".

Task > Purge Maintenance - Application Control Events

General Parameters Schedules

Name Purge Maintenance - Application Control Events

Description Purges the selected Application Control Event types from the database based upon the time range specified

Back Edit Run Task History Create a Copy View as XML

The Description text explains what this feature does: "Purges the selected Application Control Event types from the database based upon the time range specified".

1. Click on Edit and then navigate to the Parameters tab.

Task > Purge Maintenance - Application Control Events

General **Parameters** Schedules

Enter default parameter values for this task.

- * Purge Application Action events
- * Purge Application Justification events
- * Purge Application Metering events
- * Purge Application Verifier events

Max rows per chunk *

Purge events older than *

Only purge events from these policies None Selected

Here you can select parameters and set values to suit your needs for purging stored events. Click Save after you have completed the desired changes.

Maximum Event Count Option

Privilege Manager version 10.6 includes an option to specify the maximum number of events to be stored (rather than let the system continue to add events to be stored until manually purged). This option is explained below.

Maximum Event Count: Basics

1. Navigate to **Admin I Configuration** and select the **Advanced** tab.

Configuration

General Discovery Reputation User Credentials Foreign Systems Roles **Advanced** Authentication

File Inventory Solution

Collectors

ISO contents filter ⓘ	*.exe;*.cat;*.zip
MSI contents filter ⓘ	*.exe;*.cat
Package contents filter ⓘ	*.exe;*.iso;*.msi;*.cat;*.vhd;*.vmdk;*.zip
VHD contents filter ⓘ	*.exe;*.cat;*.zip
Zip contents filter ⓘ	*.exe;*.cat;*.msi;*.zip

Privilege Manager Server

General

- Allow Agent Certificate Mismatch ⓘ
- Command Timeout ⓘ 180
- Encryption provider ⓘ
- Maximum Event Count ⓘ 25000**
- Max time skew ⓘ 5
- Prevent Legacy Agent Registration (10.4 and older) ⓘ

The "Privilege Manager Server" section of the page shows the option "Maximum Event Count" and its default value, which is 25,000.

You can use the Edit button on this page to change the value of Maximum Event Count. Do bear in mind, however, that storing a large number of events could cause database issues and slow down dashboard queries.

Privilege Manager Server

General

* **Allow Agent Certificate Mismatch** ⓘ

Command Timeout ⓘ

Encryption provider ⓘ * ⓘ

Max time skew ⓘ

* **Prevent Legacy Agent Registration (10.4 and older)** ⓘ

* **Save performance counters** ⓘ

System Secret Vault ⓘ [Configure](#)

* **Validate agent event signatures** ⓘ

Maximum Event Count ⓘ *

Note: In the Cloud version of Privilege Manager, the Maximum Event Count cannot be changed by the user; it is fixed at its default value.

Maximum Event Count: Additional Information

The points below provide additional information about the Maximum Event Count:

- The count value is a total for all policies; it is not a per policy setting.
- The count is treated as a rolling window; if a new event would cause the count to exceed the maximum limit, the oldest event is removed.
- The manual purge, as described in a previous section, is still available.
- As mentioned in the previous section, the Maximum Event Count cannot be changed by the user in the Cloud version of Privilege Manager; there it is fixed at its default value.

In Privilege Manager the option to Send Policy Feedback is the main notification mechanism about application installation and execution on user endpoints. Using Send Policy Feedback is recommended while systems are in Event Discovery and Learning Mode. This helps administrators to gather data, analyze patterns, and then assign actions to application events retrospectively.

It is not recommended to use Event Discovery for all configurable options and all user endpoints all the time. Event Discovery in an established production environment should be targeted to not generate unnecessary and overwhelming amounts of data.

Privilege Manager isn't a SIEM tool, so it shouldn't be capturing events from every endpoint. On the Conditions tab of any policy, users can see what is being targeted. The Application Filters on the policies are typically built with the target file name (and with established naming conventions, the policies and filters are easier to filter and to determine what they are targeting). The Privilege Manager User role can be assigned to the employees who need to audit these policies. That role will give them the ability to read items in Privilege Manager but not make any changes. Those users, as needed, look at the policies to see what's being targeted and can then relay that information to administrators that need to know those details.

Privilege Manager should not be used to audit events on all endpoints, but small scope audit can be done. For those, an elevate policy can be copied and targeted to a specific user, machine, or very small group with send policy feedback. As long as it's a small sample, it shouldn't flood the database with events. This type of audit policy can be assigned to an AD group. Change what user or machine is in that group to change who/what is spot audited. It provides a small example of what is being elevated.

What's First

Privilege Manager includes policies to discover when an end user runs an application that requires administrative rights. Creating policies for any known applications and tasks should be first. Organizations are aware of applications that require elevated permissions to run or install. Collect any files that have already been identified and create policies targeting those applications.

Often different users have different rights on their endpoints, based by division, hierarchy, or other classifications. Privilege Manager can quickly inventory local groups and users. If current permissions are unknown, use Privilege Manager to discover which accounts have administrative permissions on each endpoint. Action can be taken to immediately remove suspicious or unwanted users and groups.

Understanding which users and groups have administrative rights, allows you to properly assess what permissions should exist on an endpoint.

Note: Do not elect to Send Policy Feedback for trusted applications for those specified groups that are cleared to use and install the applications.

Event Discovery

Event Discovery is Privilege Manager's process to determine which applications will require policies.

Based on your use cases, different Event Discovery policies should be enabled. Enable event discovery for the most common use cases like:

- applications that require elevated rights,
- installers, and
- processes that trigger a UAC prompt.

Privilege Manager admins will work through the results of Event Discovery and build policies targeting these applications. Admins will determine if a file should be added to an allow, deny, or elevation policy. If elevated, determine if the file will be silently elevated or if justification, approval, or another workflow will be required.

Add the applications that are discovered to policies with priorities to be triggered before Event Discovery. This will prevent those applications from continuing to be discovered by Event Discovery in the future.

Following this process will naturally clean up the results from Event Discovery.

Never Disable Event Discovery

Event Discovery is not a short process. It's an integral part of Privilege Manager. Once Event Discovery is enabled, it is never disabled.

Even after all policies have been built and all end user needs are met and the local admin groups are empty on all endpoints, you'll still want to know if there are new items that require elevated permissions. Or, after admin rights have been removed, you may want to setup Event Discovery to send feedback if someone runs an application in a context that is unexpected and highly suspicious.

What is discovered and who/which machines Event Discovery targets may change, but Event Discovery will always be used in some capacity.

Event Discovery will never be disabled – you will always want to discover new events that require elevated rights. Consider a maturity plan for Event Discovery.

- Begin by silently discovering applications and creating filters/policies.
- As policies are tightened, add a justification prompt for new items.
- When admin rights have been removed and policies are set, use an approval process or reputation check for newly discovered items.

Event Discovery cannot be sped up. Files will only be discovered when end users initiate a process. If a certain team has an application that is only used at the end of the quarter to finalize business, that application will only be discovered once it is run by the end user.

The scale can be adjusted to ensure the workload is manageable. Start small, understand the workload when the pipeline is slow, then scale to the workload that can be maintained.

Purpose of Event Notifications

Event notifications are helpful and important when administrators want to initially establish policies and to continually monitor the installation and execution of new/unknown applications.

For a production environment it is necessary to know when potentially dangerous applications are installed on a user endpoint. It is not important to be notified every time a white listed application is installed or run on a system.

Note: That means that silent elevation policies do not need an event notification and should not have Send Policy Feedback enabled. Information should only be given on application events that require a follow-up with actions.

Approval and justification policies always generate an event as required for an audit trail. These events cannot be subdued.

Self-elevation, blacklist, and other events on an endpoint triggering UAC are part of the never-ending event discovery process in an organization.

Best Practices

Create policies that are used for a certain amount of time before they are revisited and potentially adjusted for current needs. Target specific systems or user groups with group specific policies. Once those requirements are set, define what events will need a follow-up action in your environment:

- What exceptions can be made if any
- When to use overrides
- What to block
- What to blacklist.

For certain groups of users, it might also be an idea to target a specific machine routinely to use the data to fine-tune any policies that are enforced on the endpoint. Group policies based on existing groupings – AD OUs, AD user groups, SCCM groups, etc.

However, requirements and circumstances are not set in stone and revisiting existing and established policies is part of a best practice approach in PAM.

It is important for administrators to know when (and potentially why) blacklisting policies are triggered. It indicates that employees are violating company policy. However, if this happens a lot, it might indicate that there is a business need for this application and that the blocked software was not fully understood.

Examples

Send Policy Feedback

An UAC override policy allows a user to elevate a program not blocked by a blacklist or elevated by a whitelist, by reentering their password to install/run, is a good candidate for sending policy feedback. It presents an exception to normal execution of programs as an unprivileged user. This type of event logging should be used to identify new programs to add to silent elevation policies if the frequency warrants, or to audit user usage to elevate items they shouldn't to mark them for blocking or follow up action.

Don't Send Policy Feedback

For most business organization it makes no sense to implement a policy that sends feedback when a MS Office product or the company wide instant messaging product is installed or run. For user groups like developers, programming tools are needed and running those should not trigger any notifications.

In Privilege Manager your Policies are evaluated in a certain order for each application that runs. It is important to have an awareness of all policies that are defined and the order in which they are called by the agent. If one policy blocks an application and ends execution before a second policy that was intended to elevate privileges, then only the block will occur.

The Policy Priority setting can be found on the Policies main screen in the left column. By default, policies are ordered according to their priority. You can edit this setting under the General tab after clicking into a policy.

Why Policy Priority Matters

To illustrate the way policies are applied in order, this use case will define two policies to

- block MMC.EXE, but
- allow a specific MMC Snap-in.

Deny MMC.EXE Policy setup

1. We will create a policy at a priority level of 50. This policy will block the execution of MMC.EXE.

Privilege Manager provides a filter to identify the executable mmc.exe. This can be used in this policy to block mmc.exe. Search for mmc.exe from the main screen search tool. Select the filter named Microsoft Management Console (mmc.exe). Review how the Filter is setup. Note that both File Name and File Path parameters are used.

2. Create the deny mmc.exe policy.

1. From the home page, navigate to **ADMIN | Policies | Add New Policy**.
2. Select Windows as a platform, Show All Templates, then Other: Empty Policy as the Template Type.
3. Name the policy Deny Launching MMC Console Application Control Policy.
4. Add a description.
5. Click **Create**.
6. Enable the policy by clicking on the **Enabled** check box.
7. Set the **Policy Priority** value to 50. (This level is not required, only defined for this use case.)
8. Click on the **Conditions** tab.
9. Click on **+ Add Application Target**. Search for the MMC.EXE filter mentioned above.
10. Click on **Add**.
11. You can also set an exception filter to not have this policy apply to Administrators. Search for and select the filter named Administrators (Include Disabled). Click **Add**.
12. Click on **Add Action** under the Actions to apply to the application section.
13. Search for the Application Denied Notification Action. Click **Add**.
14. Click on **Save**. This saves the policy to the policy list accessed from the Home screen – click on Policies to view. Once the policy is delivered to the endpoint agent, mmc.exe will be denied execution for all users without administrator credentials on all target computers. See details on how to deliver policies to the endpoint in the [Sending Policies to Endpoints](#) section.

Once the policy is delivered to the endpoint, test running mmc.exe to see the results.

Allow specific MMC Snap-in

Next, we will create a policy that has a priority of less than 50 and it will allow specific MMC snap-ins. Having a priority less than 50 means this policy will be examined before the Deny MMC Console Application Control Policy.

1. As a short cut to this use case, start by making a copy of the policy we just created. Navigate to the General tab of the policy and click **Create a Copy**. Name the new policy Allow Print Management Plug-in Application Control Policy.
2. Click **Edit** and select the **Enabled** check box.
3. Set the **Policy Priority** value to less than 50. (This level is not required, only defined for this use case.) This means that this policy will be examined prior to the policy that blocks the mmc console. If the conditions are met, printmanagement.msc will run with elevation.
4. Click on the **Conditions** tab. Do not remove the Microsoft Management Console (mmc.exe) filter under Application Targets.
5. Privilege Manager provides a filter to identify the MMC snap-in for Print Management. This can be used in this policy to elevate printmanagement.msc.
 1. Select **Add Inclusion Filter** and search for the printmanagement.msc Commandline Filter.
 2. Click **Add**, then **Save**. This filter will identify the mmc.exe file ONLY if the printmanagement.msc is run.
6. Click on the **Actions** tab.
7. Click **Edit** and delete the existing Application Denied Notification Action by clicking the trash can icon on the right side.
8. Click **Confirm Remove**.
9. Select **Add Action** under the Actions to apply to the application section. Search for and add Add Administrative Rights action.
10. Click **Save**. You will now see your two policies in your Policies List. Once this policy is delivered to the endpoint agent, printmanagement.msc will be elevated with administrative rights.

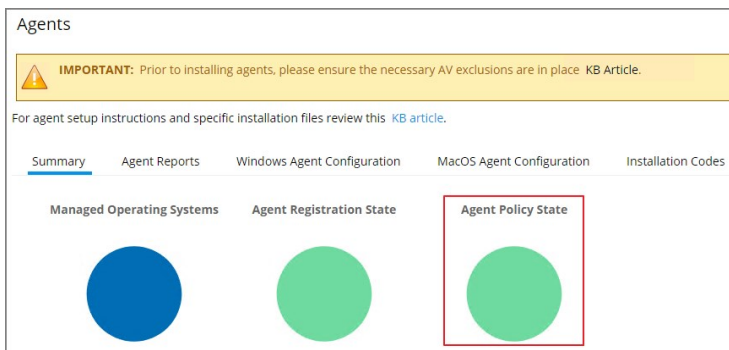
Test this use case

1. Run MMC.EXE from an endpoint where the user is NOT an administrator. This MMC.EXE execution will be denied execution.
2. Run printmanagement.msc from an endpoint where the user is NOT an administrator. This MMC snap-in will run with elevation.
3. Change the Policy Priority of your "Allow Print Management Plug-in Application Control Policy" to Priority 51 rather than priority 49. Repeat the second test.

when you now run printmanagement.msc, the application will be blocked despite your elevation policy. This is why it is crucial to keep the priority levels that are set for your policies in mind and adjust them to meet your intended system requirements.

These are the steps for verifying which policies were received by an agent:

1. Navigate to **ADMIN | Agents** and click on **Agent Policy State**.



2. On the **Agent Policy State - Drilldown** page select the computer, whose policy state you wish to examine.
3. This opens the Resource Explorer for the selected endpoint.

Policy Name	Has a Version of the Policy	Has Current Version of the Policy	Policy Last Modified	Policy Applied to Agent	Agent Last Received Policies
2nd Network Share Elevation Policy - EXE Files	True	True	8/16/19, 11:39 AM	6/4/19, 2:19 PM	11/1/19, 7:16 PM
Add Thycotic Remove Programs	True	True	10/17/19, 11:46 AM	6/4/19, 2:19 PM	11/1/19, 7:16 PM
Application Control Agent Configuration Policy (Windows)	True	True	11/1/19, 8:53 AM	6/4/19, 2:19 PM	11/1/19, 7:16 PM

On the **Policies on Endpoint** tab you can view the policies that the agent on the endpoint has received. The Filter on the **Policy Name** column allows you to search for specific policies.

The columns **Has a Version of the Policy** and **Has Current Version of the Policy** provide information about the version of the policy.

The column **Policy Last Modified** informs when a policy was last changed.

The column **Policy Applied to Agent** specifies when the policy was first received by the agent.

The column **Agent Last Received Policies** informs when the agent last contacted the server to request updates.

Various Privilege Manager policies and filters use Regular Expressions (RegEx) to specify application or file names to match against.

For Privilege Manager all RegEx strings need to be in lowercase. A good resource for testing RegEx is <https://regexr.com>

Special RegEx Characters

The following characters have special meaning in RegEx, and should be used with an escape character when there is a need to represent a literal character.

To perform the escape a \ (backslash) needs to precede the following characters: `+ * ? ^ $. [] () | \ /`

A Privilege Manager Win32 file filters path name does not use the ending directory slash \. RegEx for path names should also not include the ending \

Escape Example

For the literal `(x86)\.netC++` the RegEx is `(x86)\\.netC++`.

Wildcard Example

In RegEx: `*` is a wildcard

File Name Examples

Match with Wildcard before the File Name

Matching anything before the file name and ending with a file type, use a wildcard before the file name.

File Name=`"*eetechcode.exe"` use this in Privilege Manager (`*eetechcode\exe$`)

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- Match TesTeetechcode.exe

Match File Name Containing String and File Type

To match a filename that contains a character string on both sides of the actual file name and that must end with a specific file type:

File Name=`"*eetechcode*.exe"` use this in Privilege Manager (`*eetechcode.*\exe$`)

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- Match eetechcodeTesT.exe
- Match TesTeetechcode.exe

Match with Wildcard at end of File Name and before File Type

Matching a file name with a string that contains anything between the string and the file type.

File Name=`"eetechcode*.exe"` use this in Privilege Manager (`eetechcode.*\exe$`) this is a

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- Match eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

Match with Wildcard in the Middle of Two Strings

Matching a file name beginning with a sting, followed by a wildcard and another string with the last string that includes the file type at the end.

File Name=`"eetech*code.exe"` use this in Privilege Manager (`eetech.*code\exe$`)

Results:

- Match eetechcode.exe
- Match eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

Match with Wildcard at End of File Type

Matching a file name with the wildcard at the end of the file name after the file type, when the filename begins with a string that includes the file type and matches anything after the file type.

File Name=`"eetechcode.exe*"` USE THIS (`eetechcode\exe.*`)

Results:

- Match eetechcode.exe
- NoMatch eetecTesThcode.exe
- NoMatch eetechcodeTesT.exe
- NoMatch TesTeetechcode.exe

File Path Examples

Wildcard at the End of the Path

To match when a wildcard is at the end of the File Path like:

File Path="C:\Program Files\Thycotic\Agents\Agent*" USE THIS ("c:\program files\thycotic\agents\agent.*")

Note: The final backslash has been removed for Privilege Manager.

Also note the system variables like %ProgramFiles% don't work using regex unless %ProgramFiles% is what is shown in the Privilege Manager logs for the event.

Results:

- Match C:\Program Files\Thycotic\Agents\Agent
- NoMatch \Program Files\Thycotic\Agents\Agent
- NoMatch %ProgramFiles%\Program Files\Thycotic\Agents\Agent
- Match C:\Program Files\Thycotic\Agents\Agent\x86

Wildcard in IP Address for Network File Path

To match when a wildcard is used in an IP address for a network File Path like:

File Path="\10.10.10.*\Program Files\Thycotic\Agents\Agent" USE THIS ("\\\\10.10.10.*\program files\thycotic\agents\agents")

Note: The final backslash has been removed for Privilege Manager.

Results:

- No Match C:\Program Files\Thycotic\Agents\Agent
- NoMatch \Program Files\Thycotic\Agents\Agent
- NoMatch %ProgramFiles%\Program Files\Thycotic\Agents\Agent
- NoMatch C:\Program Files\Thycotic\Agents\Agent\x86
- Match \\10.10.10.2\ProgramFiles\Thycotic\Agents\Agent
- Match \\10.10.10.9\ProgramFiles\Thycotic\Agents\Agent

Wildcard for Application Updates for all Users

To match when a wildcard is used several times to target application updates for all Users:

File Path "*"Users%\AppData\Local\Temp\notepad+*\bin" USE THIS (".*\users\\.*\appdata\local\temp\notepad+*\.*\.*\bin\$")

This targets any drive, any user, and multiple versions of an application update. Building filters like these can help streamline Privilege Manager administration since the filter stays current even with new versions coming out and working for all users.

Results:

- Match C:\Users\MarkH\AppData\Local\Temp\notepad++\1.23.59874\bin
- Match C:\Users\DarinS\AppData\Local\Temp\notepad++\1.23.59874\bin
- Match C:\Users\MarkH\AppData\Local\Temp\notepad++\2.56.89457\bin
- Match C:\Users\DarinS\AppData\Local\Temp\notepad++\2.56.89457\bin
- NoMatch C:\Users\MarkH\AppData\Local\Temp\notepad++\2.56.89457
- NoMatch C:\Users\MarkH\AppData\Local\Temp\notepad++\2.56.89457\bin\test

Example Policies

This section contains examples on how to configure and use policies in Privilege Manager.

The following topics are available:

- [Approval Policies](#)
 - [Offline Approvals](#)
 - [HelpDesk Approvals](#)
 - [Setup a Policy to use Google Authenticator](#)
- [Whitelisting Policies](#)
 - [Google Application with File Upload](#)
 - [Microsoft Security Catalog](#)
- [Elevation Policies](#)
 - [UAC Override Policy](#)
 - [Elevating the Privilege Manager Remove Programs Utility Policy](#)
 - [Elevate Applications launched from Network Share Policy](#)
 - [Elevate msi launched from a Network Share](#)
 - [Elevate Applications whose Execution Requires Approval](#)
 - [Elevate Applications that Require User Justification](#)
 - [MS Visual Studio Installations](#)
- [Greylisting Policies](#)
 - [Using a Catch All Policy](#)
 - [Reputation Checking Policies](#)
- [Blocking Policies](#)
 - [Blocking Specific Applications](#)
 - [iTunes with File Upload](#)
 - [Quarantine Specific Malware](#)
 - [Catch-all Blocking Policy](#)
- [macOS Specific Policies](#)
 - [Allow Copy/Install of Applications](#)
 - [Request Application Installation](#)
 - [Application Self-elevation](#)
 - [Use Discovery to Determine if an Application Requires Admin Privileges](#)
 - [Require Justification for Firefox](#)
 - [Deny Photos Application](#)
 - [Adding macOS Agents to a Computer Testing Group](#)
 - [Inventoring .pkg Files](#)

Approval Policies

Approval policies require an end-user justification and use an admin approval workflow.

This policy type requires that people provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition.

The following examples are available:

- [Offline Approvals](#)
- [HelpDesk Approvals](#)
- [Google Authenticator approval](#)

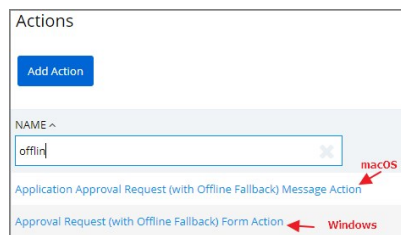
Offline Approvals

Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. If an endpoint is offline, an end user needs a way to also request an approval for an application to continue to execute, for such a situation an Offline Approval process has been implemented.

During an offline approval process a prompt is triggered for a 6-digit numeric pin also called request code. The end user then calls the Help Desk and provides system information to the Help Desk representative. The Help Desk representative generates and provides a 12-character alphanumeric response code for the deployed policy residing on the offline endpoint. Once the end user enters the response code the application execution continues and other actions can be performed, for example adding administrative rights.

The message actions used in the Offline Approval policy are OS specific. Use the action:

- Application Approval Request (with Offline Fallback) Message Action for macOS policies.
- Approval Request (with Offline Fallback) Form Action for Windows policies.

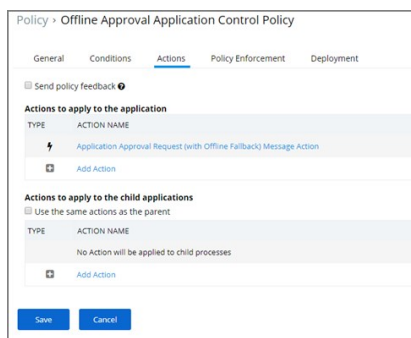


Notifications for approvals can also be issued to mobile devices. Refer to [Mobile App section - Configure the Notification Settings](#)

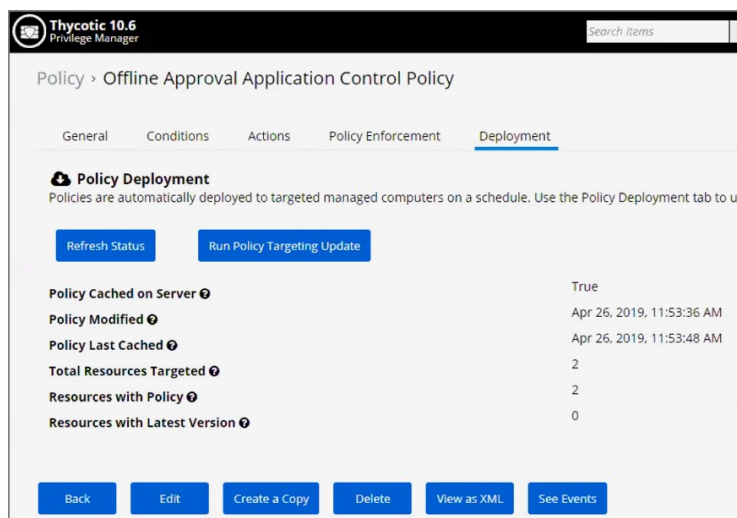
Creating an Offline Approval Policy

For offline approvals to work, a message action supporting offline fallback needs to be configured. This example uses the macOS based message action.

1. Create an Offline Approval Policy, by specifying the specific message action:
 1. Navigate to Actions and click + Add Action.
 2. Select the action **Application Approval Request (with Offline Fallback) Message Action**.



3. Click **Save**.



Endpoint Offline Approval

When the policy created above applies, the system first attempts an online approval request and if the server is unavailable it uses the request and response codes to verify authorization.

1. When trying to install an application that is not explicitly white-listed via policy while offline, the following Application Notice opens:

2. When the system is offline, the following notice opens:

3. Follow the instructions to contact your helpdesk and only click **Generate** when prompted.

4. You will then see:

Provide the information to the helpdesk, they will need the 6-digit code, in this example 191279, to create a response code.

5. Once your helpdesk contact verifies the authenticity of the request, you will be provided a 12-digit **Response Code** that needs to be entered in the text field.
6. Click **Continue** after entering the Response Code.

At this point the application installation should be able to continue.

Privilege Manager Offline Approval

The following procedures provides detailed steps about the offline approval process in the Privilege Manager UI.

1. Navigate to **Tools | Offline Approval**.

2. Click **Select..** to access the list of Computer with open offline approval requests.

Select Computer

NAME	RESOURCE ...	SYSTEMTYPE	DOMAIN	MANUFACT...	MODEL	IPADDRESS	CREATEDD...
DClientWin10	Computer	x64-based PC	WORKGROUP	Microsoft Corporation	Virtual Machine	192.48.128.148	2/6/19, 8:33 AM
DESKTOP-K580UI3	Computer	x64-based PC	WORKGROUP	Microsoft Corporation	Virtual Machine	192.33.85.33	4/8/19, 2:44 PM
DESKTOP-K580UI3	Computer	x64-based PC	alpha.thycotic...	Microsoft Corporation	Virtual Machine	192.33.85.33	4/11/19, 4:22 PM

10 items per page Showing 1 - 10

Select Cancel

- Verify the customer's name is in the list.
- Select the customer's computer from the list and click the **Select** button.

Offline Approval

Search for the endpoint that is requesting a response code. After selecting the endpoint, enter the request code provided by the end user. Press "Generate response code" and provide this response code to the end user to allow their desired application execution to continue.

Select Computer

Computer Name: [DESKTOP-K580UI3](#)

Create New Approval

Request Code

Generate Response Code

- Enter the **Request Code** provided by the customer and click **Generate Response Code**.

Response Code For End User

Provide this response code to the end user. This is a one-time use code based on this computer name and request code.

Computer Name: COM-11-DS-111
Request Code: 391342
Help Desk User: COM-11-DS-111\myname

Response Code
d3ypmy7r86hk

Phonetic Spelling
delta THREE yankee papa mike yankee SEVEN romeo EIGHT SIX hotel kilo

Close

- Read the Response Code back to the customer to enter at the endpoint.

Help Desk Approvals

Privilege Manager enables end users to request elevation and then have their request approved or denied by the helpdesk. You can approve or deny requests via the Privilege Manager console, or forward requests to a third-party ticketing system such as ServiceNow.

Creating a Helpdesk Policy

1. Navigate to **ADMIN | Policies**.
2. Click **Add New Policy**.
3. From the Platform drop-down select **Windows**.
4. From the Policy Type drop-down select **Elevate Application Privileges**.
5. Name the policy, in our example we changed New to Helpdesk.
6. From the Action drop-down select **Require Approval**.

New Policy

Platform: Windows

Policy Type: Elevate Application Privileges

Name: Helpdesk Elevate Process Rights Policy

Description: This policy elevates the security rights for specified applications.

Action: Require Approval

Buttons: Back, Create

7. Click **Create**.

Policy > Helpdesk Elevate Process Rights Policy

Warning: This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General | Conditions | Actions | Policy Enforcement | Deployment | Change History

Common

Policy Name: Helpdesk Elevate Process Rights Policy

Description: This policy elevates the security rights for specified applications.

Platform: Windows

Type:

Folder: Windows Policies

Status

Enabled: ⓘ

Policy Priority: 20 ⓘ

Buttons: Back, Edit, Simple Policy View, Create a Copy, Delete, View as XML, Export, See Events

8. Click **Edit**.
9. Navigate to the **Conditions** tab and add any applications that you want to target with this policy.

Policy > Helpdesk Elevate Process Rights Policy

Warning: When no filters are chosen, this policy will apply to ALL applications.

General | **Conditions** | Actions | Policy Enforcement | Deployment | Change History

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING) ⓘ

No Application Targets Defined

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS) ⓘ

All Windows Computers with Application Control Agent Installed (Target)

Buttons: Back, Edit, Simple Policy View, Create a Copy, Delete, View as XML, Export, See Events

1. Click on the **+** to add an Application Target.
2. Click **Add**.

10. Navigate to the **Actions** tab. Verify the following actions are listed

- **Approval Request From Action**
- **Restrict File Dialogs**
- **Add Administrative Rights**

The screenshot shows the configuration page for the 'Helpdesk Elevate Process Rights Policy'. At the top, there is a yellow warning banner that reads: 'This policy is not enabled. Managed computers won't receive this policy until it is enabled.' Below the banner are several tabs: 'General', 'Conditions', 'Actions' (which is selected), 'Policy Enforcement', 'Deployment', and 'Change History'. Under the 'Actions' tab, there is a checkbox for 'Send policy feedback'. Below that is the section 'Actions to apply to the application', which contains a table with three rows of actions:

TYPE	ACTION NAME
⚡	Approval Request Form Action
⚡	Restrict File Dialogs
⚡	Add Administrative Rights

Below the table is the section 'Actions to apply to the child applications' with a checkbox 'Use the same actions as the parent' and the text 'No actions are currently being applied.' At the bottom of the page are several buttons: 'Back', 'Edit', 'Simple Policy View', 'Create a Copy', 'Delete', 'View as XML', 'Export', and 'See Events'.

11. On the General tab, select the Enable checkbox.

12. Click **Save**.

Once the agent receives the update, users receive a message action dialog to enter their written request in the Reason (required) field which then sends a request to either the Privilege Manager console or integrated Helpdesk.

Workflow

When end users try to open a restricted application, they must enter a reason for needing the application and send it for approval. While the request is being evaluated, whenever end users start the application a status pending message will appear. Once the request has been approved or denied, end users receive an approval or denial.

Approve requests

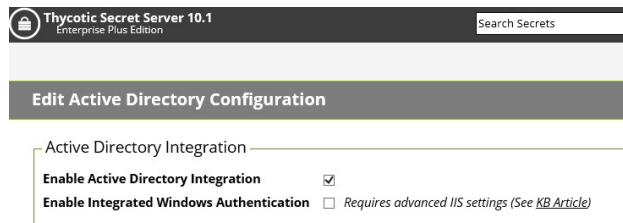
To approve or deny requests in the Privilege Manager Console, go to **TOOLS | Manage Approvals** to view all application requests.

Google Authenticator

This topic describes how to set up a Privilege Manager policy for enabling two-factor functionality with Google Authenticator.

Follow the steps described below to set up a policy for enabling two-factor functionality with Google Authenticator.

1. If you are using the Secret Server login for Privilege Manager, make sure you log in with an Active Directory credential. If you are currently using a Secret Server credential, you need to enable Active Directory Integration.



1. Once you log in with an Active Directory credential go to this URL:

[https://\[ServerName\]/Tms/Account/Totp](https://[ServerName]/Tms/Account/Totp)

2. There you will see the QR Code or Secret to input into Google Authenticator in order for your user account to authenticate on the endpoint. Each user will need to go to this URL after logging in to Secret Server and add this QR Code to their authenticator app. Users can NOT re-use the same authenticator code that they are using for Secret Server.

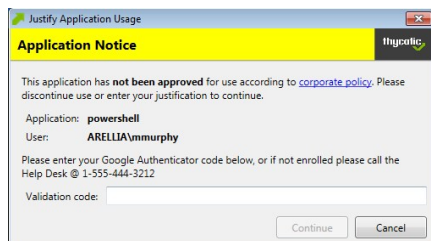
3. After you have done that with one of your user accounts, you need to import an XML file as follows:

1. Access the topic, [XML for Challenge Response Message Actions](#). It contains XML code, copy all that XML code.
2. Go to [https://\[ServerName\]/Tms/PrivilegeManager/#/item/xml/](https://[ServerName]/Tms/PrivilegeManager/#/item/xml/)
3. Paste the contents of the XML code (which you copied in a previous sub-step) into the text field and click the Import button.

4. You can then go to each policy for which you want to enable the two-factor prompt and add the "Challenge/Response Message Action" as an action.

Note: It is not recommended that you do this for ALL applications that are being run.

5. The end users will then see a prompt such as shown below, when they go to launch an application which triggers that action:



NOTE: Justification prompt messages are customizable.


```

</Style>
<!--
<Style x:Key="ImageHeadingBorderStyle" TargetType="Border">
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Padding" Value="8" />
<Setter Property="Background" Value="Black" />
</Style>

<Style x:Key="ImageHeadingStyle" TargetType="Image">
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Source" Value="Images/logo-white.png" />
<Setter Property="Height" Value="18" />
</Style>
-->
<!-- content area -->

<Style x:Key="ContentPanelStyle" TargetType="Panel">
<Setter Property="Margin" Value="8" />
</Style>

<Style x:Key="InformationRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource BaseRichTextBoxStyle}">
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Section x:Key="InformationTextSection" xml:space="preserve">
<Paragraph FontFamily="Segoe UI" FontSize="12"><Run>This application has </Run><Bold>not been approved</Bold><Run> for use according to </Run><Hyperlink Foreground="Blue" TextDecorations="Underline" TargetName=".blank"
NavigateUri="http://www.example.com/policy.html"><Run>corporate policy</Run></Hyperlink><Run>. Please discontinue use or enter your justification to continue.</Run></Paragraph>
</Section>

<Style x:Key="PropertiesPanelStyle" TargetType="Panel">
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Style x:Key="ApplicationNameLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Text" Value="Application:" />
</Style>

<Style x:Key="ApplicationFieldStyle" TargetType="TextBlock" BasedOn="{StaticResource ReadOnlyFieldStyle}">
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Text" Value="{Binding ProcessName}" />
</Style>

<Style x:Key="UserNameLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Text" Value="User:" />
</Style>

<Style x:Key="UserNameFieldStyle" TargetType="TextBlock" BasedOn="{StaticResource ReadOnlyFieldStyle}">
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Grid.Column" Value="1" />
<Setter Property="Text" Value="{Binding UserName}" />
</Style>

<Style x:Key="InstructionRichTextBoxStyle" TargetType="RichTextBox" BasedOn="{StaticResource BaseRichTextBoxStyle}">
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Section x:Key="InstructionTextSection" xml:space="preserve">
<Paragraph FontFamily="Segoe UI" FontSize="12"><Run>Please enter your Google Authenticator code below, or if not enrolled please call the Help Desk @ 1-555-444-3212</Run></Paragraph>
</Section>

<Style x:Key="ChallengeResponsePanelStyle" TargetType="Panel">
<Setter Property="Margin" Value="0,8,0,5" />
</Style>

<Style x:Key="ChallengeLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Text" Value="Request code:" />
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Grid.Column" Value="0" />
</Style>

<Style x:Key="ChallengeTextStyle" TargetType="TextBlock">
<Setter Property="Text" Value="{Binding ChallengeToken,Mode=OneWay}" />
<Setter Property="VerticalAlignment" Value="Center" />
<Setter Property="FontWeight" Value="Bold" />
<Setter Property="FontSize" Value="15" />
<Setter Property="Margin" Value="0,0,0,8" />
<Setter Property="Grid.Row" Value="0" />
<Setter Property="Grid.Column" Value="1" />
</Style>

<Style x:Key="ResponseLabelStyle" TargetType="TextBlock" BasedOn="{StaticResource BaseLabelStyle}">
<Setter Property="Text" Value="Validation code:" />
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Grid.Column" Value="0" />
</Style>

<Style x:Key="ResponseTextBoxStyle" TargetType="TextBox">
<Setter Property="Grid.Row" Value="1" />
<Setter Property="Grid.Column" Value="1" />
<Setter Property="MaxLength" Value="40" />
<Setter Property="Text" Value="{Binding ResponseToken,Mode=TwoWay,UpdateSourceTrigger=PropertyChanged}" />
</Style>

<Style x:Key="ButtonPanelStyle" TargetType="StackPanel">
<Setter Property="Orientation" Value="Horizontal" />
<Setter Property="HorizontalAlignment" Value="Right" />
<Setter Property="Margin" Value="0,8,0,0" />
</Style>

<Style x:Key="ContinueButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonStyle}">
<Setter Property="Content" Value="Continue" />
<Setter Property="Command" Value="{Binding ContinueWithChallengeResponseCommand}" />
<Setter Property="CommandParameter" Value="{Binding ResponseToken}" />
</Style>

<Style x:Key="CloseButtonStyle" TargetType="Button" BasedOn="{StaticResource BaseButtonStyle}">
<Setter Property="Content" Value="Cancel" />
<Setter Property="Command" Value="{Binding CloseCommand}" />
</Style>
</Window.Resources>

<StackPanel Style="{StaticResource MainWindowPanelStyle}"
  adx:WindowHelper.Title="{Binding Result,Source={StaticResource WindowTitle}}">
<Border Style="{StaticResource HeadingBorderStyle}">
  <Grid>
    <Grid.ColumnDefinitions>
      <ColumnDefinition Width="*" />
      <ColumnDefinition Width="Auto" />
    </Grid.ColumnDefinitions>

    <Border Style="{StaticResource TitleHeadingBorderStyle}">
      <TextBlock Style="{StaticResource TitleHeadingStyle}" />
    </Border>
    <Border Style="{StaticResource ImageHeadingBorderStyle}">
      <Image Style="{StaticResource ImageHeadingStyle}"

```

```

        acs:ImageSourceHelper.EncodedImage="{StaticResource EncodedLogoImage}"
        adx:ImageSourceHelper.EncodedImage="{StaticResource EncodedLogoImage}" />
    </Border>
</Grid>
</Border>
<StackPanel Style="{StaticResource ContentPanelStyle}">
<!-- Information of why this dialog needs attention -->
<RichTextBox Style="{StaticResource InformationRichTextBoxStyle}"
    ac:RichTextBoxHelper.Section="{StaticResource InformationTextSection}"
    adx:RichTextBoxHelper.Section="{StaticResource InformationTextSection}" />
<!-- Details about detected process -->
<Grid Style="{StaticResource PropertiesPanelStyle}">
    <Grid.ColumnDefinitions>
        <ColumnDefinition Width="Auto" />
        <ColumnDefinition Width="*" />
    </Grid.ColumnDefinitions>
    <Grid.RowDefinitions>
        <RowDefinition />
        <RowDefinition />
    </Grid.RowDefinitions>
    <TextBlock Style="{StaticResource ApplicationNameLabelStyle}" />
    <TextBlock Style="{StaticResource ApplicationFieldStyle}" />
    <TextBlock Style="{StaticResource UserNameLabelStyle}" />
    <TextBlock Style="{StaticResource UserNameFieldStyle}" />
    </Grid>
<!-- Instruction for Challenge/Response fields -->
<RichTextBox Style="{StaticResource InstructionRichTextBoxStyle}"
    ac:RichTextBoxHelper.Section="{StaticResource InstructionTextSection}"
    adx:RichTextBoxHelper.Section="{StaticResource InstructionTextSection}" />
<Grid Style="{StaticResource ChallengeResponsePanelStyle}">
    <Grid.ColumnDefinitions>
        <ColumnDefinition Width="Auto" />
        <ColumnDefinition Width="*" />
    </Grid.ColumnDefinitions>
    <Grid.RowDefinitions>
        <RowDefinition />
        <RowDefinition />
    </Grid.RowDefinitions>
    <!-- Challenge field -->
    <!-- <TextBlock Style="{StaticResource ChallengeLabelStyle}" />
    <TextBlock Style="{StaticResource ChallengeTextStyle}" />
    <!-- Response field -->
    <TextBlock Style="{StaticResource ResponseLabelStyle}" />
    <TextBox Style="{StaticResource ResponseTextBoxStyle}" />
    </Grid>
<!-- Buttons at bottom -->
<StackPanel Style="{StaticResource ButtonPanelStyle}">
    <Button Style="{StaticResource ContinueButtonStyle}"
        adx:ButtonHelper.IsDefault="true" />
    <Button Style="{StaticResource CloseButtonStyle}"
        adx:ButtonHelper.IsCancel="true" />
</StackPanel>
</StackPanel>
</StackPanel>
</Window>
]]></Xaml>
</CustomXamlExecutionActionContract>

```

Whitelisting Policies

Whitelisting is a type of policy that allows applications to run on your endpoints. You can think of Whitelisting as a neutral policy type because it does not alter an application's default permissions, it merely signifies that the application is "known/trusted" and allowed to run. Although simple whitelisting follows normal, user-level credentials, whitelisted applications are also often paired with Elevation Policies outlined [Elevation Policies](#).

The following examples are available:

- [Whitelist MS Security Catalog](#)
- [Whitelist Google Application with File Upload](#)

Google App with File Upload

In evaluation and production installations, proactive introduction of executables into Privilege Manager can be accomplished with a feature called File Upload. File Upload allows you to quickly introduce a file, then create a Filter and/or a Policy to govern the application. As example, here's how to introduce the Chrome Installer into Privilege Manager and use the file information to whitelist other Google applications.

For this use-case you will need to have access to downloaded Chrome installer files.

1. From the Privilege Manager home screen, navigate to **TOOLS | File Upload**.
2. Click **Browse** and select a file to upload.
3. Click **Upload File**.
4. When the file successfully uploads, click **Go to File Details**.
5. Click *Add to Policy*.
6. In the **Add New Policy** section select **Other: Empty Policy as Policy Type**.
7. Enter a Name, Description.
8. Verify the **Company Name** and **File Must be Signed By Filters**.
9. Click **Create**. This will bring you to your new policy's detail view. Because this is a Whitelisting example, no extra Actions need to be assigned.
10. Navigate to the General tab and select **Edit**.
11. Select **Enabled** to enable the policy.
12. Click **Save**.

MS Security Catalog

This policy uses a built-in filter to whitelist Microsoft's Signed Security Catalog. This filter is often used to dynamically whitelist update items from Microsoft. Whitelisting these executables clears them so they are not effected by any other policy, (i.e. they are allowed to run).

1. Navigate to **Admin | Policies**, then click on Create a New Policy.
2. From the Platform drop-down select **Windows**.
3. Select **Show All Templates as a Policy Type** click **Other: Empty Policy as a Template Type**.
4. Name the policy and add a Description.
5. Click **Create**.
6. Under the Conditions tab choose **Edit**, then **Add Inclusion Filter**.
7. Type **Present in Signed Security Catalog** in the search bar to pull up the correct filter for this use case.
8. Click **Add**.
9. Click **Save**.
10. Navigate to the **General** tab and click **Edit**.
11. Check the **Enabled** box to activate this policy.
12. Click **Save**.

There is no need to add actions under the Actions tab, because these applications are Whitelisted, they are allowed to run with default permissions.

Elevation Policies

Distinct from Whitelisting policies where applications are simply allowed to run with default user level privileges, an Elevation Policy will apply Administrator credentials to specified applications. This type of policy is often paired with Whitelisting to save IT Administrators time when many employees must perform trusted tasks that require Administrator credentials to complete, like installing a trusted application (Adobe) or device (printer).

In Privilege Manager 10.7 the [Restrict File Dialogs](#) action has been added to the product. Thycotic recommends using this action on elevation policies to prevent the misuse of file open and save dialogs for elevated applications.

Topics in this section:

- [UAC Override Policy](#)
- [Elevating the Privilege Manager Remove Programs Utility Policy](#)
- [Elevate Applications launched from Network Share Policy](#)
- [Elevate msi launched from a Network Share](#)
- [Elevate Applications whose Execution Requires Approval](#)
- [Elevate Applications that Require User Justification](#)
- [MS Visual Studio Installations](#)

Setting up ActiveX Policies

Setting up ActiveX Policies – this is to allow add-ins to be installed over a browser (in this example Internet Explorer). To test if ActiveX can be installed without prompting UAC, we can do a test run at <http://pcpitstop.com/>; ActiveX installation is in turn provided at <https://pcpitstop.com/testax.asp>.

Note: You will need to import local group policy definitions before editing your Active-X Group Policy Settings.

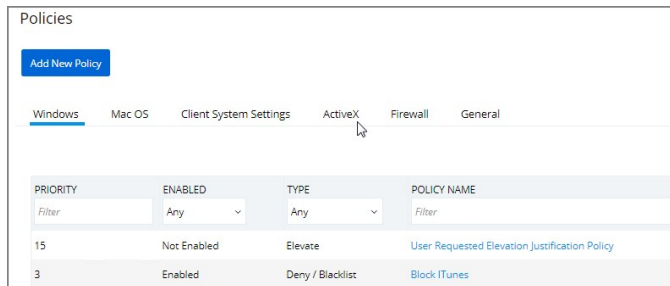
Refer to the Local Security topic, specifically [Manage Local Groups](#).

Overview

1. Create a policy for the list of websites.
2. Create a task to send the policies to the endpoints (this is for Resource Targeting).
3. Test the policy.

Creating the Policy

1. Navigate to **Admin | Policies | ActiveX** tab.



2. Click on **Add New Policy**.

New Policy

Platform: Windows

Policy Type: Active X

Name: PITSTOP Active-X Group Policy Settings

Description: Configure Group Policy settings to apply to computers.

Buttons: Back, Create

3. After the Policy has been created, navigate to the **Other Sites** Tab and add the URL. (protocols included).

Group Policy > PITSTOP Active-X Group Policy Settings

General | Trusted Zone Sites | **Other Sites** | Resource Targeting

Enabled on computers with: At least Windows Vista

Buttons: Add Site

HOST NAME	TRUSTED PUBLISHERS	SIGNED CONTROLS	UNSIGNED CONTROLS
https://www.pcpitstop.com	Silently install	Silently install	Don't install

Other options to consider:

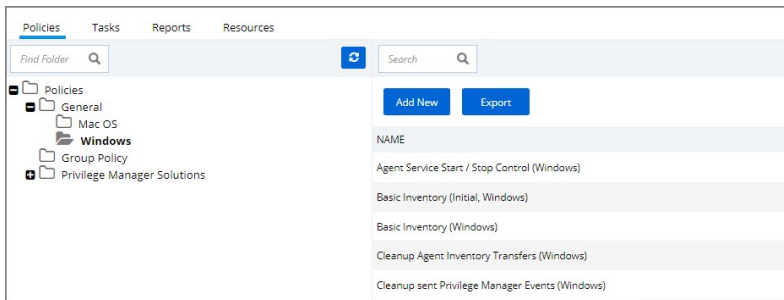
- Ignore Invalid Certificate Date
- Ignore Invalid Certificate Name (CN)
- Ignore Unknown Certification Authority (CA)
- Ignore Wrong Certificate Usage

Task and Resource Targeting

1. Navigate to **ADMIN | More... | Folders**.



2. Open the folder tree and navigate to **Policies | General | Windows**.



3. Click **Add New**.

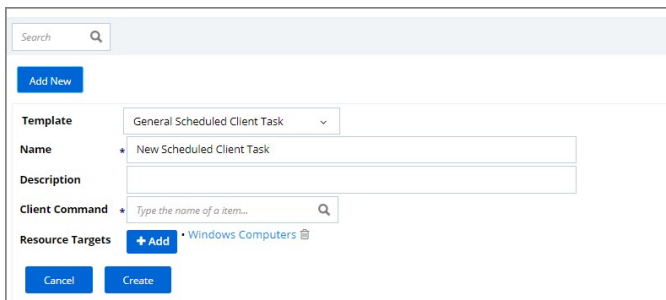
4. From the Template drop-down select **General Scheduled Client Task**.

5. Enter a Name and Description.

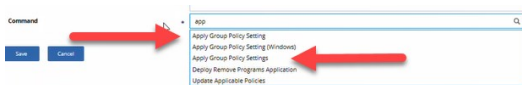
6. For Client Command select **Apply Group Policy Settings**.

7. Verify/add the Resource Target selection.

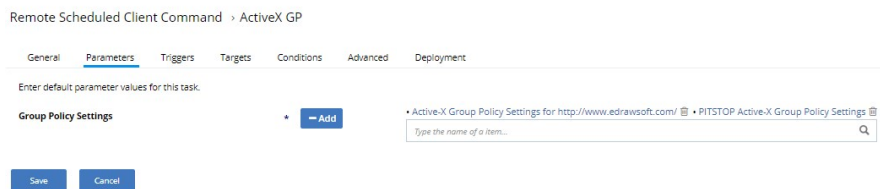
8. Click **Create**.



Note: Apply Group Policy Settings when you have 2 or more ActiveX policies to add to the Parameters.



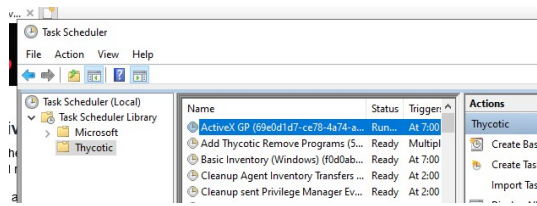
9. Navigate to the **Parameters** Tab to add the ActiveX Policy that you previously created.



Configure the Triggers and the Targets

Proceed to configuring both the Policy and Task functions. On completing this configuration, Privilege Manager Triggers feature will then send the configured task to the targeted endpoint.

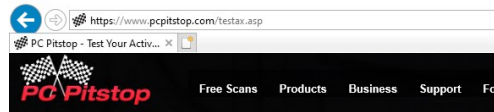
To view the Task, go to the **Task Scheduler**. You must have administrator access to view the task inside Thycotic folder.



Test the Policy

Go to the website: <https://pcpitstop.com/testax.asp> and install the **Add-In**.

You should see the **Time and Date** as seen in the image below.



Test Your ActiveX Installation

This page tests whether you have your browser properly configured to download, auth ActiveX controls, and manipulate them with JavaScript.

When prompted with a certificate, please accept it. The current date and time should e

Tue Jul 30 2019 17:43:13
GMT-0700 (Pacific Daylight
Time)

MS Visual Studio Installations

At the bottom of this page Thycotic is providing a policy and filter xml example, named **ThyPS_Example Elevate MS VisualStudio Installs** with a Policy Priority of 9.

The Policy incorporates six File Specification Filters for Visual Studio Installers, two for 2017 and four for 2019.

Each File Specification Filter incorporates a Certificate Filter for the signing cert and a Win 32 Filter for the targeted file attributes.

Import the XML Example

1. In Privilege Manager, navigate to **ADMIN I Diagnostics** and click **Import Items**.
2. Copy the complete xml example data below.
3. Paste the XML into the new Item(s) area in the Privilege Manager console.
4. Click **Import**.

Background Notes

The four Microsoft initial download files and subsequent two Windows Start Menu target files have been defined as Application targets in this policy.

Policy > ThyPS_Example Elevate MS VisualStudio Installs

This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General
Conditions
Actions
Policy Enforcement
Deployment
Change History

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

- MS.VisualStudio_2019 '\vs_installer.exe' File Specification Filter
- MS.VisualStudio_2019 '\vs_professional_29782508.1558057234.exe' File Specification Filter
- MS.VisualStudio_2019 '\vs_community_29782508.1558057234.exe' File Specification Filter
- MS.VisualStudio_2017 '\vs_installer.exe' File Specification Filter
- MS.VisualStudio_2019 '\vs_enterprise_29782508.1558057234.exe' File Specification Filter
- MS.VisualStudio_2017 '\vs_community.exe' File Specification Filter

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS)

- All Windows Computers with Application Control Agent Installed (Target)

Back
Edit
Simple Policy View
Create a Copy
Delete
View as XML
Export
See Events

If you use this policy in your environment, check frequently to update when new versions are released. Verify if there are any versions of Visual Studio you would need to include for your customization. To cover additional versions, use these filters as a basis and download desired versions from Microsoft.

Additionally, work is needed to sort out what needs elevation when using the application's various modules. Not every Module install was tested with these filters.

The Applications Elevation Policy should be a separate Policy, as it should be located differently in the Policy Stack.

Prior to rolling this out to a production environment, proper testing by a developer should be performed.

XML Example Code

```
<items>
<ApplicationControlPolicyContract xmlns:adc="http://schemas.arellia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arellia.com/dc/ApplicationControl/Policy">
<adc:Description>This policy elevates the security rights for Microsoft Visual Studio All Versions Installers</adc:Description>
<adc:FolderId>60954d0-4bd3-4e2d-92cc-a0069d3d8651</adc:FolderId>
<adc:ItemId>8d22702a-5707-4a14-a8a7-9a0b44223a5c</adc:ItemId>
<adc:Name>ThyPS_Example Elevate MS Visual Studio Installs</adc:Name>
<adc:ProductId>27bedb8a-d37-4d53-b748-bc6651461e4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
<arr:string>pm.policy.type.elevate</arr:string>
</adc:Tags>
<adc:ApplyToResourcesSettings xmlns:d2p1="http://schemas.arellia.com/dc/Resource">
<d2p1:AllowedTargetRoleTypeIds>493435f7-3c17-4c4c-b07f-c23e7ab77811</d2p1:AllowedTargetRoleTypeIds>
<d2p1:RequiresScopingSecurity>false</d2p1:RequiresScopingSecurity>
<d2p1:RestrictionCollectionId>00000000-0000-0000-0000-000000000000</d2p1:RestrictionCollectionId>
<d2p1:ScopingSecurityOperationId>00000000-0000-0000-0000-000000000000</d2p1:ScopingSecurityOperationId>
</adc:ApplyToResourcesSettings>
<adc:DefaultResourceTargetIds>
<arr:guid>e98be43-b0ea-4330-ae49-459e43995bf5</arr:guid>
</adc:DefaultResourceTargetIds>
<adc:Enabled>false</adc:Enabled>
<ApplicationActionIds>
<arr:guid>54bfa458-bd1c-4e1b-8033-9c7888179f6c</arr:guid>
</ApplicationActionIds>
<AppliesToAllProcesses>false</AppliesToAllProcesses>
<ChildApplicationActionIds>
<arr:guid>54bfa458-bd1c-4e1b-8033-9c7888179f6c</arr:guid>
</ChildApplicationActionIds>
<ChildAssociations />
<EndsProcessing>true</EndsProcessing>
<EndsProcessingChild>true</EndsProcessingChild>
<MandatoryFilterIds />
<NegativeFileFilterIds />
<OwnsItemIds />
<PositiveFileFilterIds>
<arr:guid>4481df90-f1ae-4dd4-b641-b7a373908536</arr:guid>
<arr:guid>a7f0812d-6973-4d9f-bce7-89a0007527b3</arr:guid>
<arr:guid>68f19b13-a8e8-4cca-1-b47b-89b630c5casc</arr:guid>
<arr:guid>9f6e20cc-c9ea-4daa-8d12-26161951728a</arr:guid>
<arr:guid>9933ee7-c241-4d23-9c0b-19c41e7ad4a0</arr:guid>
<arr:guid>8f27957-d04d-48d0-974f-0657d51dec12</arr:guid>
</PositiveFileFilterIds>
<Priority>9</Priority>
<SendActionEvent>false</SendActionEvent>
<Stage2Processing>false</Stage2Processing>
</ApplicationControlPolicyContract>
```

```
<Win32ExecFilterContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arrs="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arella.com/dc/ClientItem/" xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arella.com/dc/FileInventory/Filters"/>
<adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159f055</adc:FolderId>
<adc:ItemId>4481d90-f1a8-4d64-b641-b7a373908536</adc:ItemId>
<adc:Name>Win 32 Filter for vs_installer.exe</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
</adc:Tags>
<adc:Company>Microsoft Corporation</Company>
<adc:DriveTypes></DriveTypes>
<adc:ExeProduct>Visual Studio</ExeProduct>
<adc:FileName>(vs_installer.)</FileName>
<adc:FilePath>/>
<adc:FilePathSubdir>true</FilePathSubdir>
<adc:FileVersion>/>
<adc:InternalName>/>
<adc:LocalDiscoveryInterval>0</LocalDiscoveryInterval>
<adc:OriginalFileName>/>
<adc:ProductVersion>/>
<adc:UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExecFilterContract>

<Win32ExecFilterContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arrs="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arella.com/dc/ClientItem/" xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arella.com/dc/FileInventory/Filters"/>
<adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159f055</adc:FolderId>
<adc:ItemId>a7d812d-6973-4d9f-bce7-89a0007527b3</adc:ItemId>
<adc:Name>Win 32 Filter for vs_professional_29782508.1558057234.exe</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
</adc:Tags>
<adc:Company>Microsoft Corporation</Company>
<adc:DriveTypes></DriveTypes>
<adc:ExeProduct>Microsoft Visual Studio Professional</ExeProduct>
<adc:FileName>(vs_professional.)</FileName>
<adc:FilePath>/>
<adc:FilePathSubdir>true</FilePathSubdir>
<adc:FileVersion>/>
<adc:InternalName>/>
<adc:LocalDiscoveryInterval>0</LocalDiscoveryInterval>
<adc:OriginalFileName>/>
<adc:ProductVersion>/>
<adc:UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExecFilterContract>

<Win32ExecFilterContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arrs="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arella.com/dc/ClientItem/" xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arella.com/dc/FileInventory/Filters"/>
<adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159f055</adc:FolderId>
<adc:ItemId>d6d19b19-a6e8-4ca1-b47b-8bb63b9caacc</adc:ItemId>
<adc:Name>Win 32 Filter for vs_community_29782508.1558057234.exe</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
</adc:Tags>
<adc:Company>Microsoft Corporation</Company>
<adc:DriveTypes></DriveTypes>
<adc:ExeProduct>Microsoft Visual Studio Community</ExeProduct>
<adc:FileName>(vs_community.)</FileName>
<adc:FilePath>/>
<adc:FilePathSubdir>true</FilePathSubdir>
<adc:FileVersion>/>
<adc:InternalName>/>
<adc:LocalDiscoveryInterval>0</LocalDiscoveryInterval>
<adc:OriginalFileName>/>
<adc:ProductVersion>/>
<adc:UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExecFilterContract>

<Win32ExecFilterContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arrs="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arella.com/dc/ClientItem/" xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arella.com/dc/FileInventory/Filters"/>
<adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159f055</adc:FolderId>
<adc:ItemId>9f6e2ce8-c9ea-4daa-8d12-26161951728a</adc:ItemId>
<adc:Name>Win 32 Filter for vs_installer.exe</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
</adc:Tags>
<adc:Company>Microsoft Corporation</Company>
<adc:DriveTypes></DriveTypes>
<adc:ExeProduct>Visual Studio</ExeProduct>
<adc:FileName>(vs_installer.)</FileName>
<adc:FilePath>/>
<adc:FilePathSubdir>true</FilePathSubdir>
<adc:FileVersion>/>
<adc:InternalName>/>
<adc:LocalDiscoveryInterval>0</LocalDiscoveryInterval>
<adc:OriginalFileName>/>
<adc:ProductVersion>/>
<adc:UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExecFilterContract>

<Win32ExecFilterContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arrs="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arella.com/dc/ClientItem/" xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arella.com/dc/FileInventory/Filters"/>
<adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159f055</adc:FolderId>
<adc:ItemId>8c27657-d04d-48d0-974f-0657d5fdec12</adc:ItemId>
<adc:Name>Win 32 Filter for vs_community.exe</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
</adc:Tags>
<adc:Company>Microsoft Corporation</Company>
<adc:DriveTypes></DriveTypes>
<adc:ExeProduct>Microsoft Visual Studio Enterprise</ExeProduct>
<adc:FileName>(vs_enterprise.)</FileName>
<adc:FilePath>/>
<adc:FilePathSubdir>true</FilePathSubdir>
<adc:FileVersion>/>
<adc:InternalName>/>
<adc:LocalDiscoveryInterval>0</LocalDiscoveryInterval>
<adc:OriginalFileName>/>
<adc:ProductVersion>/>
<adc:UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>
</Win32ExecFilterContract>

<Win32ExecFilterContract xmlns:adc="http://schemas.arella.com/dc/" xmlns:arrs="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="http://schemas.datacontract.org/2004/07/System"
xmlns:d1p4="http://schemas.arella.com/dc/ClientItem/" xmlns:is="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.arella.com/dc/FileInventory/Filters"/>
<adc:FolderId>bd1b4d12-8dfc-4fcf-a6ea-fe09159f055</adc:FolderId>
<adc:ItemId>8c27657-d04d-48d0-974f-0657d5fdec12</adc:ItemId>
<adc:Name>Win 32 Filter for vs_community.exe</adc:Name>
<adc:ProductId>27bedb8a-db37-4d53-b748-bc6651461fe4</adc:ProductId>
<adc:Tags>
<arr:string>pm.platform.windows</arr:string>
</adc:Tags>
<adc:Company>Microsoft Corporation</Company>
<adc:DriveTypes></DriveTypes>
<adc:ExeProduct>Microsoft Visual Studio</ExeProduct>
<adc:FileName>(vs_community.)</FileName>
<adc:FilePath>/>
<adc:FilePathSubdir>true</FilePathSubdir>
<adc:FileVersion>/>
</Win32ExecFilterContract>
```

```
<InternalName />  
<LocalDiscoveryInterval>0</LocalDiscoveryInterval>  
<OriginalFileName />  
<ProductVersion />  
<UseLocalDiscoveryInterval>false</UseLocalDiscoveryInterval>  
<Win32ExeFilterContract>  
</items>
```

Elevate MSI Files on the Network Share

A wizard generated UNC or Network Share Path Elevation Policy elevates .exe files but not .msi files.

When launching an .msi file, the following command line is executed:

```
C:\Windows\System32\msiexec.exe /i "[path-to-network-share]\file"
```

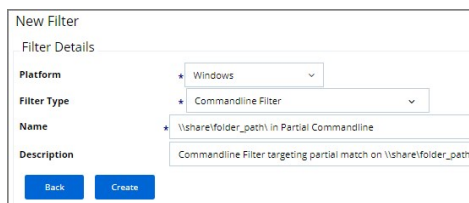
This means that the application is not elevated because the msiexec.exe file is not in the elevated Network Share directory.

This topic details two options for elevating .msi files from a network share.

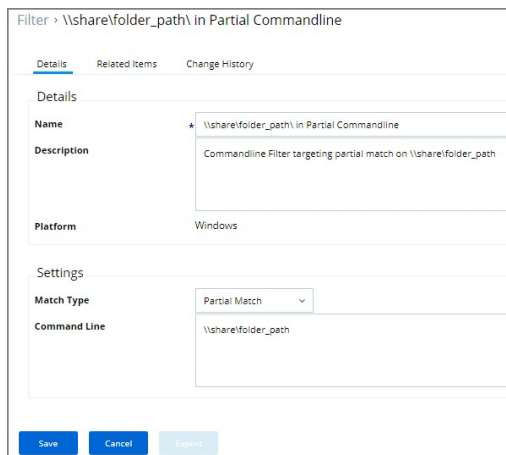
Option 1

In order to enable elevation for .msi files on the network share, a command line filter can be created and added to the Elevation Policy.

1. In the Privilege Manager, navigate to **ADMIN | Filters**.
2. Click **Add Filters**.
3. From the **Platform** pull-down menu, select **Windows**.
4. From the **Filter Type** pull-down menu, select **Commandline Filter**.
5. Give this filter a custom name and description.



6. Click **Create**.
7. On the newly created filter, click **Edit**.
8. Under **Settings | Match Type**, select **Partial Match**.
9. In the Command line field, enter the network share path that needs to be elevated (such as \share\folder_path).



10. Click **Save**.
11. Navigate to your Elevation Policy. On the **Conditions** tab under **Application Targets** add the command line filter you just created.

Now MSI files in the network share will be elevated.

Option 2

An application control policy can be created that targets "msiexec.exe" and uses a secondary file filter as an include only filter.

1. In the Privilege Manager, navigate to **ADMIN | Filters**.
2. Click **Add Filters**.
3. From the **Platform** pull-down menu, select **Windows**.
4. From the **Filter Type** pull-down menu, select **File Specification Filter**.
5. Give this filter a custom name and description.

New Filter

Filter Details

Platform: Windows

Filter Type: File Specification Filter

Name: msi's in \\share\folder_path\

Description: Targets all .msi files located in \\share\folder_path\

Back Create

6. Click **Create**.
7. On the newly created filter, click **Edit**.
8. Under **Settings | File Names**, enter *.msi.
9. For **Path**, enter the approved UNC path.
10. Under **Attributes**, select **Include subdirectories**.

Filter > msi's in \\share\folder_path\

Details Related Items Change History

Details

Name: msi's in \\share\folder_path\

Description: Targets all .msi files located in \\share\folder_path\

Platform: Windows

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names: *.msi

Path: \\share\folder_path\

Drive Types:

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes:

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

11. Click **Save**.
12. Click **Back**.
13. Click **Add Filters**.
14. From the **Platform** pull-down menu, select **Windows**.
15. From the **Filter Type** pull-down menu, select **Secondary File Filter**.
16. Give this filter a custom name and description.

New Filter

Filter Details

Platform: Windows

Filter Type: Secondary File Filter

Name: Secondary File Filter for .msi in \\share\folder_path\

Description: The Secondary File Filter that uses the 'msi's in \\share\folder_path\ File Specification Filter

Back Create

17. Click **Create**.
18. Click **Edit**.
19. Under **Settings**, select **+** **Add** button for Filters and select the file specification filter you just created.

Filter > Secondary File Filter for .msi in \\share\folder_path\

Details Related Items Change History

Details

Name Secondary File Filter for .msi in \\share\folder_path\

Description The Secondary File Filter that uses the .msi's in \\share\folder_path\ File Specification Filter

Platform Windows

Settings

The selected filters will be applied to the target application. The target file is taken from the command-line of the application.

Filters

+ Add msi's in \\share\folder_path\

Type the name of a filter...

Save Cancel Export

20. Click **Save**.

21. Navigate to the Elevation Policy. On the **Conditions** tab under **Application Targets** add the secondary file filter you just created.

MSI files in the network share will be elevated.

Adding the Secondary File Filter created to the Applications Targets on the Conditions tab of the Policy will catch all instances where .msi files are run from \\share\folder_path. Only msiexec.exe will run .msi files, so the Secondary File Filter can be added to an Elevation Policy that has other Application Targets.

An Elevation Policy can be built with this Secondary File Filter as the Application Target and add the built-in Microsoft Installer File Filter as an Inclusion Filter to specifically target msiexec.exe runs an .msi from \\share\folder_path.

Network Share Applications

Many organizations put trusted installers on a network share that employees can use. Those installers can be elevated automatically from the shared network location by assigning an elevation policy to the network share location.

There are different options to elevate rights to launch applications from a network share location.

- One option is to create a file specification filter setting the path for the network share location. Then use that filter in a policy to apply administrative rights to all application launches from that path.
- The other option is to download the Application Control - UNC Elevation Policy Template via Config Feeds and customize the template.

Applying Administrator Rights to a Network Share

Creating the Filter

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **File Specification Filter**. This also allows you to link in hashes or signatures.
 -
5. Enter the name and a description for the filter, for example "network share" and "filter to elevate applications installed from network share".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under **Details**, click **Edit**.
9. Add the Path that points to your Fileshare folder, click **Save**. Use the same UNC path format for both macOS and Windows endpoints.

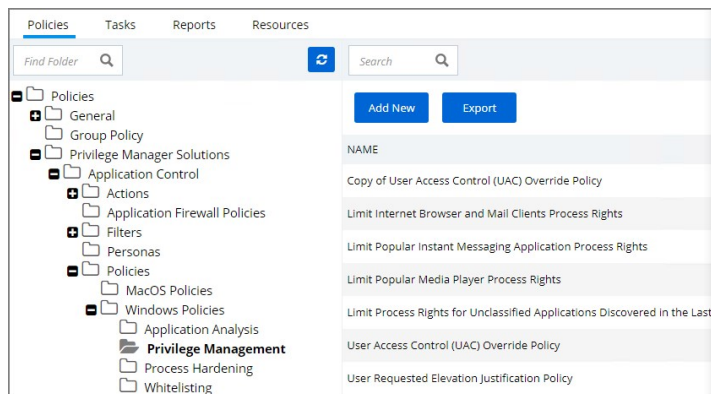
Creating the New Policy

1. Navigate to Policies, click **Add New Policy**
2. In the New Policy screen, select Windows as a Platform.
3. Select Show All Templates as a Policy Type, then Other: Empty Policy.
4. Add a Name and Description, click **Create**.
5. Select the Conditions tab, click **Edit**
6. Click **Add Inclusion Filter**.
7. In the Search bar, type in the name of your new Filter and select it, click **Add**.
8. Click **Save**.
9. Navigate to the Actions tab, choose
10. Click **Edit**.
11. Click **Add Action**.
12. Select the box for **Add Administrative Rights**.
13. Click Add and Save.
14. To activate your policy, click Edit under the General Tab and select the Enable box.
15. Click **Save**.

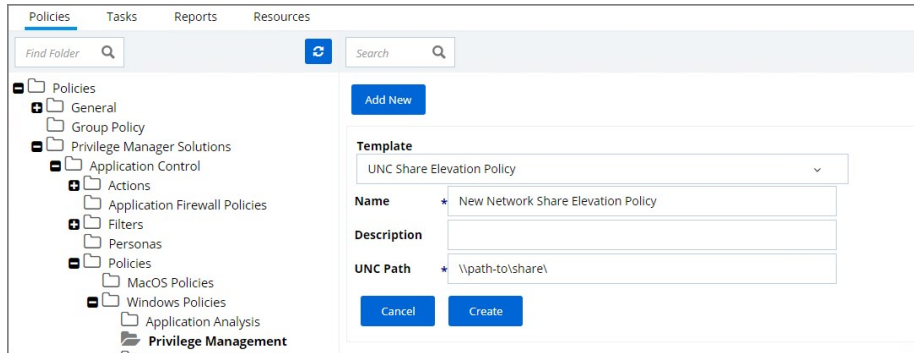
Using the UNC Elevation Policy Template

Use the UNC Elevation Policy Template to create a customized policy that lets you scan a network share and automatically elevates launches of MSI and EXE files from that share.

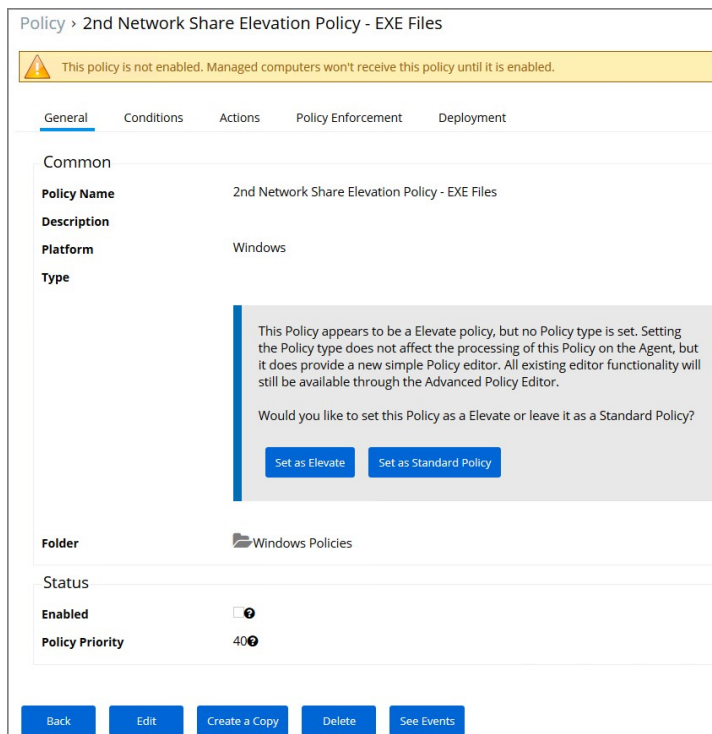
1. Navigate to **Admin | More**, select **Config Feeds**.
2. Find **Privilege Manager Product Configuration Feeds**, click **Select Items**
3. Find **Application Control Solution**, click **Select Items**.
4. Find **Application Control - UNC Elevation Policy Template**, click **Download**. The template is being installed.
5. Navigate to **Admin | More**, click **Folders**.
6. In the folder tree open **Privilege Manager Solutions | Application Control | Policies | Privilege Management**.



7. Click **Add New**.
8. From the template drop-down select **UNC Share Elevation Policy**.
9. Enter a name and description.
10. Enter the UNC Path to the network share. Use the same UNC path format for both macOS and Windows endpoints.



11. Click **Create**.
12. The Policy is created, but needs some attention. Confirm that this is an elevation policy and click **Set as Elevate**.



13. Click **Edit**.
14. Under Status select **Enabled**, if Status is not visible on your page, select **Advanced Policy View**.
15. Change the priority based on how this policy needs to interact with other policies for your organization, click **Save**.

UAC Override Policy

By creating a User Access Control (UAC) Override Policy you can override UAC prompts for end-users. You can create custom messages that require users to submit a reason for requesting administrator rights, which replace UAC prompts for credentials.

Using the Default Policy

1. Navigate to **ADMIN | Policies** and search for **User Access Control (UAC) Override Policy**.

The screenshot shows the configuration page for the 'User Access Control (UAC) Override Policy'. At the top, there is a yellow warning banner stating 'This policy is not enabled. Managed computers won't receive this policy until it is enabled.' Below this is a blue information banner stating 'This item is read-only.' The page has several tabs: 'General', 'Conditions', 'Actions', 'Policy Enforcement', 'Deployment', and 'Change History'. The 'General' tab is active. Under the 'Common' section, the following details are shown:

- Policy Name:** User Access Control (UAC) Override Policy
- Description:** This policy allows standard users to provide a justification for elevation instead of seeing the UAC prompt.
- Platform:** Windows
- Type:** A dialog box is displayed asking 'Would you like to set this Policy as an Elevate or leave it as a Standard Policy?' with two buttons: 'Set as Elevate' and 'Set as Standard Policy'.
- Folder:** Privilege Management
- Status:**
 - Enabled:** A toggle switch is currently turned off.
 - Policy Priority:** 15

 At the bottom of the page, there are several action buttons: 'Back', 'Edit', 'Enable', 'Create a Copy', 'View as XML', 'Export', and 'See Events'.

The UAC Override Policy is a read-only item.

2. Depending on how you wish to run this policy, you either select
 - **Set as Elevate** or
 - **Set as Standard Policy**.

3. If you are in the **Simple Policy View** indicated by only a subset of tabs showing,

The screenshot shows the configuration page for the 'User Access Control (UAC) Override Policy' in the 'Advanced Policy View'. The layout is similar to the previous screenshot, but the tabs are different: 'General', 'Elevation', 'Targets', 'Deployment', and 'Change History'. The 'General' tab is active. Under the 'Common' section, the following details are shown:

- Policy Name:** User Access Control (UAC) Override Policy
- Description:** This policy allows standard users to provide a justification for elevation instead of seeing the UAC prompt.
- Platform:** Windows
- Type:** (This field is empty in this view)
- Folder:** Privilege Management
- Status:**
 - Enabled:** A toggle switch is currently turned off.
 - Policy Priority:** 15

 At the bottom of the page, the action buttons are: 'Back', 'Edit', 'Enable', 'Advanced Policy View', 'Create a Copy', 'View as XML', 'Export', and 'See Events'.

Switch to **Advanced Policy View** by clicking the **Advanced Policy View** button.

Policy > User Access Control (UAC) Override Policy

This policy is not enabled. Managed computers won't receive this policy until it is enabled.

This item is read-only.

General | Conditions | Actions | Policy Enforcement | Deployment | Change History

Common

Policy Name User Access Control (UAC) Override Policy

Description This policy allows standard users to provide a justification for elevation instead of seeing the UAC prompt.

Platform Windows

Type

Folder Privilege Management

Status

Enabled

Policy Priority 15

Back Edit Enable Simple Policy View Create a Copy View as XML Export See Events

4. To edit this policy, you need to make a copy and assign a different name, to do so click the **Create a Copy** button.

5. On the **Conditions** tab you edit the

- o Application Targets
- o Inclusion Filters
- o Exclusion Filters
- o Resource Targets

General | **Conditions** | Actions | Policy Enforcement | Deployment | Change History

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

User Access Control Consent Dialog Detected

INCLUSION FILTERS (ONLY APPLIES WHEN ALL MATCH)

Interactive Users

EXCLUSION FILTERS (DOES NOT APPLY WHEN ANY MATCH)

Administrators (Include Disabled)

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS)

All Windows Computers with Application Control Agent Installed (Target)

6. On the **Actions** tab edit

- o if you want to Send Policy Feedback (as a learning mode/monitoring feature)
- o the Justify Application Elevation Action
- o the Add Administrative Rights Action
- o the Suppress User Account Control Consent Dialog Action

General | Conditions | **Actions** | Policy Enforcement | Deployment | Change History

Send policy feedback

Actions to apply to the application

TYPE	ACTION NAME
	Justify Application Elevation Action
	Add Administrative Rights
	Suppress User Account Control Consent Dialog

Actions to apply to the child applications

Use the same actions as the parent

No actions are currently being applied.

The checkbox **Use the same actions as the parent** lets you establish how to apply actions to child applications.

7. Click **Save**, if you created a copy and made edits.

8. Click the **Enable** button, to enable the policy.

By default the UAC Override Policy has a priority setting of 15.

Elevating the Privilege Manager Remove Programs Utility Policy

If standard users need to be able to use the Remove Program Utility the **Elevate Privilege Manager Remove Programs Utility Policy** needs to be elevated.

1. Navigate to **Admin | Policies**.
2. Search for **Elevate Privilege Manager Remove Programs Utility Policy**.

Policies

[Add New Policy](#)

Windows | Mac OS | Client System Settings | ActiveX | Firewall | General

View 10 rows 1 to 10 of 15

PRIORITY	ENABLED	TYPE	POLICY NAME	FOLDER	ENDS PROCESSING
Filter	Not Enabled	Any	elevate		Any
2	Not Enabled	Elevate	Elevate Privilege Manager Remove Programs Utility Policy	Windows Policies	Ends Processing
20	Not Enabled	Elevate	New Elevate Process Rights Policy	Windows Policies	Continues Processing

3. Click on the policy link **Elevate Privilege Manager Remove Programs Utility Policy**.

Policy > Elevate Privilege Manager Remove Programs Utility Policy

This policy is not enabled. Managed computers won't receive this policy until it is enabled.

This item is read-only.

General | Conditions | Actions | Policy Enforcement | Deployment | Change History

Common

Policy Name Elevate Privilege Manager Remove Programs Utility Policy

Description This policy elevates the security rights for the Privilege Manager Remove Programs Utility

Platform Windows

Type

Folder Windows Policies

Status

Enabled

Policy Priority 20

[Back](#) [Edit](#) [Enable](#) [Simple Policy View](#) [Create a Copy](#) [View as XML](#) [Export](#) [See Events](#)

The default policy is read-only. If you need to customize any policy settings like the Conditions, Actions (like an approval action to run it), Policy Enforcement, or the Deployment, create a copy to make edits.

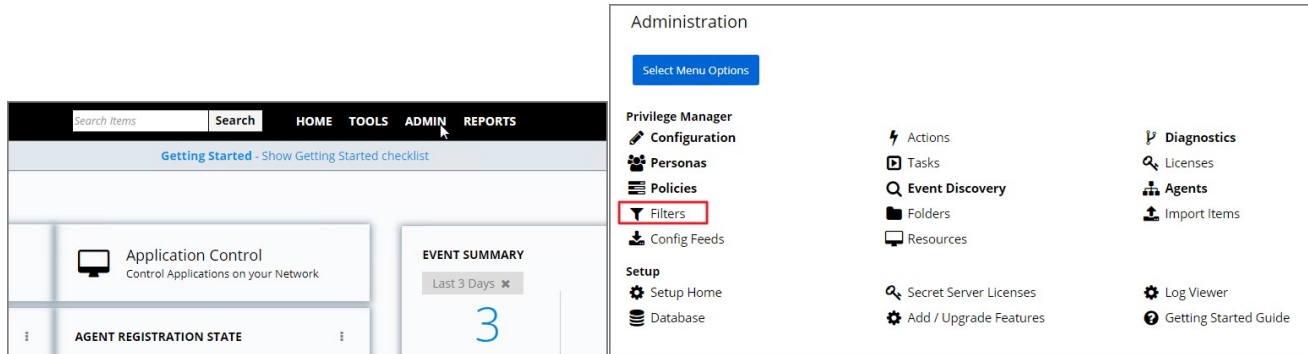
4. Click **Enable** to enable the policy.

Refer to [Using the Remove Programs Utility](#) for further details about the utility set-up and functionality.

Application Execution Requires Approval

This policy type requires a user to provide a justification reason as to why they need to run a process (installer or executable). Then, the reason is submitted to specified managers via Privilege Manager **Tools | Manage Approvals** for approval. It also depends on whether or not the Manual Approval process is used. For instance, if you have configured Service Now as your approval process handler, these approval requests won't appear in the **Tools | Manage Approvals** area. There are several pieces to the Actions in this policy. Because Conditions and Actions are independent, these actions for approval can be applied to any condition. In this use case, we will apply this action to the LICecap creator. First create a filter that will identify the process/executable on which Privilege Manager will act.

1. Navigate to **ADMIN | Filters**.



2. Click on **Add Filter**.

Note: In this use case, we will target the LICecap application (LICecap.exe).

3. From the Platform drop-down select **Windows**.
4. From the Filter Type drop-down select **Blank Win32 Executable Filter**.
5. Add a name and description, click **Create**.

The screenshot shows the 'New Filter' form. The 'Filter Details' section includes the following fields:

- Platform:** Windows (selected in a dropdown menu)
- Filter Type:** Blank Win32 Executable Filter (selected in a dropdown menu)
- Name:** LICecap application
- Description:** (empty text field)

At the bottom of the form, there are two buttons: 'Back' and 'Create'. The 'Create' button is highlighted with a red box.

6. Click **Edit** at the bottom of the page.
7. Enter **LICecap.exe** in the File Name field under File Specifications as well as in the Original filename field under File Details.

Filter > LICEcap.exe filter

Details Related items Change History

Details

Name * LICEcap.exe filter

Description

Platform Windows

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name

File Path

First Discovered

Include subdirectories

Anytime

In the last

0 minute(s)

File Details

To only match files with specific properties in the file details, enter those values in the fields below. A wildcard character

Internal name

Original filename

File version

Product name

Product version

Company name

Copyright

8. Click **Save**.

Create a workflow policy to assign to this filter

1. Navigate to **ADMIN I Policies**.
2. Click on **Add New Policy**.

Policies

Windows Mac OS Client System Settings ActiveX Firewall General

PRIORITY	ENABLED	TYPE	POLICY NAME
Filter	Any	Any	Filter

3. From the Platform drop-down select **Windows**.
4. From the Policy type drop-down select **Show All Templates**.
5. From the Template Type drop-down select **Other: Empty Policy**.
6. Add a name and description, click **Create**.

New Policy

Platform * Windows

Policy Type * Show All Templates

Template Type * Other: Empty Policy

Name * Request Approval Policy

Description

7. Click **Edit** and check the **Enabled** box.

Policy > Request Approval Policy

General Conditions Actions Policy Enforcement Deployment Change History

Common

Policy Name * Request Approval Policy

Description

Platform Windows

Type

Folder Windows Policies

Status

Enabled

Policy Priority * 50

Save Cancel Export

8. Navigate to the **Conditions** tab.
9. Click **Add Application Target**
10. Search and select the **(LICEcap)** filter.
11. Click **Add**.

Policy > Request Approval Policy

General Conditions Actions Policy Enforcement Deployment Change History

Select the applications to control along with any optional criteria.

When no filters are chosen, this policy will apply to ALL applications.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

ADD APPLICATION TARGET

Select an Application Target from the folders below. Use the Application Target page to define more.

View by List

NAME	TYPE
<input type="checkbox"/> LICEcap application	Win32 Exe Filter
<input type="checkbox"/> LICEcap.exe filter	Win32 Exe Filter

Add Cancel

12. Navigate to the **Actions** tab.
13. Click on **add Action**.

Policy > Request Approval Policy

General Conditions Actions Policy Enforcement Deployment Change History

Send policy feedback

Actions to apply to the application

TYPE	ACTION NAME
<input type="checkbox"/>	Add Action

Actions to apply to the child applications

Use the same actions as the parent

TYPE	ACTION NAME
<input type="checkbox"/>	No Action will be applied to child processes
<input type="checkbox"/>	Add Action

Save Cancel Export

14. In the search field, type **Approval**.
15. Select **Approval Request Form Action**.
16. **Add** the action.
17. Click on **Save**.

Policy > Request Approval Policy

General Conditions **Actions** Policy Enforcement Deployment Change History

Send policy feedback

Actions to apply to the application

TYPE	ACTION NAME
ADD ACTION	
View by	List <input type="text" value="approval"/>
<input type="checkbox"/>	NAME
<input type="checkbox"/>	Approval Request Form Action

Actions to apply to the child applications

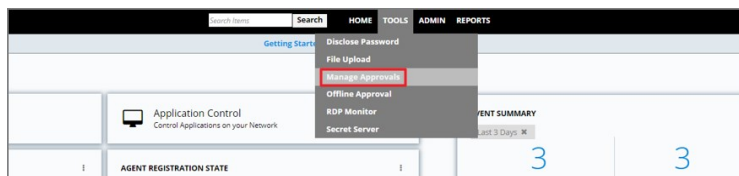
Use the same actions as the parent

TYPE	ACTION NAME
No Action will be applied to child processes	
<input type="button" value="Add"/>	Add Action

18. This saves the policy to the policy list accessed from the Home screen
19. Click on Policies to view from the Home page.
 - o Once the policy is delivered to the endpoint agent LICCap.exe will require the user to enter a justification reason for running this application:
 - o Once the reason is entered by the user, the user clicks Continue to forward to the request to Privilege Manager for approval. On their desktop the Application Notice approval status is marked as Pending.
 - o Finally, a privilege manager user will approve this application request

To Approve Requests

1. Return to the Privilege Manager Dashboard and navigate to **TOOLS | Manage Approvals**.



2. Click the **+** left of the request to view the options for approval.
3. Click on **Approve**.
4. Select **One Time or an allotted time frame for access** and **Manage Approve**.
5. You can now return to the desktop where the user initiated the executable, and you will see the request has been approved.
6. Click on **Continue** and the user is allowed to run that executable.

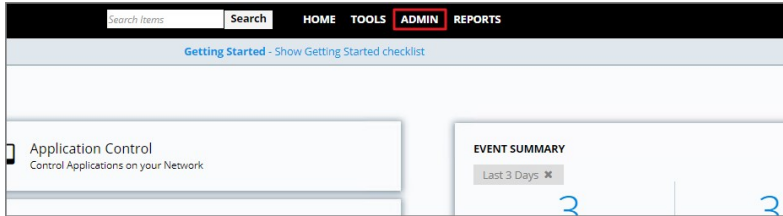
Note: To adjust this policy to apply to specific users or endpoints, Click on the Advanced Policy View in the policy's General tab, then click the Conditions tab to add Inclusion/Exclusion filters and Computer Groups.

User Justification Required to Run

This policy type requires a user to provide a justification for why they need to run an application before elevating with administrator privileges. User Justification refers to the policy action. Since Conditions and Actions are independent, this action can be applied to any condition. In this use case, we will simply apply this action to a specific application.

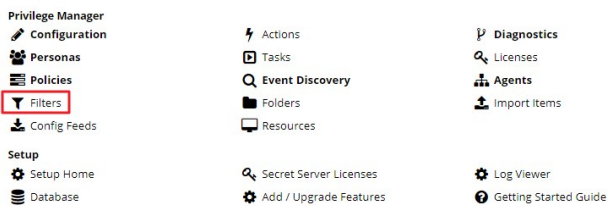
First, create a filter that identifies the application.

1. Navigate to **ADMIN I Filters**.



Administration

Select Menu Options

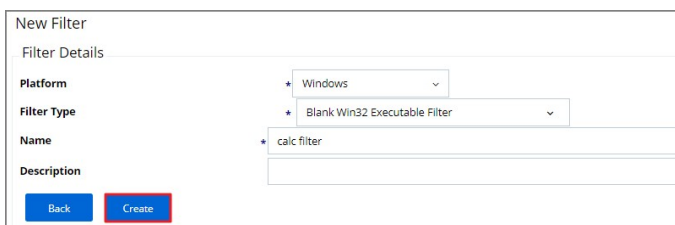


2. Click on **Add Filter**.

Note: In this use case, we will target the Calculator application (calc.exe).



3. From the Platform drop-down select **Windows**.
4. From the Filter type drop-down select **Blank Win32 Executable Filter**.
5. Add a name and description, click **Create**.



6. Click **Edit** at the bottom of the page.
7. Enter **calc.exe** in the File Name field.
8. Click **Save**.

Filter > calc filter

Details Related Items Change History

Details

Name * calc filter

Description

Platform Windows

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name

File Path

Include subdirectories

First Discovered

Anytime

In the last

minute(s)

File Details

To only match files with specific properties in the file details, enter those values in the fields below. A wildcard cha

Internal name

Original filename

File version

Product name

Product version

Company name

Copyright

You can now use this Condition filter in the policy to govern the calc.exe executable.

How to Create the Policy

1. Navigate to **ADMIN I Policies**.
2. Click on Add **New Policy**.

Policies

Windows Mac OS Client System Settings ActiveX Firewall General

PRIORITY	ENABLED	TYPE	POLICY NAME
<input type="text" value="Filter"/>	Any	Any	<input type="text" value="Filter"/>
15	Not Enabled	Elevate	User Requested Elevation Justification Policy

3. From the Platform drop-down select **Windows**.
4. From the Policy Type drop-down select **Elevate Application Privileges**.
5. Add a name and description.
6. From the the Action drop-down select **Request Justification**.
7. click **Create**.

New Policy

Platform * Windows

Policy Type * Elevate Application Privileges

Name * New Elevate Process Rights Policy

Description This policy elevates the security rights for specified applications.

Action Request Justification

8. Click **Edit** and check the **Enabled** box.

Policy > New Elevate Process Rights Policy

This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General | Conditions | Actions | Policy Enforcement | Deployment | Change History

Common

Policy Name * New Elevate Process Rights Policy

Description This policy elevates the security rights for specified applications.

Platform Windows

Type Elevate

Folder Windows Policies

Status

Enabled

Policy Priority * 20

Simple Policy View | Save | Cancel | Export

9. Navigate to the **Conditions** tab.

10. Click **Add Application Target**

11. Search and select the **Calc** filter.

12. Click **Add**

Policy > New Elevate Process Rights Policy

This policy is not enabled. Managed computers won't receive this policy until it is enabled.

General | **Conditions** | Actions | Policy Enforcement | Deployment | Change History

Select the applications to control along with any optional criteria.

When no filters are chosen, this policy will apply to ALL applications.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

ADD APPLICATION TARGET

Select an Application Target from the folders below. Use the Application Target page to define more.

View by List

NAME	TYPE
<input type="checkbox"/> calc filter	Win32 Exe Filter

13. Click on **Save**.

Note: This saves the policy to the policy list accessed from the Home screen – click on Policies to view from the Home page. Once the policy is delivered to the endpoint agent, calc.exe will require the user to enter a justification reason for running this application. This policy will be applied to all users on all computers.

To adjust this policy to apply to specific users or endpoints

1. Click on **Advanced Policy** view in the policy's General tab.
2. Navigate to the **Conditions** tab
3. Click add **Inclusion/Exclusion filters** and **Computer Groups**

The user will see a justification message as a result of the policy. When the user adds a reason, they will then click the **Continue** button and the application is allowed to execute.

Note: You can then view a user's provided reasons in Privilege Manager on the **ADMIN | Events Discovery | Policy Activity** page or under **Reports | Application Justification Summary Details Report**.

Monitoring Policies

Monitoring or Greylisting Policies apply to any unknown applications that will attempt to run in your environment. It is important to discover unknown applications and determine whether to let them run or whether they are harmful. Greylisting provides a system for discovering the unknowns and adding an action that hinges on a reputation check.

The following examples are available:

- [Catch-All Policy](#)
- [Reputation Checking](#)

Catch-All Policy

A useful Learning Mode Policy to set up in Production environments is called a Catch-All Policy. This type of policy will gather information on any executables in your environment that are not satisfied by other Privilege Manager policies.

1. Navigate to **ADMIN | Policies** and click **Add New Policy**.
2. From Policy Type drop-down select **Show All Templates**.
3. For POC and testing environments from Template Type drop-down, select **Other: Empty Policy Targeting Test Computers**.
4. Name the policy *Catch-All Policy*, and add a description.
5. Click **Create**.
6. Click **Edit**.

This policy is supposed to catch all processes not caught by any defined policy above it, change to priority to the highest possible value (100).

The screenshot shows the 'Test Catch-All Policy' configuration page in the 'General' tab. At the top, a yellow warning banner states: 'This policy is not enabled. Managed computers won't receive this policy until it is enabled.' Below this, the 'General' tab is active, showing the following fields:

- Policy Name:** Test Catch-All Policy
- Description:** Application Control policy that only applies to test computers
- Platform:** Windows
- Type:** (empty)
- Folder:** Windows Policies
- Status:** Enabled (checkbox is unchecked)
- Policy Priority:** 100

At the bottom, there are three buttons: 'Save', 'Cancel', and 'Export'.

7. Select the **Enable** checkbox.
8. Customize the policies Conditions, Actions, and Policy Enforcement. Refer to the following screenshots for example configuration of the the policy:

The screenshot shows the 'Test Catch-All Policy' configuration page in the 'Conditions' tab. At the top, the same yellow warning banner is present. Below this, the 'Conditions' tab is active, showing the following configuration:

- Information:** Select the applications to control along with any optional criteria.
- APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING):**
 - Interactive Users
 - Add Application Target
- INCLUSION FILTERS (ONLY APPLIES WHEN ALL MATCH):**
 - Add Inclusion Filter
- EXCLUSION FILTERS (DOES NOT APPLY WHEN ANY MATCH):**
 - LocalSystem and Service applications
 - Present in Signed Security Catalog
 - Add Exclusion Filter
- RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS):**
 - Application Compatibility Testing Windows Computers (Target)
 - Add Resource Target

At the bottom, there are three buttons: 'Save', 'Cancel', and 'Export'.

General Conditions **Actions** Policy Enforcement Deployment Change History

Send policy feedback ⓘ

Actions to apply to the application

TYPE	ACTION NAME
+	Add Action

Actions to apply to the child applications

Use the same actions as the parent

[Save](#) [Cancel](#) [Export](#)

General Conditions Actions **Policy Enforcement** Deployment Change History

Determine how this Policy is enforced.

- Continue enforcing policies after enforcing this policy ⓘ
- Continue enforcing policies for child processes after enforcing this policy ⓘ
- Stage 2 processing ⓘ
- Pause Policy Analysis During Boot ⓘ
- Applies to all processes ⓘ

[Save](#) [Cancel](#) [Export](#)

9. Click **Save**.

Reputation Checking

Privilege Manager analyzes applications in real-time. This unique feature allows for reputation analysis of any unknown applications that will mitigate endpoint attacks from Ransomware, Zero-day attacks, Drive-by Downloads, and other unknown malicious software.

The monitor approach used here is that all applications that meet a general condition (i.e. executed from a specific directory or directories) will be sent to VirusTotal for a reputation check. For this use case we will perform real-time reputation analysis of unknown applications using VirusTotal.

First, you will need to integrate Privilege Manager and VirusTotal by following the Integration steps listed in the [Setting Up VirusTotal for Reputation Checking](#) topic. That section will walk you how to do the following:

1. Configure VirusTotal Ratings Provider
2. Install VirusTotal in Privilege Manager
3. Create a Security Rating Filter for VirusTotal

For information and setup steps to configure reputation checking using Cylance, see the [Cylance Integration](#) topic.

Creating Security Rating Filter

Next you have to create a Security Rating Filter for VirusTotal. Follow these steps:

1. Navigate to **Home | Filters**, then click **Add Filter**.
2. Select a platform, then **Security Rating Filter** as a Filter Type. Name the policy and add a description.
3. Next to Security Rating System, select **Application Control Rating System**.

New Filter

Filter Details

Platform * Windows

Filter Type * Security Rating Filter

Name * New Security Rating Filter

Description

Security rating system

[View Parameters](#)

*Application Control Rating System

Select	Name	Resource Type	Description	CreatedDate
<input type="checkbox"/>				month/day/yea... <input type="checkbox"/>
<input type="checkbox"/>	Application Control Rating System	Security Rating	Application Control Rating System	5/31/19, 12:52 PM
<input type="checkbox"/>	Cylance Rating System	Security Rating	Security Rating System for Application Control Cylance	5/31/19, 1:01 PM
<input type="checkbox"/>	VirusTotal Rating System	Security Rating	Security Rating System for Application Control VirusTotal	5/31/19, 1:01 PM

10 items per page 1 - 3 of 3 items

4. Next to VirusTotal Rating System click +.

5. Click **Create**.

6. Click **Edit**.

7. Under **Settings**, change the **Rating Level** drop-down to specify **Bad**.

Filter > Virustotal Security Rating Filter

Details Related Items Change History

Details

Name * Virustotal Security Rating Filter

Description

Platform Windows

Settings

Security Rating System * VirusTotal Rating System

Rating Level * Bad

Timeout * Unknown cond(s)

Error Handling

On timeout, consider the result * Bad

On failure, consider the result * Error Condition

Save Cancel

The rating level trigger is supposed to match what you want to accomplish with the policy that will be using this filter. A rating level of Bad should be used for Deny policies, and Clean for applications or files that are part of the safe list. A rating level of Suspect can be used in justification and/or learning/discovery policies.

8. Click **Save**.

Creating User's Downloads Location, Temp Dir, and Collection Filters

1. In the Privilege Manager Console search field, enter User's Temp Directory File Specification Filter.

Search

User's Temp Directory File Search

Number of Results
5000

User's Temp Directory File Specification Filter
10/8/19, 9:33 AM - File Specification Filter
Used to target any file in the user's temp directory C:\Users\USERNAME\AppData\Local\Temp
File Specification Filter (1)

2. Select the filter **Users' Temp Directory File Specifications Filter**, click **Create a Copy**.

3. Name the new filter *User's Download Directory File Specification Filter*, provide a description and click **Create**.

4. Click on **Edit**.

5. Change the regular expression in the Path field to the following: (c:\users\[^\]+)downloads), save your changes.

Filter > User's Downloads Directory File Specification Filter

Details Related Items Change History

Details

Name * User's Downloads Directory File Specification Filter

Description Used to target any file in the user's temp directory C:\Users\USERNAME\AppData\Local\Temp

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path (c:\users\[^\]\+\\downloads)

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

6. Finally, combine the 2 filters into a single filter to target both directories:

1. Click **Create a Copy**.
2. Enter the name for the new filter *User's Directory Collection File Specification Filter*, click **Create**.
3. Click **Edit**.
4. Clear the data in the Path field.
5. Under Additional Filters, click the **Add** button to the right of **File filters**.
6. Type **User's Download** to search for the filter.
7. Click **User's Downloads Directory File Specification Filter** from the list to add it.
8. Type **User's Temp Directory** to search for the filter.
9. Click **User's Temp Directory File Specification Filter** from the list to add it (this is a default filter).

Additional Filters (optional)

File filters • User's Downloads Directory File Specification Filter • User's Temp Directory File Specification Filter

Include only filters None Selected

Exclude any filters None Selected

10. Click **Save**.

Creating a Policy

Next you have to create a Policy and add the filters for VirusTotal:

1. Navigate to **Home | Policies**, then click on **Add New Policy**.
2. Select Windows as a Platform, **Show All Policies** as a Policy Type, then **Other: Empty Policy**.
3. Name the policy **Allow Applications - VirusTotal Rating**, and add a description *Deny applications flagged by VirusTotal as bad*, click **Create**.

Policy > Deny Applications – VirusTotal Rating Policy

General Conditions Actions Policy Enforcement Deployment Change History

Common

Policy Name * Deny Applications – VirusTotal Rating Policy

Description Deny applications flagged by VirusTotal as bad

Platform Windows

Type

Folder Windows Policies

Status

Enabled

Policy Priority * 50

Save Cancel

4. Click **Edit**.
5. Next, select the **Actions** tab.
6. Select **Add Action**.
7. In the search field, type Application Denied, and locate the **Application Denied Message Action**.
8. Select the action and click **Add**.
9. On the Conditions tab, add the filters.
 1. Under **Application Targets** add the *VirusTotal Security Rating Filter*.
 2. Under **Inclusion Filters** add the *User's Directory Collection File Specification Filter*.

Policy > Deny Applications – VirusTotal Rating Policy

General **Conditions** Actions Policy Enforcement Deployment Change History

Select the applications to control along with any optional criteria.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

VirusTotal Security Rating Filter

Add Application Target

INCLUSION FILTERS (ONLY APPLIES WHEN ALL MATCH)

User's Directory Collection File Specification Filter

Add Inclusion Filter

EXCLUSION FILTERS (DOES NOT APPLY WHEN ANY MATCH)

Add Exclusion Filter

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS)

All Windows Computers with Application Control Agent Installed (Target)

Add Resource Target

Save Cancel

10. Click **Save**.

If you want the policy to apply to specific users or endpoints, it can be adjusted by clicking on the Advanced Policy View in the policy's General tab. Other edits can be done via the Conditions tab, to add Inclusion/Exclusion filters and Resource Targets.

Note: This policy will send any application run from the user's Downloads or Temp directory to VirusTotal for a reputation check in real-time. If the application is graded with Bad from VirusTotal, the application will be denied.

Viewing a File Security Ratings Report

To view a File Security Ratings report, from the main page go to **REPORTS | File Security Rating Details Report**. To see details of the applications in the report, click on the file name in the File column.

Blocking Policies

Blocking is a policy that denies applications from running on your endpoints based on application attributes, file hash, location, or certificates. This is a powerful type of policy and it may be used to block specific, known and unwanted applications from running. A block policy can target programs that prevent productivity for your end users or applications that are known malware. If malware, you can also add a quarantine action for your block policy as outlined in the second example below.

Thycotic Privilege Manager controls any application on a machine. When you configure Privilege Manager correctly, targeted applications can be elevated, whitelisted, or blocked. But if you create new policies without careful consideration then you can potentially block core system processes.

Before you create new policies, keep in mind the following best practices:

- Do not enable policies until after you have configured them. As a safety precaution, all newly-created application control policies are turned off until you enable them.
- Important: New policies that you create will automatically target all applications until you add application filters that will narrow the scope.
- Additionally, Thycotic highly recommends testing all policies on a limited number of machines before they are deployed to the entire environment. See [Best practices for Application Control Solution policies](#) for more information.

The following examples are available:

- [Blocking Specific Applications](#)
- [iTunes with File Upload](#)
- [Quarantine Specific Malware](#)
- [Catch-all block Policy](#)

Catch-all Deny

A catch-all deny policy is the last policy executed following the execution of a group of whitelist policies. This enables you to configure your whitelist to allow approved applications, like the Windows directory or other installed applications, and then to deny everything else, like applications downloaded from the internet or a thumb drive.

To create a catch-all deny policy, do the following steps:

1. Begin by selecting Policies from the Privilege Manager Dashboard.
2. Next, click Add New Policy.
3. Select Other Policies and click the Next button.
4. Select Empty Application Control Policy and click the Next button.
5. Provide a name and description for your Policy and click Create.
6. Set the Policy Priority to 99 so it applies after all other Policies.
7. Click the Condition tab and click the plus button under Exclusion Filters. Search for "LocalSystem and Service applications" and click Add at the bottom.
8. Click the Actions tab, click Add Action, search for "Deny Execute", select Deny Execute, and click Add.
9. Click the Policy Enforcement tab, ensure only Stage 2 processing is checked, and click Save.

If you are creating a new catch-all policy to be used in conjunction with whitelist policies, please verify that the whitelist is catching all system applications and that the new deny policy is the last policy executed. For additional safety you can define the exclude any parameter to exclude system and service applications.

iTunes with File Upload


As we've seen, there are multiple ways to introduce a new application into Privilege Manager before assigning a policy to it. For this example we will perform a File Upload for the iTunes installer to quickly Blacklist the iTunes program from running on target endpoints.

Note: When the iTunes default filter is used to verify the correct Company name is entered to match the application targeted by the policy.

First create the iTunes filter by using downloaded iTunes files:

1. On the Application Control dashboard home page, select the **Upload File** tile or navigate to **TOOLS | File Upload**.
2. Browse to select file (i.e. the iTunes installer), click **Upload File**.

Upload a file


Application File:  No file selected.

Notice: Files uploaded to the server will be stored temporarily during the inventory process without the ability to be executed. The file is then deleted once the process completes.

[Back](#) [Upload File](#)

3. When the file successfully uploads, choose **Go to File Details**.

Upload a file

 The file was successfully uploaded. Click the button below to view the file inventory details and optionally create filters or assign it to a policy.

[Back](#) [Go to File Details](#)

4. The Resource Explorer opens for the uploaded file. Click **Add New Filter**.

Resource Explorer > iTunes.exe

Summary	File Name	iTunes.exe
Known Data	Original File Name	
Events	Product Name	
Associations	Version	0.0.0.0
	Internal Name	
	Company Name	
	Copyright	
	File Hashes	Authenticode 2: 1dc58f11ba13b4e97eacfb7d443a8e0033f7451a49727bf6f0b7db51be7a54f md5: 95ffceec0dbc817762c1ba19e0557a7d sha256: 3b876ffe872b8d8cfd3e1c3cb621a56ed2a3b89b486947ced1d8220bf5713ae sha1: 4881b9fba3280bd896ee76b8f46c1df7836fc125 Authenticode: f6b6f47d11018b7b2c3f09bdddd943b59c71286d
	View Reputation	VirusTotal.com Cylance.com

[Back](#) [View as XML](#) [Add New Filter](#) [Add To Policy](#) [Delete](#)

[Computer Locations](#) [Policy Events](#) [Similar Files Report](#)

No results.

5. Check, modify, and/or enter the Filter criteria you want to block like the File Name, the Original File Name, and the Product Name.
6. Click **Create**.

Next create the iTunes Deny Policy:

1. Click on the **Deny (Blacklist) Applications** tile on the Application Control dashboard.
2. Click **Create a New Policy**.
3. Select a **Platform**, then **Blacklist: Deny Specific Applications**.
4. Add Name and Description, click **Create**.
5. In the **Advanced Policy View** under the **Conditions** tab, select **Edit**.
6. Add the **Inclusion Filter**.
7. Select your iTunes filter/s.
8. click **Add**, then **Save**.
9. Under the General tab, click Edit.
10. Select **Enabled** to enable the policy.
11. Click **Save**.

Under the Actions tab, do not change the settings, but notice it is set to Deny Execute Message. This will produce a pop-up message to the user telling them this application execution is denied.

You can edit the policy further, if needed. Adjust the Policy Priority as needed. Policy Priority will be discussed in detail later in this document.

Quarantine Specified Malware

For known cases of malware or ransomware, you can use Privilege Manager to prevent specified applications from running and place them in a quarantine. For this example we'll target the generic executable "malware.exe," but you can do this with any file name.

First, create your malware filter:

1. Choose the Filters Tile from the Application Control home page dashboard or navigate to ADMIN | Filters.
2. Click **Add Filter**.
3. Select **Windows** as a platform and **Blank Win32 Executable Filter** as a Filter Type.
4. Name your filter **Malware Example** and add a description.
5. Click **Create**.
6. Click **Edit** and add the file name **malware.exe**.
7. Click Save.

Next, create a Blacklist Policy that will quarantine this filter's target.

1. From the dashboard click the **Policies** tile.
2. Click **Add New Policy**.
3. Select **Windows** as a Platform.
4. Select **Show All Templates**.
5. Select **Blacklist: Quarantine Specific Applications** as a Template Type.
6. Add a Name and Description, click **Create**.
7. Click **Edit** and the **Enabled** checkbox.
8. Choose the Advanced Policy View button if possible.
9. Under the **Conditions** tab, click **Edit**.
10. Add **Application Target** and search for your malware example filter and add the filter.
11. Click **Save**.

Once this policy has been applied to your endpoint/s, any executable called malware.exe will be automatically blocked and quarantined if prompted to run

Specific Applications

To create a new policy that blocks specific applications, do the following steps:

1. Begin by selecting Deny (Blacklist) Applications from the Privilege Manager Dashboard.
2. Select Block Application by Name and click Next.
3. You will have to supply a application under File Name and/or File Path. Optionally you may choose a message to display to the user when they attempt to execute the target application. Once you feel satisfied to proceed, click Finish.
4. On the General tab, you can customize the name and description of your Policy and observe where it will be placed in Privilege Manager's folder structure. You should enable the Policy by ticking the checkbox next to Enabled and you can decide on what priority the Policy should have in comparison to other Policies. The lower numbered Policies will apply before higher numbered Policies.
5. Click the Policy Enforcement tab. If you wish to ensure that this Policy will not affect system or service applications, select Applies to all processes. Otherwise, keeping the Applies to all processes setting disabled will force this policy to apply to only applications launched by the interactive user. Ensure all other boxes are unchecked here and click Save to finish creating your blacklist Policy.

Be sure to test the new policy on a few machines before you roll it out to the environment.

macOS Specific Policies

Once your macOS agent is registered, creating policies for your macOS machines follows a very similar process to creating policies for Windows machines in Privilege Manager:

1. Collect File Data—This enables Privilege Manager to recognize specific files and file types in your environment. The file data that you want to target with policies are called Events. All imported files can be viewed in the Event Discovery | Files page.
2. Create Filters—This step sorts important file data (Events) according to different criteria.
3. Create Policies—This step defines what 1) Actions to perform on applications and the 2) Targets (Locations) for those actions.
4. Assign Filters to Policies—This step directs a Policy's actions to the appropriate Events happening on your network. This step also allows a Policy to be Enabled, or activated.
5. Order your Policies based on priority level—Once your policies are created, the order they execute across your network matters. See the Policy Priority section in this guide for more details.

In macOS, roles are bifurcated into two groups: Admins, and Users rather than by Group Policy Objects (GPO) found in Windows environments.

Actions supported by macOS Agents

The following actions are supported by macOS agents:

- Allow Copy to /Applications/Directory
- Allow Package Installation
- Application Approval Request (with Offline Fallback) Message Action
- Application Approval Request (with ServiceNow Request Item Number) Message Action
- Application Approval Request Message Action (workflow request)
- Application Denied Message Action
- Application Justification Message Action
- Application Warning Message Action
- Deny Execute / Deny Execute Message
- File Quarantine
- Quarantine Message
- Run as Root (Elevate)

Available Topics

- [Allow Copy/Install of Applications](#)
- [Request Application Installation](#)
- [Application Self-elevation](#)
- [Use Discovery to Determine if an Application Requires Admin Privileges](#)
- [Require Justification for Firefox](#)
- [Deny Photos Application](#)
- [Adding macOS Agents to a Computer Testing Group](#)
- [Inventinging .pkg Files](#)

Allow Copy to Install Applications

A policy can be created to allow or deny standard users to install specific applications by copying/pulling the application into the Applications folder. Follow this example to create a policy that will enable this functionality for your Mac OS user.

1. Navigate to **Admin | Policies** and click the **Add New Policy** button.
2. From the Platform drop-down select **Mac OS**.
3. From the Policy Type drop-down select **Show All Templates**.
4. From the Template Type drop-down select **Other: Allow Standard Users to Copy to Applications Directory (via Drag and Drop)**, this can also be done via **Other: Empty Policy**.

5. Enter a name and description for the new policy and click **Create**.
6. Once the policy is created, it can be modified to be restricted to certain applications instead of targeting every application:
 1. Click **+ Add Application Target** to specify an application bundles filter for Mac OS applications.
 2. Click **+ Add Inclusion Filter** to specify the Copy Install Application filter.
 3. Click **Save**.

7. Navigate to the **General** tab.
8. Click **Edit**.
9. Select the **Enabled** checkbox to enable the policy.

10. Click **Save**.

Note: The new Copy Install Application Filter should not be used with the existing Privilege Manager Copy/Installer Helper Parent Process Filter, which should be removed from any policy before adding the new Copy Install Application Filter to the policy.

Updating Existing Policies to Use the Copy Install Application Filter

If you have policies that currently use the Privilege Manager Copy/Installer Helper Parent Process Filter use the following steps to update them to use the Copy Install Application Filter in the Privilege Manager UI:

1. Navigate to **Admin | Policies**.
2. Click **Edit** and navigate to **Conditions** tab.
3. Under Inclusion Filters remove the **Privilege manager copy/installer helper parent process filter**.
4. Under Add Inclusion Filter search for and select **Copy Install Application** and click **Add**.
5. Navigate to the Actions tab and remove **Allow copy to/Applications/Directory**.
6. Click **Add Action** and select Application Approval Request Message Action then click **Add**.
7. Navigate to Policy Enforcement and select any of the options:
 - Continue enforcing policies after enforcing this policy
 - Continue enforcing policies for child processes after enforcing this policy

On the macOS endpoint,

1. Login as Admin user.
2. Open the macOS Agent via Terminal and run an update using command:

```
sudo /usr/local/thycotic/agent/agentUtil.sh updateclientitems
```

The agent updates with new and updated policies and synchronizes.

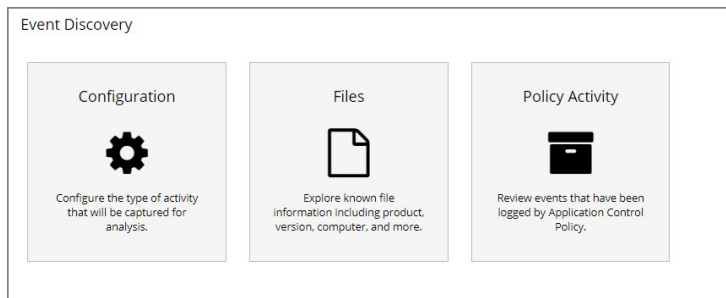
Deny Photos Application

With your Learning Mode policy properly set up, anything you do on your Mac test machine will be discovered by Privilege Manager. For this example we will create a policy that blocks the Photos and Photo Booth applications.

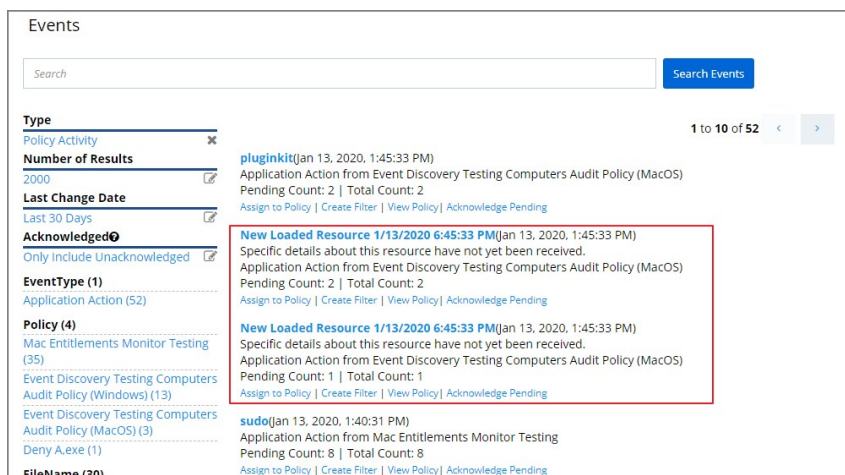
Event Discovery

Open the Photos and PhotoBooth applications on an macOS test endpoint. When these applications are opened, Privilege Manager discovers these as an *Application Action from Event Discovery Testing Computers Audit Policy (MacOS)*.

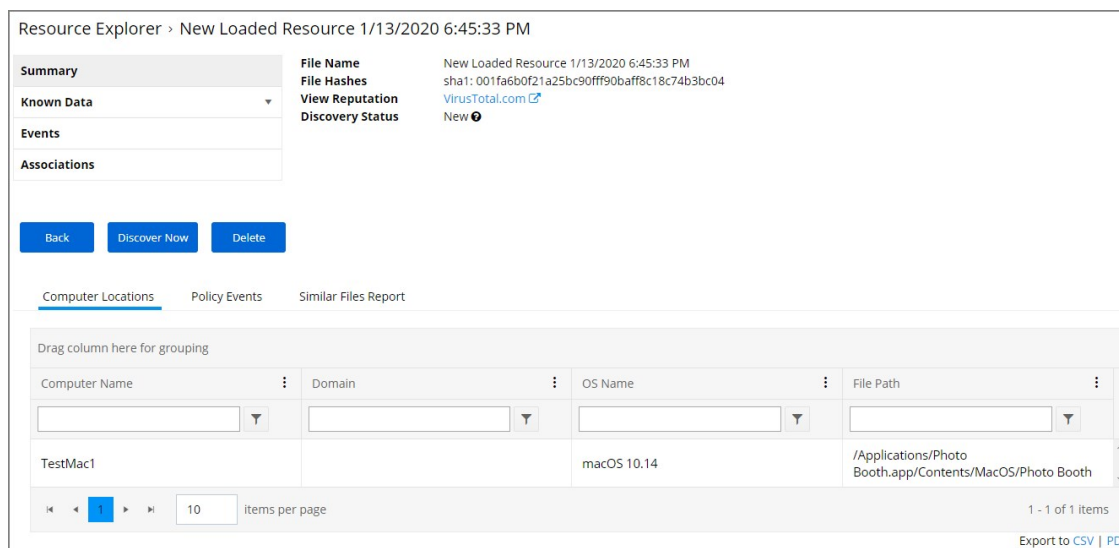
1. In the Privilege Manager Console, navigate to **Event Discovery | Policy Activity**.



2. Verify new items have been registered by your Event Discovery Testing Computers (MacOS) policy. These may be listed as **New Loaded Resources**.



1. Select a **New Loaded Resource** link.
2. On the loaded Resource Explorer page, click the **Discover Now** button. It still may take time to properly load details about these new events, usually indicated by a **Discovery Status of New**.



Clicking the Discover Now button creates and executes a **Manual client-side resource discovery** task. If you click the status link the task page opens (not shown in this example sequence).

When a resource is fully discovered it is displayed with full name on the discovery events page:

The screenshot shows the 'Events' page with a search bar and a 'Search Events' button. Below the search bar, there are several filter sections: 'Type' (Policy Activity), 'Number of Results' (21 to 30 of 70), 'Last Change Date' (2000), 'Last 30 Days', 'Acknowledged' (Only include, Unacknowledged), and 'Event Type' (1). The results list two items: 'Photos' and 'Photo Booth', each with a brief description and links for 'Assign to Policy', 'Create Filter', 'View Policy', and 'Acknowledge Pending'.

From the events page you can now use the **Assign to Policy** or **Create Filter** links to create specific policies for the discovered applications.

Assign to Policy

Once the resources have been fully discovered, the fastest way to either create a new policy or add to an existing one is via the Assign to Policy link on the Events page.

1. Click the **Assign to Policy** link.
2. The Resource Explorer opens for the selected resource, here it is the Photo Booth application.

The screenshot shows the 'Resource Explorer > Photo Booth' page. It features a left-hand navigation menu with 'Summary', 'Known Data', 'Events', and 'Associations'. The main content area displays a list of application details: File Name (Photo Booth), Bundle Identifier (com.apple.PhotoBooth), Bundle Name (Photo Booth), Display Name (Photo Booth), Version (1009), Short Version (10.0), Type (APPL), Region (English), Bundle Executable (Photo Booth), Min System Version (10.14), Application (public.app-category.entertainment), Category, Copyright (Copyright © 2005–2018 Apple Inc. All rights reserved.), File Hashes (md5: 8d0f4cdec583ce1c127ba3292cd1aaf9, sha1: 001fa6b0f21a25bc90fff90baff8c18c74b3bc04), and View Reputation (VirusTotal.com). At the bottom, there are four buttons: 'Back', 'Add New Filter', 'Add To Policy', and 'Delete'.

3. Click **Add To Policy**.

This screenshot shows the same 'Resource Explorer > Photo Booth' page as above, but with the 'Add To Policy' button highlighted. Below the main content area, a dialog box titled 'Add New Policy' is open. It contains the following text: 'Create a new Policy targeted by the options selected below. A new Filter will be created that can also be used in conditions for other Policies. After the Policy is created it will need to be targeted at Managed Computers in order to be applied.' Under 'Policy Options', there is a section for 'Add New Filter To' with a dropdown menu showing 'New Policy' and a plus icon, and a 'Policy Type' dropdown menu with the text '-- select a policy template --'. Below this is a 'Filter Options' section.

This lets you either create a new policy or add to an existing policy. No matter which option you choose, a new filter for the resource (Photo Booth) is automatically created and all fields are pre-populated based on the discovered application details.

4. From the **Add New Filter to** drop-down select **New Policy**.

1. From the **Policy Type** drop-down select **Blacklist: Deny Specific Applications**.
2. In the Name field enter **Deny Photo Booth Application Execution Policy** as a new policy name.
3. Under Filter Options, only select **File Name** and **Path** filter options if you want to limit the filter to match the exact name and installation path. By default these are not pre-populated to avoid unintentional limitations. Customize the filter options if needed.

Add New Policy

Create a new Policy targeted by the options selected below. A new Filter will be created that can also be used in conditions for other Policies. After the Policy is created it will need to be targeted at Managed Computers in order to be applied.

Policy Options

Add New Filter To: New Policy

Policy Type: Blacklist: Deny Specific Applications

Name: Deny Photo Booth Application Execution Policy

Description: This policy prevents processes from running.

Filter Options

File Name: Photo Booth

Path: /Applications/

App Category: is equal to public.app-category.entertainment

Bundle Identifier: is equal to com.apple.PhotoBooth

Bundle Name: is equal to Photo Booth

Bundle Version: is equal to 1009

Bundle Version (short): is equal to 10.0

Executable File: is equal to Photo Booth

Min System Version: is equal to 10.14

Info String

File must be signed by: + Add CN=Software Signing, OU=Apple Software, O=Apple Inc., C=US

Cancel Create

5. Click **Create**.
6. Navigate back to the Events page and select the **Assign to Policy** link underneath the Photos resource.
7. From the **Add New Filter To** drop-down select **Existing Policy**.
 1. In the **Policy Name** search field enter the policy name created for the Photo Booth app.
 2. Specify and customize filter options.

Add New Policy

Create a new Policy targeted by the options selected below. A new Filter will be created that can also be used in conditions for other Policies. After the Policy is created it will need to be targeted at Managed Computers in order to be applied.

Policy Options

Add New Filter To: Existing Policy

Policy Name: Deny Photo Booth Application Execution Policy

Filter Options

File Name: Photos

Path: /Applications/

App Category: is equal to public.app-category.photography

Bundle Identifier: is equal to com.apple.Photos

Bundle Name: is equal to Photos

Bundle Version: is equal to 3461.7.150

Bundle Version (short): is equal to 4.0

Executable File: is equal to Photos

Min System Version: is equal to 10.14

Info String

File must be signed by: + Add CN=Software Signing, OU=Apple Software, O=Apple Inc., C=US

Cancel Create

8. Click **Create**.
- Note:** Policies are not automatically enabled. For any further customization or to enable a policy, navigate to ADMIN | Policies and search for and edit the newly created policy.

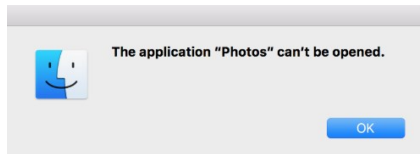
Policy Verification

To make sure your policy is effective, pull up Terminal on your testing macOS endpoint and run the `sudo /usr/local/thycotic/agent/agentUtil.sh updateclientitems` command.

```
macadmins-MacBook-Pro:~ macadmin$ sudo /usr/local/thycotic/agent/agentUtil.sh up
dateclientitems
Updating policy client items...
Updating unknown client items...
Updating command client items...
Updating action client items...
Updating filter client items...

22 client items are up to date
13 policies are up to date
Updated policy "Block Photos (MacOS)" (657ded1a-79af-4bae-b444-fb52b098f29)
macadmins-MacBook-Pro:~ macadmin$
```

Once this Deny-policy is updated on your endpoint, when you click Photo Booth or Photos, you will see a message like this:



Create a Filter Only

If you just want to create a filter based on the discovered resource, use the Create Filter option link underneath the discovered resource.

1. Navigate to **Admin | Event Discovery | Policy Activity**. You should see an event titled **Photos** and another titled **Photo Booth**.
2. Select **Create Filter** underneath each of these events. (Example shows create filter action for Photo Booth app.)

Filter Options

- File Name
- Path
- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File
- Min System Version
- Info String
- File must be signed by

<input checked="" type="checkbox"/> App Category	is equal to	public.app-category.entertainment
<input checked="" type="checkbox"/> Bundle Identifier	is equal to	com.apple.PhotoBooth
<input checked="" type="checkbox"/> Bundle Name	is equal to	Photo Booth
<input checked="" type="checkbox"/> Bundle Version	is equal to	1009
<input checked="" type="checkbox"/> Bundle Version (short)	is equal to	10.0
<input checked="" type="checkbox"/> Executable File	is equal to	Photo Booth
<input checked="" type="checkbox"/> Min System Version	is equal to	10.14

Info String
 File must be signed by

• CN=Software Signing, OU=Apple Software, O=Apple Inc., C=US

Computer Locations Policy Events Similar Files Report

Drag column here for grouping

Computer Name	Domain	OS Name	File Path
TestMac1		macOS 10.14	/Applications/Photo Booth.app/Contents/MacOS/Photo Booth

10 items per page 1 - 1 of 1 items

[Export to CSV](#) | [PDF](#)

3. Customize the filter options if needed.

4. Click **Create**.

The filter can later be added to new or existing policies.

Determine Admin Requirement

Use discovery with event notification to determine if an application requests or requires administrative privileges to perform tasks or run on a macOS endpoint.

1. Use/Create a **Codesign Entitled Elevated Application Filter**. This filter creates events for application bundles that have a specific entitlement that might prompt for administrative permissions if launched.

1. Create a copy of Codesign Entitled Elevated Application Filter:

Codesign Entitled Elevated Application Filter

i This item is read-only.

Details

Name Codesign Entitled Elevated Application Filter

Description Filter used to detect codesign entitled applications

Platform Mac OS

Settings

Back Edit Create a Copy

2. Use/Create an **Executable Declared as Privileged Filter**. This filter creates events for application bundles that list a privileged helper in their info.plist files.

Executable Declared as Privileged Filter

i This item is read-only.

Details

Name Executable Declared as Privileged Filter

Description Filter used to detect SMPrivilegedExecutables in an App Bundle

Platform Mac OS

Settings

There are no configurable settings for this item.

Back Edit

This is a read-only filter, no customization via **Create a Copy** is available.

3. Add both filters as the application target to a new policy and enable the **Send Policy Feedback** action for that policy.

1. Navigate to **Admin I Policies** click **Add New**.
2. As the Platform Type select Mac OS.
3. From the Templates drop-down select Other: Empty Policy Template.
4. Name your policy and add a description.

New Policy

Platform * Mac OS

Policy Type * Show All Templates

Template Type * Other: Empty Policy

Name * Determine Admin requirements on macOS

Description Policy to determine if applications require admin rights to run. Sends policy feedback.

Back Create

5. Click Create.
6. Click Edit on the newly created policy page.
7. Under status select **Enabled**.
8. Select the **Conditions** tab.
9. Under **Application Targets**, add the two filters:
 - The copy of the codesign filter you created in step 1.
 - The default of the *Executable Declared as Privileged Filter*.

Policy > Determine Admin requirements on macOS

General **Conditions** Actions Policy Enforcement Deployment

i Select the applications to control along with any optional criteria.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

- Find Admin Codesign Entitled Elevated Application Filter
- Executable Declared as Privileged Filter
- Add Application Target

INCLUSION FILTERS (ONLY APPLIES WHEN ALL MATCH)

- Add Inclusion Filter

EXCLUSION FILTERS (DOES NOT APPLY WHEN ANY MATCH)

- Add Exclusion Filter

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS)

- All MacOS Computers with Application Control Agent Installed (Target)
- Add Resource Target

Save Cancel

- Navigate to the **Action** tab.
- Select the **Send Policy Feedback** option.

Policy > Determine Admin requirements on macOS

General Conditions **Actions** Policy Enforcement

Send policy feedback

Actions to apply to the application

TYPE	ACTION NAME
	Add Action

Actions to apply to the child applications

Use the same actions as the parent

TYPE	ACTION NAME
	No Action will be applied to child processes
	Add Action

Save Cancel

- Click **Save**.
- Navigate to the **Deployment** tab.
- Click the **Run Policy Targeting Update**.

Note: There is currently no option to determine if command-line tools require admin privileges.

Require Justification - FireFox

The following example provides information on setting up a justification required policy for FireFox on a macOS endpoint.

1. With a Learning Mode Policy enabled, open Firefox on a test macOS endpoint. A few minutes after doing this you should find a new item in **Admin | Event Discovery | Policies** titled **Firefox**.
2. Click **Create Filter**, enter a name and description and click **Create**.
 - Note:** If you are not immediately directed to an **Add New Filter** screen, this means Privilege Manager doesn't have enough information to target this application. In these cases you may need to create Filters manually (**Admin | Filters | Add Filter**).
3. Navigate to **Admin | Policies** and **Add New Policy**.
4. Select **MacOS** as a Platform, **Show All Templates** for Policy Type and then **Other: Empty Policy** as Template Type.
5. Name your new policy "**Firefox - Request Access (MacOS)**" and add a **Description**.
6. Click **Create**.
7. On the **Conditions** tab, click **Edit**.
8. Under **Add Application Target** search for the filter name as created for your Firefox policy (refer to steps above) click **Add**.
9. Verify the **Resource Targets** section at the bottom of this page lists the correct target computer group for macOS endpoints that you want to apply this policy to.
10. Under the **Actions** tab, click **Add Action**.
11. Search for **Application Justification Message Action** and **Application Approval Request Message Action**, add both of those.
12. Navigate to the **General** tab and check the **Enabled** box.
13. Click **Save**.

To make sure your policy is effective, pull up Terminal on your testing macOS endpoint and run `sudo /usr/local/thycotic/agent/agentUtil.sh updatedclientitems` command.

Once this Request Access-policy is updated on your endpoint, when you click Firefox you will see a prompt where the user can enter their reason for accessing Firefox:

Application Notice

Please provide a reason as to why you require this application to be run with elevated rights.

Application: Firefox
User: macadmin

Type a brief explanation describing why this application is necessary. This explanation will be recorded and may be reviewed by the IT staff for consideration into [corporate policy](#).

Reason (required)
What does the fox say?

Buttons: Cancel, Publish Info, Continue

To Accept this request, in the Privilege Manager Console navigate to **Tools | Manage Approvals**. Click the request and approve, you may do so for one time access or for a time interval:

Manage Approval Requests

Name	Policy	User	Request
Firefox - Request Access	Firefox - Request Access	macadmin	Request ID: 12345678

Confirm Approval

Approve: One time For: 1 hour(s)

Buttons: Approve, Cancel

On the macOS endpoints the user will see these messages:

Waiting for approval:

Waiting for approval response...

Buttons: Cancel, Refresh

Approval confirmation:

This application has been approved. Press the continue button to proceed.

Buttons: Cancel, Continue

Request Application Installation

Privilege Manager can allow macOS users to install packages on demand. Do the following to create a policy to allow users to request installation of certain packages. For this to work, your endpoint must be online. If the system is offline, refer to the Offline Approval process documentation.

1. Navigate to **Admin | Policies** and select **Add Policy**.
2. Choose the Mac OS Platform and select **Show All Templates** and then **Other: Approve Installer Packages**.

The screenshot shows a 'New Policy' configuration window with the following fields:

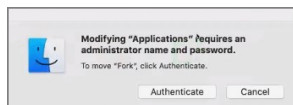
- Platform:** Mac OS
- Policy Type:** Show All Templates
- Template Type:** Other: Approve Installer Packages
- Name:** New Approval Request Policy for Package Installations
- Description:** This policy allows users to install packages after they are approved.

Buttons for 'Back' and 'Create' are visible at the bottom left.

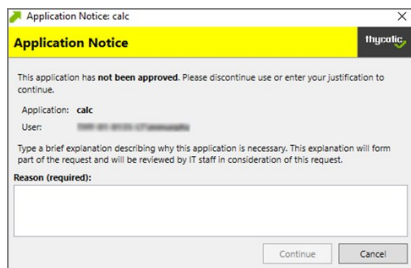
3. Customize the Name and Description and click **Create**.
4. Enable the policy after it has been created and update policies at the endpoint.

Once the policy is enabled and in place at the endpoint, a user will typically go through the following steps to request an application installation:

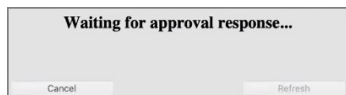
1. Mount the DMG containing the application you'd like to install to Applications. If the DMG contains an application bundle that can be dragged to the Applications folder, do so. If the DMG contains an installer application, double-click and proceed with the steps outlined in installing an application.
2. The Authentication required dialog opens:



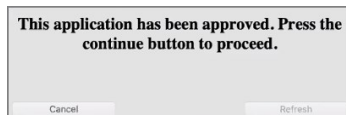
3. Click the Authenticate button. The following Application Notice opens:



4. Enter the Reason why the application should be installed and click the Request Approval button. The Waiting for approval response dialog opens.



5. Once approved, the "This application has been approved..." text displays. Click the Continue button to proceed with the installation. If you click Cancel, the application will not be copied to the Applications folder and you may need to request approval again.



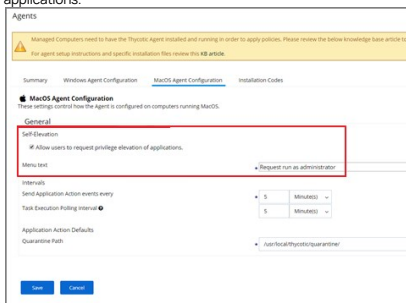
Application Self-elevation

Finder Sync Extensions allow application control on macOS endpoints. Just as on Windows endpoints, users can request application self-elevation via right-click mouse action. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.

Configuring Application Self-elevation

Your Privilege Manager needs to be configured to allow self-elevation of applications on an endpoint. Follow these server configuration steps:

1. Navigate to **Admin | Agents** and select the **MacOS Agent Configuration** tab.
2. Click **Edit**.
3. Under the General section enable Allow users to request privilege elevation of applications.

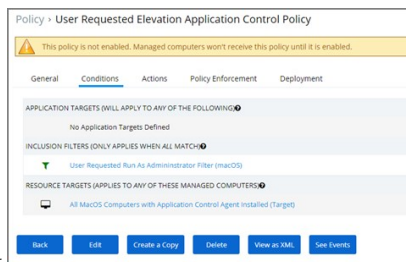


4. In the Menu text entry field enter something like Request run as Administrator.
5. Click **Save**.

Note: When Self-Elevation options are modified in the **MacOS Agent Configuration**, client items on a macOS system must be updated and on older versions of macOS the user must logout and login for the changes to take effect.

After enabling the Allow users to request privilege elevation of applications in the **MacOS Agent Configuration**, you can create policies to target the User Requested Run As Administrator Filter (macOS) and specify which action you want taken. If you choose Approval Request, users will have to request and gain approval before having the application elevated.

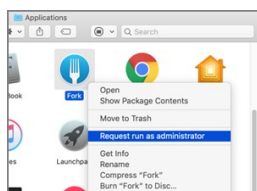
1. Navigate to **Admin | Policies**.
2. Click **Add New Policy**.
3. Navigate to the Conditions tab and Inclusion Filters section.



4. Click **+ Add Filter** and select the User Requested Run As Administrator Filter (macOS) filter.
5. Click **Save**.

How to Request an Application Run as Administrator

To request to run an application as Administrator, the user at the macOS endpoint navigates to and selects the applications in Finder and uses either right-click or Control+Click to invoke Finder's context menu:



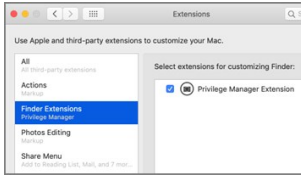
Here the user selects the Request run as administrator menu option.

Depending on the policy in place, this will either be granted immediately or trigger an approval request.

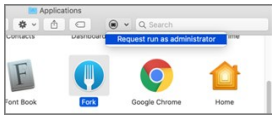
Troubleshooting: Verify the Finder Extension is Installed

The Finder Privilege Manager extension installs by default during an agent install or upgrade. The extension is enabled/disabled based on the **MacOS Agent Configuration** policy on the Privilege Manager Server. If the extension is not enabled, check with your system administrator.

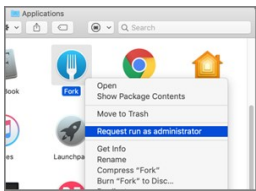
1. Open **System Preferences | Extensions**.
2. Select **Finder Extensions**.
3. Verify that Privilege Manager Extension is listed and enabled for customizing Finder.



Once the Privilege Manager Extension is enabled, the extension icon is visible in Finder.



The extension is also present as a menu item when you right-click or control+click an application in Finder.



Adding macOS Agents to a Computer Testing Group

The Policy Configuration examples in the following section will use a Learning Mode Policy that enables us to perform actions (i.e. run applications) on a test computer that Privilege Manager will then pick up. This makes targeting specific applications during policy creation easy.

Setting Up Learning Mode Policies for macOS

To create a Learning Mode Policy on your Mac, begin by adding your newly registered macOS Agent to your Test Computer Group for Macs:

1. In Privilege Manager go to **Admin | Event Discovery | Configuration**, then click the underlined Application Compatibility Testing Computers link next to the Log all MacOS activity option.
2. Under the **Filter Definition** tab, select the macOS computer(s) you want to target for testing under the Include Specific Resources section. This "Testing Computers" group should only be used for testing specific machines and configuration purposes. It should not be assigned to large groups of computers in your production environment.

Note: You may have both macOS and Windows target computers listed in this group, but policies are platform-specific, meaning they will distinguish between macOS and Windows computers.

1. To activate your learning mode policy for this target group, verify that the **Log all MacOS activity from Application Compatibility Testing Computers** is checked under the General tab of **Admin | Event Discovery | Configuration**.

Under **Admin | Policies | Mac OS** tab, you should also see an Event Discovery Testing Computers (MacOS) policy enabled.

Inventinging .pkg Files

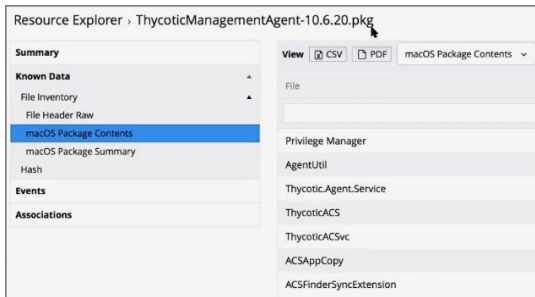
Privilege Manager allows the inventory of macOS .pkg files. With the ability to upload and extract the contents within the .pkg files Privilege Manager inventories the applications that are bundled in any given .pkg.

After uploading a .pkg file select the **Go To File Details** button.

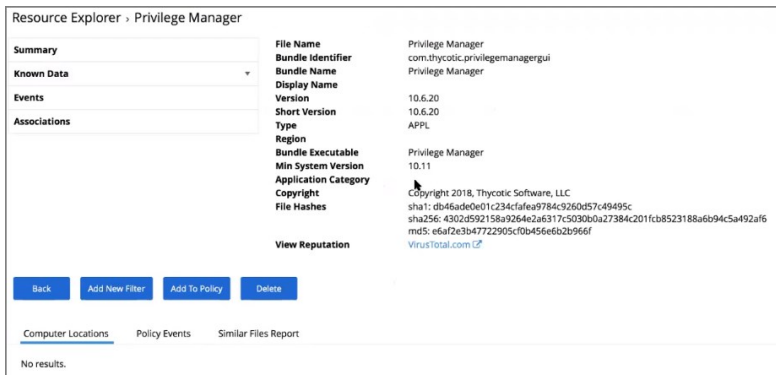


In the Resource Explorer an Administrator can now look at all the details from the inventory.

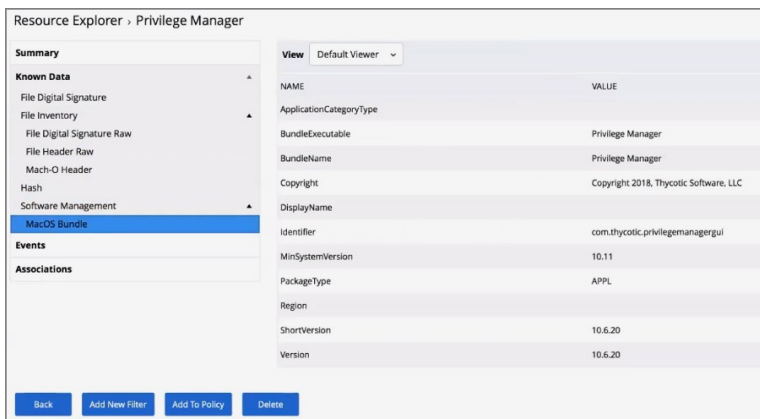
- Showing the list of applications:



- Showing the main application details:



- Showing the information specified in the macOS bundle:



Note: Any packages that deviate from the standard configuration and layout might not have their contents inventoried correctly. If that is the case, unpack the .pkg and upload each contents file individually for inventory purposes.

Here is the complete list of policies that come with Privilege Manager out-of-the-box, grouped by folder type. Once you create custom policies they are listed along the default policies under the tab respective to the template used, as the template associates the folder type.

Process Hardening

Remove Advanced Privileges for Interactive Users	Removes advanced privileges for users interacting with a system via Desktop	n/a	50	n
--	---	-----	----	---

System Options

Client Option - Elevate Adding Printers via Control Panel	Elevates privileges of users to allow printer drivers to be installed through the Control Panel	Elevate	60	n
Client Option - Elevate Adding Printers via PrintUI.exe	Elevates privileges of users to allow printer drivers to be installed by the PrintUI Utility	Elevate	60	n
Client Option - Elevate Changing Time and Date	Elevates privileges of users to allow them to change the system time and date	Elevate	60	n
Client Option - Elevate Device Pairing	Elevates privileges of users to allow new drivers to be installed during the device pairing wizard.	Elevate	60	n
Client Option - Elevate Disk Defragmentation (Vista/7)	Elevates privileges of users to allow them to defragment their hard disks on Windows Vista and Windows 7.	Elevate	60	n
Client Option - Elevate Disk Defragmentation (XP)	Elevates privileges of users to allow them to defragment their hard disks on Windows XP.	Elevate	60	n
Client Option - Elevate Installing Display Languages	Elevates privileges of users to allow display languages to be installed	Elevate	60	n
Client Option - Elevate Network Adapter Settings	Elevates privileges to allow user to change network adapter settings.	Elevate	60	n
Client Option - Elevate Resource and Performance Monitoring	Elevates privileges of users to allow them to run Windows Resource and Performance Monitor utilities	Elevate	60	n
Client Option - Elevate Windows Backup	Elevates privileges of users to allow them to run Windows Backup	Elevate	60	n

Privilege Management

Limit Internet Browser and Mail Clients Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for standard Internet browsers and mail clients. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Popular Instant Messaging Application Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for instant messaging applications. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Popular Media Player Process Rights	This policy implements the fundamental security principle of least privilege by restricting the process rights for media player applications. Running these applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within these applications.	Reduce	50	n
Limit Process Rights for Unclassified Applications Discovered in the Last Week	This policy implements the fundamental security principle of least privilege by restricting the process rights for an application. Unnecessarily running applications with administrative rights can present significant security problems. This policy reduces the risk of an exploit infecting a computer from within an application. This policy affects applications that have been discovered locally in the last week.	Reduce	95	n
User Access Control (UAC) Override Policy	This policy allows standard users to provide a justification for elevation instead of seeing the UAC prompt.	Elevate	15	n
User Requested Elevation Justification Policy	This policy allows users to request applications to run with Administrative Rights if they provide a justification.	Elevate	15	n

Application Analysis

Administrative Rights Required Detection Policy (Application Compatibility)	This policy detects applications that are deemed to require Administrative rights by Windows.	Elevate	45	n
Administrative Rights Required Detection Policy (Security Manifest)	This policy detects applications that contain a security manifest that specifies administrative rights are required.	Elevate	45	n
Event Discovery Audit Elevated Privileges Policy	This policy will detect all applications that are run with Administrator Rights on endpoints with the agent. This policy can be configured on the Event Discovery Configuration page.		45	n
Setup Detection Policy	This policy reports on applications that are detected as an installer.		45	n

Windows Policies

Event Discovery Testing Computers Audit Policy (Windows)	This policy is enabled through the Event Discovery configuration by enabling the option to log all activity from the test group.	97	n	
Elevate Privilege Manager Remove Programs Utility Policy	This policy needs to be enabled if users are supposed to be able to remove programs and apps via the Remove Programs Utility.	2	n	

macOS Policies

Event Discovery Testing Computers Audit Policy (MacOS) This policy is enabled through the Event Discovery configuration by enabling the option to log all activity from the test group. 97 n

Automatic Elevation via Windows Client System Settings

Common Windows client settings can be deployed to endpoint agents the same way as any policy. These settings target **All** Windows Computers with Application Control Agent Installed (Target)* as the default resource target. Once a setting is selected from the list, the resource target can be modified to include specific computer or other existing resource targets can be assigned on screen.

Add Devices	Allow users to add drivers, installing drivers as necessary.
Add Printers	Allow users to add printers, installing drivers as necessary.
Backup the System	Allow users to perform system backup operations.
Change the Date and Time	Allow users to change the date, time and timezone.
Change Network Adapter Settings	Allow users to change the network adapter settings.
Defragment the Disk	Allow users to perform disk defragmentation operations.
Install Language Packs	Allow users to install operating system display languages.
Monitor Performance	Allow users to run the Windows Performance Monitor utility.

ActiveX

ActiveX Setting define which sites can run ActiveX controls for standard users.

To create an ActiveX setting, a new policy must be created based on the ActiveX policy type template.

Note: You will need to import local group policy definitions before editing your Active-X Group Policy Settings.

Firewall

An Application Firewall Policy policy type allows for firewall rules to be applied as an Action in an Application Control Policy.

To create Firewall rules, a new policy must be created based on the Windows Application Policy type template.

When defining the Firewall Policy an Application Classification must be set. An Action of type Application Classification can then apply that classification to an Application Control Policy, which then enforces all of the defined Firewall Policies that are defined with that classification.

General

The policies available on the General tab are covering the basic Privilege Manager functionality and are enabled by default. Most of these policies are fulfilling utility functions otherwise also considered tasks.

Basic Inventory (Initial, Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory. This policy takes an inventory as soon at the agent and the initial policies are deployed and should be removed from the machines afterwards.
Basic Inventory (Initial, Windows)	Instructs computers to report the Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server. This policy takes an inventory as soon at the agent and the initial policies are deployed and should be removed from the machines afterwards.
Basic Inventory (Mac OS)	This scheduled task triggers the Agent to send Mac OS basic inventory.
Basic Inventory (Windows)	Instructs computers to report changes to their Win32_ComputerSystem, Win32_ComputerSystemProduct and Win32_OperatingSystem WMI classes to the server on a scheduled basis, like once a week for example.
Cleanup Agent Inventory Transfers (Windows)	Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.
Cleanup sent Privilege Manager Events (Mac OS)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.
Cleanup sent Privilege Manager Events (Windows)	Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.
Default File Inventory Policy (MacOS)	The purpose of this policy is to inventory software programs running on the managed computer.
Default File Inventory Policy (Windows)	The purpose of this policy is to inventory software programs running on the managed computer.
Ensure UAC Override Setting (Windows)	Ensures that the UAC Override Registry Key is set.
Local User Inventory Policy	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.
Local User Inventory Policy (MacOS)	The purpose of this policy is to inventory Local User account, groups and group membership on the client. This policy can also be used to inventory for specific account privileges.
Perform Resource Discovery (Mac OS)	Schedule on which agents will check with server to determine if any local resources require discovery.
Perform Resource Discovery (Windows)	Schedule on which agents will check with server to determine if any local resources require discovery.
Retry errored TMS Events (Mac OS)	Scan Agent queue for any events that require retransmission.
Retry errored TMS Events (Windows)	Scan Agent queue for any events that require retransmission.

Scheduled Check Pending Client Tasks - Internet Clients (Windows)	Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.
Scheduled Registration - Internet Clients (Windows)	Initiate agent registration with server less frequently than internal clients.
Scheduled Registration (Mac OS)	When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.
Scheduled Registration (Windows)	Initiate agent registration with server.
Update Agent Commands (Mac OS)	When this policy is triggered the Agent will update agent command items.
Update Agent Commands (Windows)	Instructs Agent to update any agent commands if required.
Update Applicable Policies (Mac OS)	When this policy is triggered the Agent will check the server for updated policies.
Update Applicable Policies (Windows)	When this policy is triggered the Agent will check the server for updated policies.
Update Applicable Policies - Internet Clients (Windows)	Instructs Agent to check with server for policy changes less frequently than internal clients.
Update Provisioned Resource Client Items (MacOS)	
Update Provisioned Resource Client Items (Windows)	
User Logon Inventory Policy	Updates user logon data on the given schedule.
Windows Service Inventory Policy	The purpose of this policy is to inventory Windows Services on the client.

Not Enabled

COM Inventory Policy	The purpose of this policy is to inventory COM+ and DCOM packages installed on the client.
Disable Local Guest Accounts	Provisioning policy to disable local Guest accounts on Windows computers.
Randomize Administrator Password	
Shared Folder Inventory Policy	The purpose of this policy is to inventory shared folders on the client.

In Privilege Manager, using a robust filtering system is the key to creating accurate and effective Policies.

A filter is made up of specific criteria that Privilege Manager uses to target important file data (or Events) that occur across your environment. You can think of Filters as the core identifiers in your Privilege Manager system. They are used to identify various levels of activity across your organization's computers, including processes (applications) that are launched on computers, who is executing an application, or the state of the computer that the process is being executed on.

An Event in Privilege Manager is any piece of file data or executable on a computer that is targeted by a policy.

There are different methods for Filter-creation and usage, but if you take the time to familiarize yourself with our out-of-the-box filters they can help make your policy-creation process easy. This article will provide details and descriptions for Windows Filters in Privilege Manager and how you can begin using out-of-the-box Filters, or create your own.

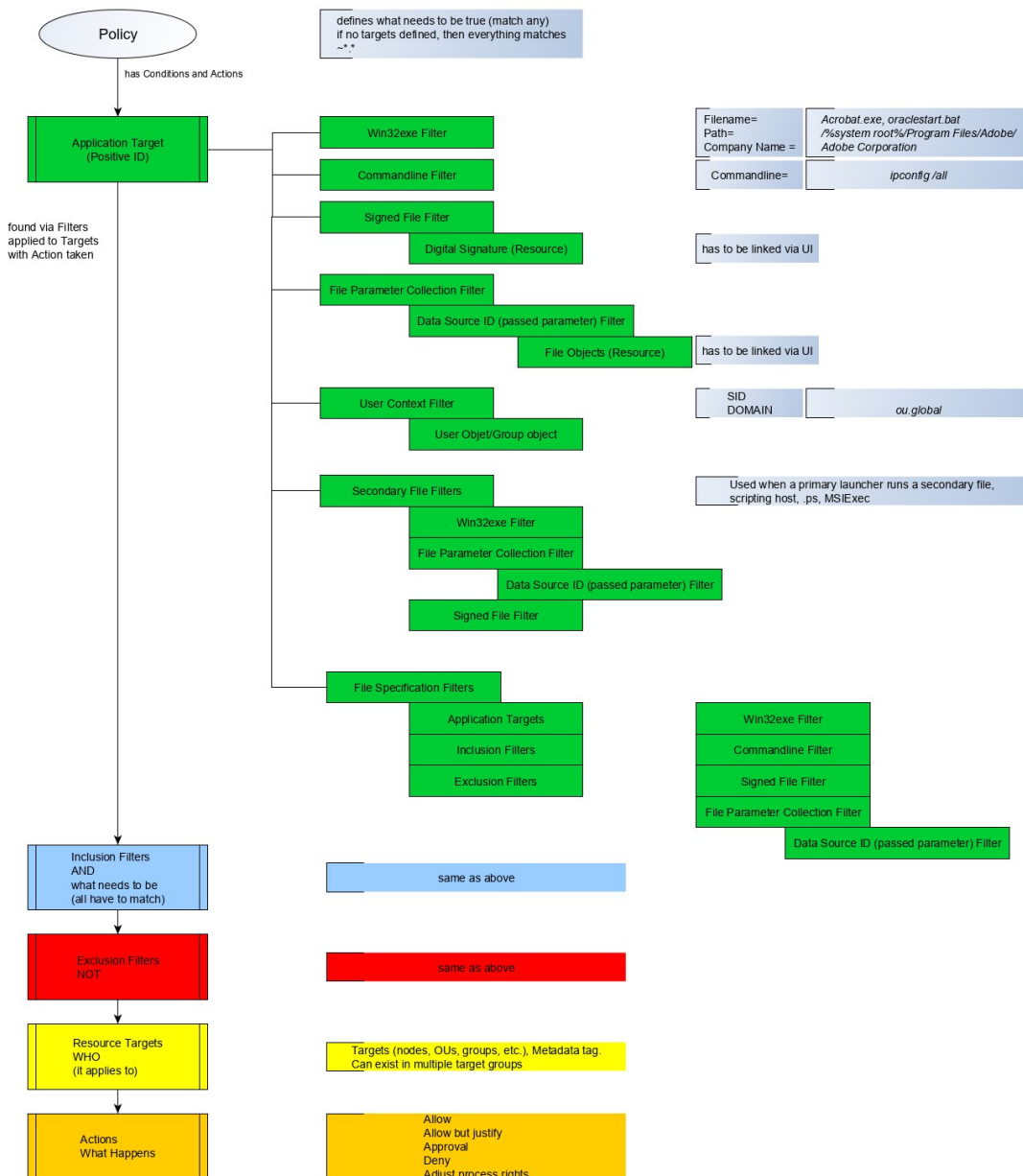
Types of Filters

We recommend leveraging Privilege Manager's out-of-the-box filters to get your policies up and running fast! For a complete list of out-of-the-box filters according to category type, review our Filters' Catalog for Privilege Manager here.

You can search your full list of available filters by navigating to Admin | Filters in Privilege Manager. If you already know what you want to target, simply try typing keywords in the search bar to check whether a filter exists that fits your target goal.

Note: If using the default filters provided with Privilege Manager, always verify existing targeting information.

Review the [Filters Catalog for Privilege Manager](#) for details about all out-of-the-box filters shipped with the product.



Creating New Filters using Event Discovery

One way to begin creating new Filters that identify specific files or applications on your network is to set up a Learning Mode Policy and use the events pulled in by Privilege Manager from actions performed on a test machine. See our User Guide's section on Event Discovery for more information on setting up a Learning Mode Policy.

In Privilege Manager, navigate to Admin | Event Discovery | Files. Under a recognized event, clicking Create Filter should bring you to an Add New Filter page* with the known identifiers needed for targeting this event auto-populated.

*If you are NOT directed to an Add New Filter screen, this means Privilege Manager doesn't have enough information to target this event yet. In these cases you may need to create Filters manually. See section below for Adding New Filters Manually.

This Add New Filter page reveals the available list of building blocks, attributes, or criteria used for creating a Windows' filter. In other words, the following list of criteria are possible data fields that Privilege Manager can look and sift for on any given event that your policies target for Windows machines. Note that criteria can vary depending on the type of filter you are creating:

- File Name
- Path
- Internal Name
- Original File Name
- File Version
- Product Name
- Product Version
- Company Name
- File Signature (File must be signed by)

You can choose which criteria to use by checking or un-checking any of the filter line-items listed above. If you are new to the filter creation process, we recommend experimenting with these different identifiers in your test environment to ensure that you are using a comprehensive list of identifiers in your filter, enough to target the application or file intended but not too specific that variations to your target will fall through the filter's criteria hooks.

Creating a New Filter Manually

Navigate to **Admin | Filters** in Privilege Manager and click **Add Filter**. Under Filter Details, select a platform type and then choose a Filter Type from the dropdown (see our Filters' Catalog for descriptions of filter types). Name your new filter and type a Description, then click Create.

Editing options for this new filter will depend on the type of filter selected.

Creating macOS Filters Manually

Usually when you navigate to the Files Event Discovery View page (**Admin | Event Discovery | Files**) and click **Create Filter**, you are directed to an **Add New Filter** screen. If this does not happen, insufficient information is available. In cases when Privilege Manager does not have enough information from the discovery process, filters have to be created manually.

To manually find granular information required for targeting applications in Privilege Manager on a macOS endpoint,

1. Right-click the target application and select **Show Package Contents**.
2. Navigate to **Contents | Info.plist**, this gives you a coded list of items that you can match into the details page of your Filter.

For example, the highlighted section below can be entered into the **Bundled Identifier** line item when creating a Firefox filter.

```

Info.plist
<string>idcom.apple.firefox</string>
</array>
<key>CFBundleTypeIconName</key>
<string>Mozilla_Visual_WebUI</string>
<key>CFBundleTypeRole</key>
<string>Viewer</string>
</dict>
</array>
<key>CFBundleExecutable</key>
<string>Firefox</string>
<key>CFBundleIdentifier</key>
<string>Firefox 50.0.1</string>
<key>CFBundleIconFile</key>
<string>Firefox.icns</string>
<key>CFBundleIconName</key>
<string>Firefox</string>
<key>CFBundleName</key>
<string>Firefox</string>
<key>CFBundlePackageType</key>
<string>APPL</string>
<key>CFBundleShortVersionString</key>
<string>50.0.1</string>
<key>CFBundleSignature</key>
<string>MOZ</string>
<key>CFBundleURLTypes</key>
<array>
<dict>
<key>CFBundleURLIconFile</key>
<string>com.apple.firefox</string>
<key>CFBundleURLName</key>
<string>http://www.mozilla.org</string>
<key>CFBundleURLSchemes</key>
<array>
</array>
</dict>
</array>
</dict>
<key>CFBundleIconFile</key>
<string>com.apple.firefox</string>
<key>CFBundleName</key>
<string>http://www.mozilla.org</string>
<key>CFBundleURLSchemes</key>
<array>
</array>

```

Create A Copy - How to Use Filter Templates

Out-of-the-Box filters are designed to be used as templates, meaning when you open these filters you will see a Create A Copy button rather than the option to immediately Edit. These filter templates are protected to provide a jumping off point whenever creating new filters. They are formed by specific criteria that you can tailor according to your specific use case after copying.

Keep in mind that every filter in Privilege Manager - whether or not it is a template - can be leveraged by the Copying feature.

Filter Types and Descriptions

There are different types of filters. When creating a new filter for Windows or macOS, the "Filter Type" dropdown gives you a list of options that include the categories:

- [Application Filters](#)
- [File Filters](#)
- [Inventory Filters - Windows only option](#)
- [macOS Specific Filters](#)

These are loose groupings that signify a few different approaches to the filtering method or targets.

Common Filter Characteristics

Each filter has a Details area that contains the filter name, description, and platform association. These details are usually specified when you create the filter, either by choosing the New Filter button, editing an existing filter, or making a copy of an existing filter.

Those characteristics are used for searches or filtering and allow users to easily find existing filters.

Application Filters

These generally target specific executables or things about the environment. These types of filters can be used to limit policies to a certain time of day, the parent process of an application, the security rating of an application, or the user or group running the process.

The following Application Filter type filter topics are available:

- [Blank Win32 Executable Filter](#)
- [Commandline Filter](#)
- [Download Source Filter](#)
- [Environment Filter](#)
- [Network Location Filter](#)
- [Parent Process Filter](#)
- [Secondary File Filter](#)
- [Security Rating Filter](#)
- [Signed File Filter](#)
- [Time Of Day Filter](#)
- [User Context Filter / User Context Filter via SID](#)

Blank Win32 Executable Filter

Identifies specific application files by specifications like name, path, and when first discovered.

Filter > New Win32 Executable Filter

Details Related Items Change History

Details

Name	New Win32 Executable Filter
Description	
Platform	Windows

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name ⓘ

File Path ⓘ

Include subdirectories

First Discovered

Anytime

In the last

0 minute(s)

File Details

To only match files with specific properties in the file details, enter those values in the fields below. A wildcard character (*) included in the set.

Internal name ⓘ

Original filename ⓘ

File version ⓘ

Product name ⓘ

Product version ⓘ

Company name ⓘ

Copyright ⓘ

Back Edit Create a Copy Delete View as XML

Parameters

Win32 Executable filters have two sets of parameters:

- **File Specifications**, such as
 - File Name
 - File Path with option to include subdirectories
 - First Discovered, which can specified as "Anytime" or "In the last" either Minutes, Hours, Days, or Weeks.
- **File Details** (common attributes), such as
 - Internal name
 - Original filename
 - File version
 - Product name
 - Product version
 - Company name
 - Copyright (version 10.7 and up)

Examples

Used to target specific applications, for example allowing `acrobat.exe` or `notepad++.msi` to be used on endpoints.

Commandline Filter

These filters will perform an exact, partial or regex match on the commandline of the process. Privilege Manager comes with default commandline filter types, which are all read-only, but can be copied to be customized.

This filter is available for both Windows and macOS systems.

Search for Commandline Filters

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Type** column enter commandline.

Filters

[Add Filter](#)

NAME	DESCRIPTION	TYPE ^
<input type="text" value="Filter"/>	<input type="text" value="Filter"/>	<input type="text" value="commandline"/>
Add Printer Commandline Arguments	Filter used to identify the Add Printer UI applet.	Commandline Filter
azman.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Authorization Manager	Commandline Filter
Backup and Restore Commandline Arguments	Filter used to identify the Backup and Restore component, used as a commandline argument to a process.	Commandline Filter
certmgr.msc Commandline Filter for MMC Snap-in	Filter used to detect Windows Certificate Manager	Commandline Filter
ciadv.msc Commandline Filter for MMC Snap-in	Filter used to detect Indexing Service Management	Commandline Filter
compmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect Computer Management	Commandline Filter
Defragment Component (dfrg.msc)	Identifies the MMC snap-in used to defragment disks in Windows XP.	Commandline Filter
devmgmt.msc Commandline Filter for MMC Snap-in	Filter used to detect Device Manager	Commandline Filter

3. Select a filter to view its details and/or create a copy to customize the filter.

Filter > Network Enable or Disable Elevate Attempt

i This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Details

Name Network Enable or Disable Elevate Attempt

Description Filter used to detect when a user right-clicks on a network adapter and selects Enable or Disable

Settings

Match Type v

Command Line /AdminProxy:{BA126F01-2166-11D1-B1D0-00805FC1270E}

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

Create a new Commandline Type Filter

1. Navigate to **Admin | More...** and select **Filters**.
2. Click **Add Filter**.
3. On the New Filter page, select the platform. For this example, select **Windows**.
4. From the **Filter Type** drop-down select **Commandline Filter**.
5. Enter a name and description and click **Create**.
6. Click Edit on the newly created filter page to customize.

Filter > New Commandline Filter

Details Related Items Change History

Details

Name * New Commandline Filter

Description testing new cmdline filter

Platform Windows

Settings

Match Type Exact Match

Command Line

Exact Match
Partial Match
Regular Expression

Save Cancel Export

7. Click **Save**.

Parameters

Commandline Filters have one section to set the parameters for the filter.

The **Match Type** gives you the options:

- Exact Match
- Partial Match
- Regular expression

Command Line:

- This is the section where you would enter in the given command parameters to pull up the file or action.

Examples

A commandline filter examines the commandline (excluding the primary executable) and applies a pattern match (Exact, Partial or Regular Expression).

For example allowing /FlushDNS as a command for IPConfig.

Download Source Filter

The filter checks where a file is being downloaded from. This filter allows you to identify specific download sources, and allows the ability to whitelist sources you trust or block sources you don't. *No out-of-box filters exist in Privilege Manager for this type.*

Filter > New Download Source

[Details](#) [Related Items](#)

Details

Name New Download Source

Description

Settings

This filter checks for the existence of download source information associated with a file.

Include files that contain any download source information

Include files that contain specific download source information

Match Type

Host

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [View as XML](#)

This filter is available for both Windows and macOS systems.

Parameters

The filter checks for the existence of download source information associated with a file.

Settings:

- Include files that contain any download source information
- Include files that contain specific download source information
- Match type
- Host

Examples

This filter would allow you to control what download sources should be allowed or blocked.

Environment Variable Filter

This type of filter can target environment variables of a process that is started.

□

Parameters

Filter > New User Requested Run As Administrator

Details Related Items

Details

Name • New User Requested Run As Administrator

Description Detects whether a user has right-clicked on an application and used Privilege Manager's custom 'Request Run as Administrator' option

Settings

Name ACSRUNASADMIN

Value

Match Type

- Name
- Value
- Match Type

Examples

A environment variable filter type detects whether a user has right clicked on an application and used Privilege Manager's custom *Request Run as Administrator* option.

Network Location Filter

This type of filter identifies a computer's connection to specific networks like public, private, or unclassified networks.

Filter > New Domain Network Location Filter

[Details](#) [Related Items](#)

Details

Name: New Domain Network Location Filter
Description: Filter to detect when the computer is attached to a network classified as domain

Settings

Only allow network connections of type: Domain

Network Connectivity
Include connections where

<input type="checkbox"/> IPv4 Internet	is	undetected
<input type="checkbox"/> IPv4 Local Network	is	undetected
<input type="checkbox"/> IPv4 Subnet	is	undetected
<input type="checkbox"/> IPv4 No Traffic	is	undetected
<input type="checkbox"/> IPv6 Internet	is	undetected
<input type="checkbox"/> IPv6 Local Network	is	undetected
<input type="checkbox"/> IPv6 Subnet	is	undetected
<input type="checkbox"/> IPv6 No Traffic	is	undetected

Results should be: Excluded

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#)

Parameters

You can adjust the following setting options for Network Location filters:

- **Only allow network connections of type:**

- Public
- Private
- Domain

- **Network Connectivity:**

- IPv4 and IPv6 options for connectivity

- **Results should be:**

- Included or excluded

Examples

Some examples of this filter can be set to detect:

- when the computer is not attached to a network
- when the computer is attached to a network classified as public
- when the computer is attached to a network classified as domain

Filter > New Private Network Location Filter

[Details](#) [Related Items](#)

Details

Name: New Private Network Location Filter
Description: Filter to detect when the computer is attached to a network classified as private

Settings

Only allow network connections of type: Private

Network Connectivity
Include connections where

<input type="checkbox"/> IPv4 Internet	is	undetected
<input type="checkbox"/> IPv4 Local Network	is	undetected
<input type="checkbox"/> IPv4 Subnet	is	undetected
<input type="checkbox"/> IPv4 No Traffic	is	undetected
<input type="checkbox"/> IPv6 Internet	is	undetected
<input type="checkbox"/> IPv6 Local Network	is	undetected
<input type="checkbox"/> IPv6 Subnet	is	undetected
<input type="checkbox"/> IPv6 No Traffic	is	undetected

Results should be: Excluded

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#)

Parent Process Filter

This type of filter can identify parent processes of certain executables.

Filter > New Privilege Manager Copy/Installer Helper Parent Process Filter

Details Related Items

Details

Name + New Privilege Manager Copy/Installer Helper Parent Process Filter

Description Filter to detect when a user attempts to copy a file using the Privilege Manager copy helper. Use this filter in policies.

Platform Mac OS

Settings

Applications + Add • Privilege Manager Copy/Installer Helper Application

Conditions (optional)

Include Only Filters + Add None Selected

Exclude Any Filters + Add None Selected

Save Cancel

This filter is available for both Windows and macOS systems.

Parameters

- Applications
- Conditions
- Include only filters
- Exclude only filters

Examples

This filter is used to detect when a user attempts to copy a file using the Privilege Manager copy helper.

Using Secondary File Filters

This topic explains how to create policies for applications that trigger file executions. Implementing a policy to filter on a file type, which is used by another executable, is done by setting a **Secondary File Filter**. The Secondary File Filter is available for both Windows and macOS systems.

This article shows the steps used to create filters and policies that enforce actions on endpoints when batch files, PowerShell scripts, or Microsoft Installer files execute. Any type of executer can be specified and policed this way.

In general, the steps are similar for the different file types to be policed.

- You first create an application or file filter that identifies the executing application, for example *.ps1,
- then you create the secondary file filter identifying the file type by adding the file or application filter (*.ps1) under Settings,
- then you create a policy, specifying Application Targets, and
- use an Inclusion and/or Exclusion filter specified as and using the Secondary File Filter.

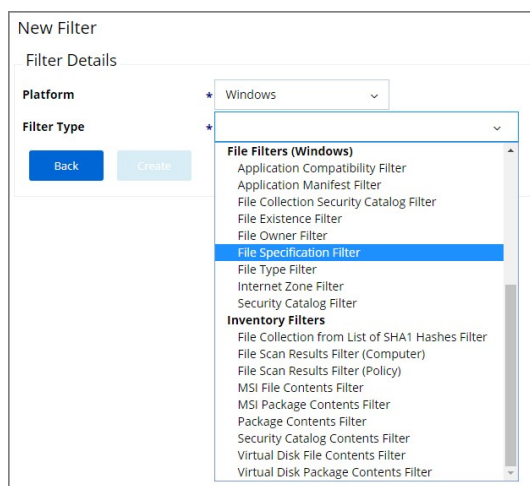
The following three examples show how to setup file filters to deny running single files, such as a .bat, .ps1, and .msi.

Batch File Example

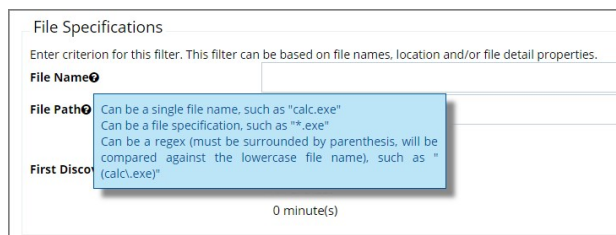
Creating the File Filter for .bat Files

In this example we are creating a filter for the target executing .bat files.

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **File Specification Filter**. This also allows you to link in hashes or signatures.



5. Enter the name and a description for the filter, for example "test.bat" and "filter for batch files".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under File Specifications in the File Name field enter either a single file name, file specification, or RegEx.



For this example, we use **test.bat** to police a single file name.

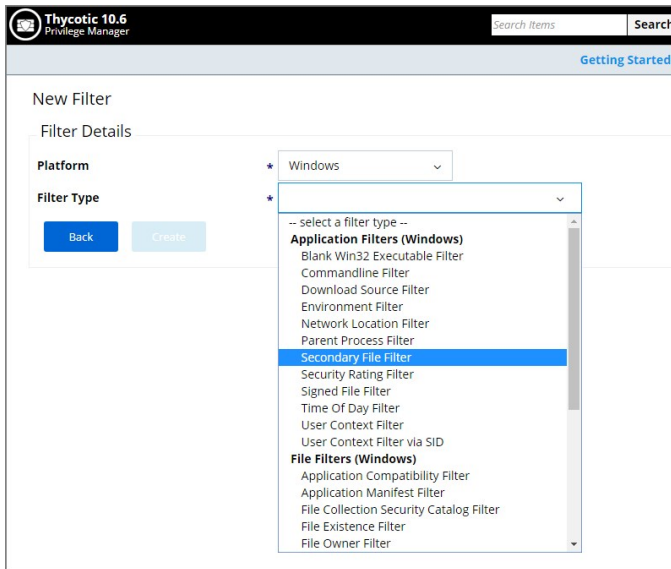
9. Verify that First Discovered is set to **Anytime**.
10. Click **Save**.

Creating the Secondary Filter

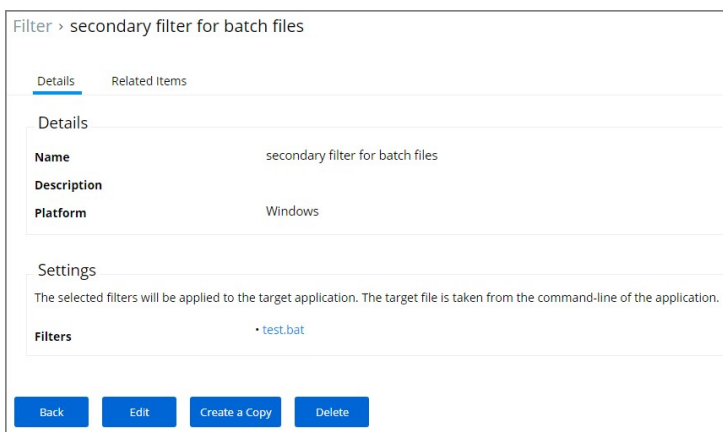
In this example we are creating the secondary file filter.

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.

- From the Filter Type drop*down select **Secondary File Filter**.



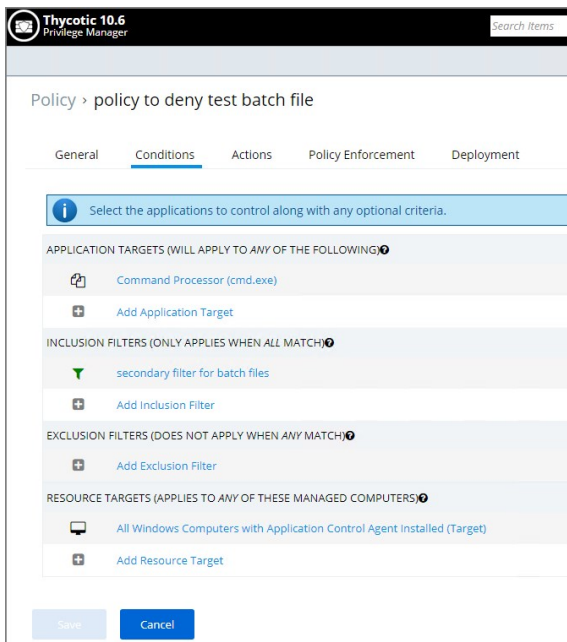
- Enter the name and a description for the filter, for example "secondary file filter for batch files".
- Click **Create**.
- The page for the new filter opens, click **Edit**.
- Under Settings click **+Add** to add the test.bat filter created in "Creating the File Filter for .bat" procedure.



- Click **Save**.

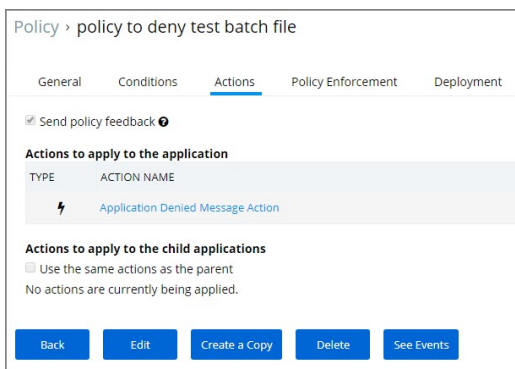
Creating the Policy

- Navigate to **Admin | Policies**.
- Click **Add New Policy**.
- From the Platform drop*down select **Windows**.
- From the Policy Type drop*down select **Show All Templates**.
- From the Template Type drop*down select **Other: Empty Policy**.
- Enter a Name and Description, click **Create**.
- Click **Edit**.
- On the **General** tab in the Status area set the policy to **Enabled**.
- Select the **Conditions** tab.
- Under Application Targets click **+ Add Application Target**.
- In Search, enter command and select **Command Processor (cmd.exe)** from the list, click **Add**.
- Under Inclusion Filters click **+ Add Inclusion Filter**.
- In Search, enter secondary and select **secondary filter for batch files** from the list, click **Add**. This is the filter you created in the "Creating the Secondary Filter" procedure above.



Resource Targets are automatically added based on the policy template selected.

14. Select the **Actions** tab.
15. Enable Send policy feedback.
16. Under Actions to apply to the application click **+ Add Action**.
17. Select **Application Denied Message Action** from the list, click **Add**.



18. Click **Save**.

PowerShell Script Example

In this example we are creating a policy to deny running a test.ps1 file.

Creating the File Filter for .ps1 Files

In this example we are creating a filter for the target executing .ps1 files.

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **File Specification Filter**. This also allows you to link in hashes or signatures.

New Filter

Filter Details

Platform: Windows

Filter Type: File Specification Filter

File Filters (Windows)

- Application Compatibility Filter
- Application Manifest Filter
- File Collection Security Catalog Filter
- File Existence Filter
- File Owner Filter
- File Specification Filter**
- File Type Filter
- Internet Zone Filter
- Security Catalog Filter

Inventory Filters

- File Collection from List of SHA1 Hashes Filter
- File Scan Results Filter (Computer)
- File Scan Results Filter (Policy)
- MSI File Contents Filter
- MSI Package Contents Filter
- Package Contents Filter
- Security Catalog Contents Filter
- Virtual Disk File Contents Filter
- Virtual Disk Package Contents Filter

5. Enter the name and a description for the filter, for example "test.ps1" and "filter for powerscript files".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under File Specifications in the File Name field enter either a single file name, file specification, or RegEx.

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name

File Path

Can be a single file name, such as "calc.exe"
 Can be a file specification, such as "**.exe"
 Can be a regex (must be surrounded by parenthesis, will be compared against the lowercase file name), such as "(calc.exe)"

First Discovered: 0 minute(s)

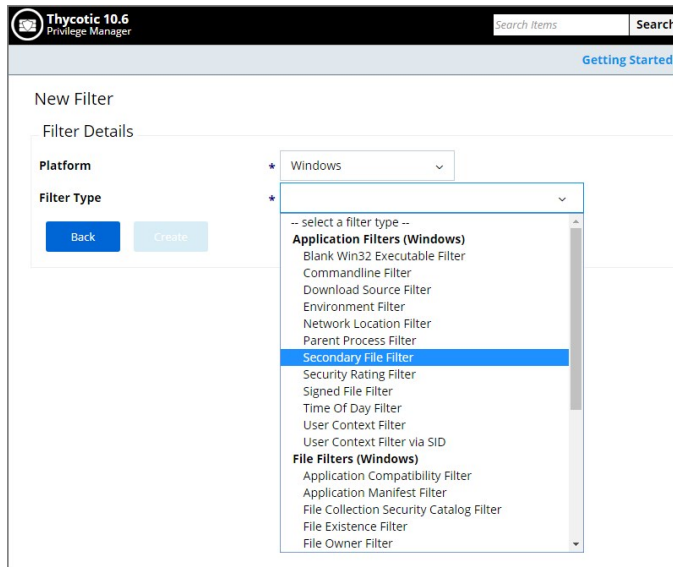
For this example, we use **test.ps1** to police a single file name.

9. Verify that First Discovered is set to **Anytime**.
10. Click **Save**.

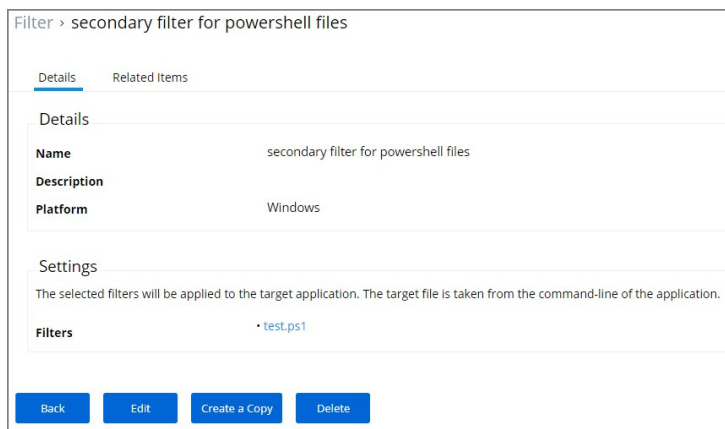
Creating the Secondary Filter

In this example we are creating the secondary file filter.

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS. Windows** or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **Secondary File Filter**.



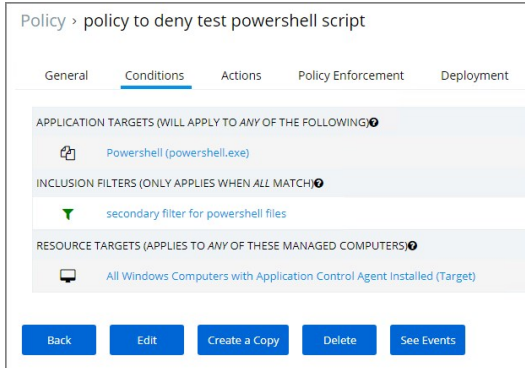
5. Enter the name and a description for the filter, for example "secondary file filter for PowerShell files".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under Settings click **+Add** to add the test.ps1 application filter created in "Creating the File Filter for .ps1 Files" procedure.



9. Click **Save**.

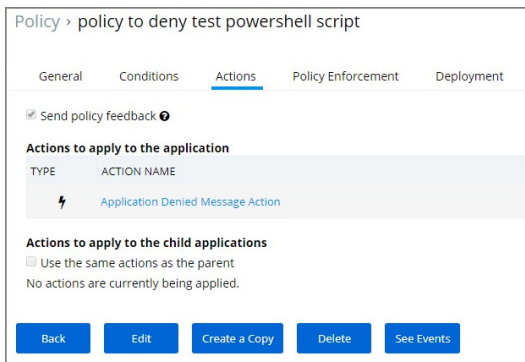
Creating the Policy

1. Navigate to **Admin | Policies**.
2. Click **Add New Policy**.
3. From the Platform drop*down select **Windows**.
4. From the Policy Type drop*down select **Show All Templates**.
5. From the Template Type drop*down select **Other: Empty Policy**.
6. Enter a Name, for example "policy to deny test PowerShell script" and Description, click **Create**.
7. Click **Edit**.
8. On the **General** tab in the Status area set the policy to **Enabled**.
9. Select the **Conditions** tab.
10. Under Application Targets click **+ Add Application Target**.
11. In Search, enter command and select **Powershell (PowerShell.exe)** from the list, click **Add**.
12. Under Inclusion Filters click **+ Add Inclusion Filter**.
13. In Search, enter secondary and select **secondary filter for PowerShell files** from the list, click **Add**. This is the filter you created in the "Creating the Secondary Filter" procedure above.



Resource Targets are automatically added based on the policy template selected.

14. Select the **Actions** tab.
15. Enable Send policy feedback.
16. Under Actions to apply to the application click **+ Add Action**.
17. Select **Application Denied Message Action** from the list, click **Add**.



18. Click **Save**.

MSI File Example

In this example we are creating a policy to deny running a test.msi file.

Creating the File Filter for .msi Files

In this example we are creating a filter for the target executing .msi files.

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **File Specification Filter**. This also allows you to link in hashes or signatures.

New Filter

Filter Details

Platform: Windows

Filter Type: File Specification Filter

File Filters (Windows)

- Application Compatibility Filter
- Application Manifest Filter
- File Collection Security Catalog Filter
- File Existence Filter
- File Owner Filter
- File Specification Filter**
- File Type Filter
- Internet Zone Filter
- Security Catalog Filter

Inventory Filters

- File Collection from List of SHA1 Hashes Filter
- File Scan Results Filter (Computer)
- File Scan Results Filter (Policy)
- MSI File Contents Filter
- MSI Package Contents Filter
- Package Contents Filter
- Security Catalog Contents Filter
- Virtual Disk File Contents Filter
- Virtual Disk Package Contents Filter

5. Enter the name and a description for the filter, for example "test.msi" and "filter for msi files".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under File Specifications in the File Name field enter either a single file name, file specification, or RegEx.

File Specifications

Enter criterion for this filter. This filter can be based on file names, location and/or file detail properties.

File Name

File Path

Can be a single file name, such as "calc.exe"
 Can be a file specification, such as "*.exe"
 Can be a regex (must be surrounded by parenthesis, will be compared against the lowercase file name), such as "(calc.exe)"

First Discovered: 0 minute(s)

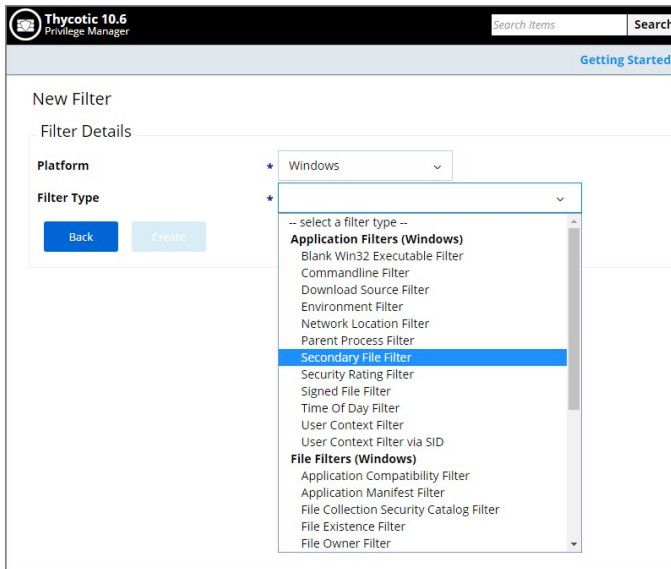
For this example, we use **test.msi** to police a single file name.

9. Verify that First Discovered is set to **Anytime**.
10. Click **Save**.

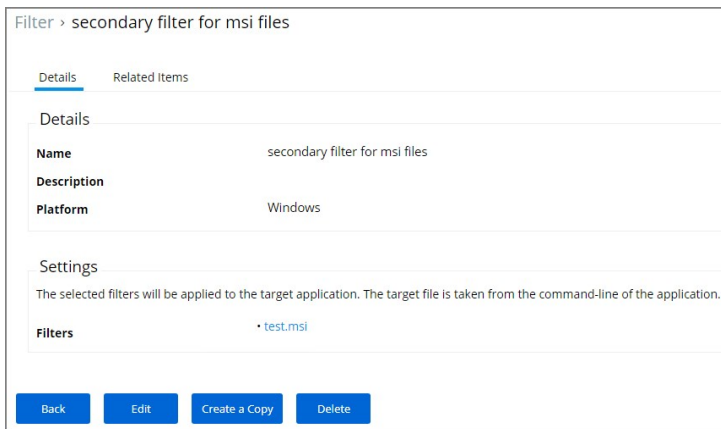
Creating the Secondary Filter

In this example we are creating the secondary file filter.

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **Secondary File Filter**.



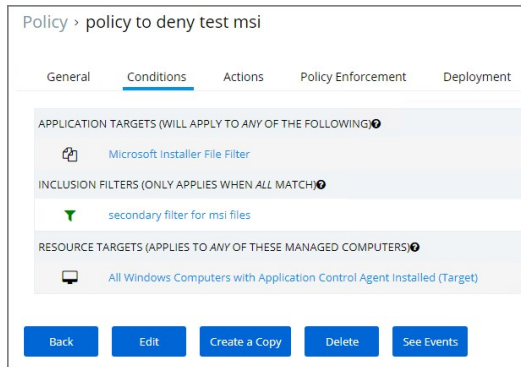
5. Enter the name and a description for the filter, for example "secondary file filter for msi files".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under Settings click **+Add** to add the test.msi application filter created in "Creating the File Filter for .msi Files" procedure.



9. Click **Save**.

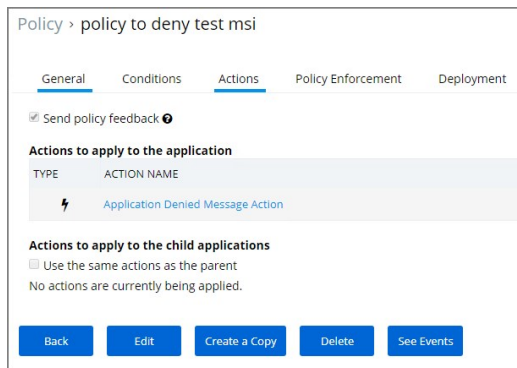
Creating the Policy

1. Navigate to **Admin | Policies**.
2. Click **Add New Policy**.
3. From the Platform drop*down select **Windows**.
4. From the Policy Type drop*down select **Show All Templates**.
5. From the Template Type drop*down select **Other: Empty Policy**.
6. Enter a Name and Description, click **Create**.
7. Click **Edit**.
8. On the **General** tab in the Status area set the policy to **Enabled**.
9. Select the **Conditions** tab.
10. Under Application Targets click **+ Add Application Target**.
11. In Search, enter command and select **Microsoft Installer File Filter** from the list, click **Add**.
12. Under Inclusion Filters click **+ Add Inclusion Filter**.
13. In Search, enter secondary and select **secondary filter for msi files** from the list, click **Add**. This is the filter you created in the "Creating the Secondary Filter" procedure above.



Resource Targets are automatically added based on the policy template selected.

14. Select the **Actions** tab.
15. Enable Send policy feedback.
16. Under Actions to apply to the application click **+ Add Action**.
17. Select **Application Denied Message Action** from the list, click **Add**.



18. Click **Save**.

Best Practices

As a best practice you create an elevate policy with a priority of X (for example 20) to elevate or allow specific scripts or files to run. Then you add a policy with a priority of X+1 (for this example 21) to deny any other execution of the command processor, PowerShell, or Microsoft installer files. For this example .msi is used.

Creating the Allow notepad

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **File Specification Filter**.

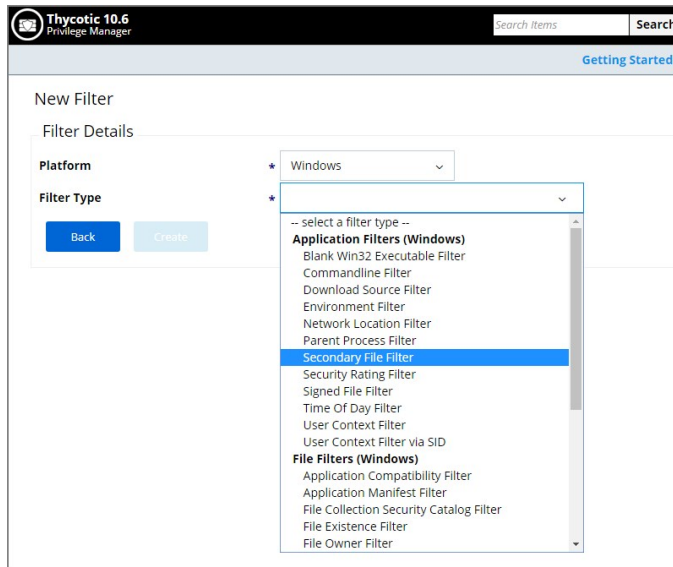
5. Enter the name and a description for the filter, for example "notepad+*.msi"
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under File Specifications in the File Name field enter either a single file name, file specification, or RegEx.

For this example, we use RegEx (**notepad+.*[az09\.,]+**) to elevate any Notepad++ version.

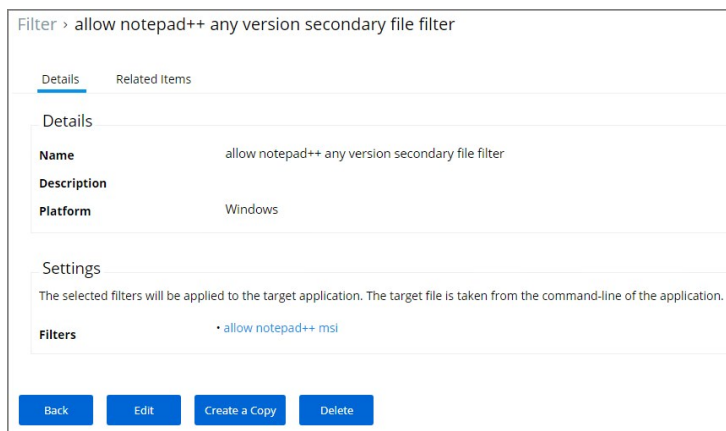
9. Verify that First Discovered is set to **Anytime**.
10. Click **Save**.

Creating the Secondary Filter

1. In the Privilege Manager Console navigate to **Admin | More | Filters**.
2. On the Filter page, click **Add New Filter**.
3. On the New Filter page, select the platform. This can be either **Both Windows / Mac OS, Windows**, or **Mac OS**. For this example, select **Windows**.
4. From the Filter Type drop*down select **Secondary File Filter**.



5. Enter the name and a description for the filter, for example "secondary file filter for notepad++ msi files".
6. Click **Create**.
7. The page for the new filter opens, click **Edit**.
8. Under Settings click **+Add** to add the **notepad++*.msi** application filter created in "Creating the Allow notepad++*.msi Filter" procedure.



9. Click **Save**.

Creating the Allow a Specific .msi File to Run Policy

1. Navigate to **Admin | Policies**.
2. Click **Add New Policy**.
3. From the Platform drop*down select **Windows**.
4. From the Policy Type drop*down select **Show All Templates**.
5. From the Template Type drop*down select **Other: Empty Policy**.
6. Enter a Name and Description, click **Create**.
7. Click **Edit**.
8. On the **General** tab in the Status area set the policy to **Enabled**.
9. Select the **Conditions** tab.
10. Under Application Targets click **+ Add Application Target**.
11. In Search, enter command and select **Microsoft Installer File Filter** from the list, click **Add**.
12. Under Inclusion Filters click **+ Add Inclusion Filter**.
13. In Search, enter secondary and select the **allow notepad++ any version secondary file filter** created in "Creating the Secondary Filter" procedure steps, click **Add**.

Policy > allow notepad++ msi

General Conditions Actions Policy Enforcement Deployment

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

Microsoft Installer File Filter

INCLUSION FILTERS (ONLY APPLIES WHEN ALL MATCH)

allow notepad++ any version secondary file filter

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS)

All Windows Computers with Application Control Agent Installed (Target)

Back Edit Simple Policy View Create a Copy Delete See Events

Targets are automatically added based on the policy template selected.

14. Click **Save**.

Creating the .msi Deny Policy

1. Navigate to **Admin | Policies**.
2. Click **Add New Policy**.
3. From the Platform drop* down select **Windows**.
4. From the Policy Type drop* down select **Blacklist / Deny Application Execution**.
5. From the Template Type drop* down select the **Blacklist: Deny Specific Applications**.
6. Enter a Name, for example "deny .msi execution" and Description.

New Policy

Platform * Windows

Policy Type * Blacklist / Deny Application Execution

Template Type * Blacklist: Deny Specific Applications

Name * deny .msi execution

Description This policy prevents processes from running.

Back Create

7. Click **Create**.
8. Click **Edit**.
9. On the **General** tab in the Status area set the policy to **Enabled**.
10. Set the **Policy Priority** to **21**.
11. Select the **Blacklist** tab.
12. Select **Modal Deny Message** and keep the selection for **Send Event Feedback to Server**.
13. Click **Add Existing File Filter**.
14. Search for Microsoft and select **Microsoft Installer File Filter**, click **Add**.

Once added this filter is listed as msixec.exe in the list. Targets are automatically added based on the policy template selected.

15. Click **Save**.

Updating the Endpoints with the Policies

After adding new filters and policies, the endpoints need to be updated to enforce the new rules.

This can be done directly:

1. On the Policy Details page select the **Deployment** tab.
2. Click **Run Policy Targeting Update**.

From any other location in the Privilege Manager console follow these steps:

1. Navigate to **Admin I Config**
2. Select the **General** tab.
3. Click **Policy Targeting Update**.

RegEx Examples

When using RegEx instead of a single file name or file specification, make sure to verify the syntax and test your filter before using it in production.

Program name with version in file name:

(flashutil[a-zA-Z0*9\.\.]+exe)

Winamp58_3660_beta_full_en*.us

(winamp[a-zA-Z0*9\.\.]+exe)

Wiresharkwin642.6.6.exe

(wireshark*win64[a-zA-Z0*9\.\.]+exe)

Security Rating Filter

If you have integrated Privilege Manager with a Reputation Checking provider like VirusTotal, these filters allow you to look up a rating for a file or application (is it good, bad, suspect/suspicious, or unknown).

New Filter

Filter Details

Platform * Windows

Filter Type * Security Rating Filter

Name * New Security Rating Filter

Description

Security rating system [View Parameters](#)

*Application Control Rating System

Select	Name	Resource Type	Description	CreatedDate
<input type="checkbox"/>				month/day/yea ...
<input type="checkbox"/>	Application Control Rating System	Security Rating	Application Control Rating System	5/31/19, 12:52 PM
<input type="checkbox"/>	Cylance Rating System	Security Rating	Security Rating System for Application Control Cylance	5/31/19, 1:01 PM
<input type="checkbox"/>	VirusTotal Rating System	Security Rating	Security Rating System for Application Control VirusTotal	5/31/19, 1:01 PM

10 items per page 1 - 3 of 3 items

This filter is available for both Windows and macOS systems.

Parameters

Filter > Virustotal Security Rating Filter

[Details](#) [Related Items](#) [Change History](#)

Details

Name * Virustotal Security Rating Filter

Description

Platform Windows

Settings

Security Rating System * VirusTotal Rating System

Rating Level * Bad

Timeout * Unknown cond(s)

Error Handling

On timeout, consider the result * Bad

On failure, consider the result * Error Condition

The parameters for the Security Rating Filter would include the following:

- Security Rating System
- Rating level
- Timeout
- Error Handling
 - On timeout, consider the result
 - On Failure, consider the result

Examples

The example above displays how to create a security rating filter after integrating Privilege Manager with VirusTotal.

Signed File Filter

This filter allows you to associate one or more Digital Certificate(s) that are trusted and verify that an application or file is signed by one of those certificates. *No out-of-box filters exist in Privilege Manager for this type.*

Filter > New Signed File Filter

Details Related Items Change History

Details

Name * New Signed File Filter

Description Includes only files that are signed by the specified digital certificates.

Platform Windows

Settings

Digital Certificates + Add None Selected

Subject Name

Save Cancel

These filters can be used in several of the following ways:

- A target for ACS policies
- A parameter to prevent spoofing

Signed Application filters identify applications based on their digital certificates.

This filter is available for both Windows and macOS systems.

Parameters

Under Settings users:

- add one or more digital certificates, which are discovered via inventory.
- enter a Subject Name (version **10.7 and up**). If Subject Name is specified, the digital certificates above will be ignored. The following three match types are supported:
 - The * character can be pre- or post- appended to a string to perform a begins with or ends with match (i.e. Microsoft*).
 - Lower-case RegEx is also supported and must be surrounded with parenthesis. (i.e. (micro.*))
 - Setting the subject name to * will match any file signed with a valid certificate. (**Not recommended by Thycotic**)

Examples

Adobe (TM) requires several certificates that are used to sign applications.

Because of this, you may want all applications signed by Adobe to be whitelisted, so that a signed application filter targeting Adobe Certificates allows all applications signed by Adobe to run.

Targeting the latest Adobe Flash Installer via a Win32 Executable filter and then using the application filter ensures that the application really is the adobe flash installer. The Signed Application Filter works as a validation filter for applications.

Time of Day Filter

This type of filter exists to create policy parameters for specific time frames.

Filter > New Business Hours (8:30AM to 5:30PM)

[Details](#) [Related Items](#)

Details

Name New Business Hours (8:30AM to 5:30PM)

Description This filter is limited to 8:30AM to 5:30PM weekdays

Settings

Same Period Every Day

From to

Different Periods on Different Days

Sunday from to

Monday from to

Tuesday from to

Wednesday from to

Thursday from to

Friday from to

Saturday from to

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#)

This filter is available for both Windows and macOS systems.

Parameters

The time of day filter has two different settings to allow you to set time and day allowances.

- Same period everyday from
- Different Periods on Different Days

Examples

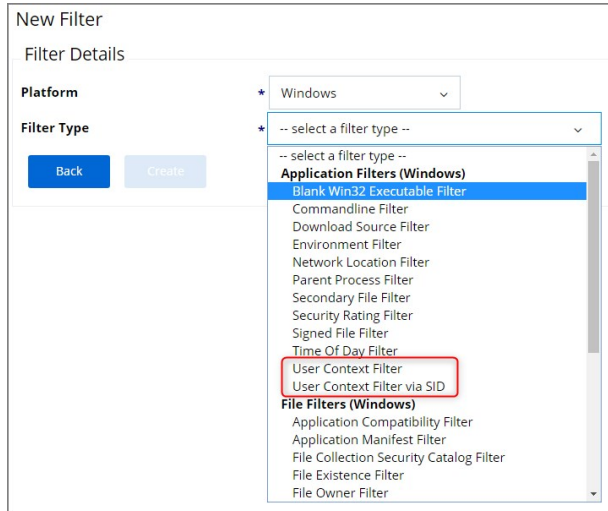
You can use the time of day filter in a policy to only pickup specific times or days of the week.

Using User Context Filters

User Context Filters are used in a policy as either an

- inclusion filter, to specify that the policy only applies to users in a specific AD Group
- exclusion filter, to specify that the policy applies to everyone except the users in a specific AD Group.

The User Context Filters are part of the Application Filter templates listed for Windows:



This filter is available for both Windows and macOS systems.

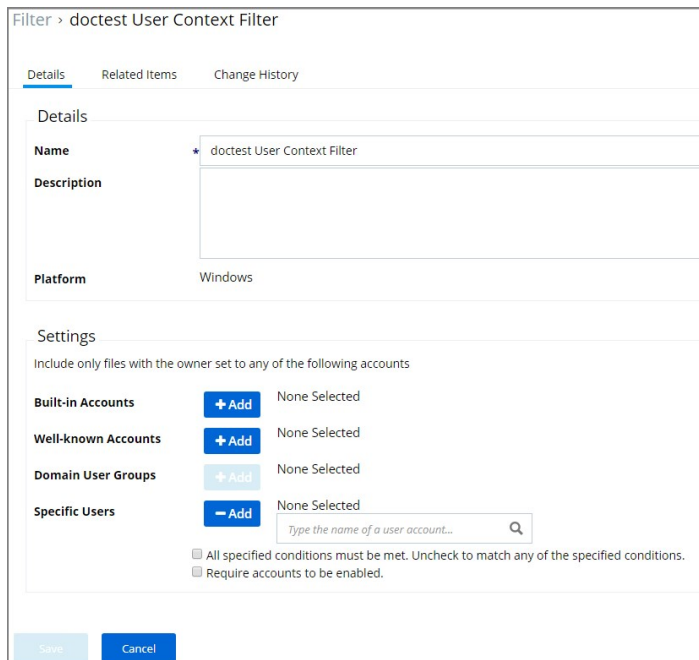
On-Premise

For Privilege Manager on-premises the **User Context Filter** can be used after the Active Directory synchronization completes. When creating and editing the filter, add any

- Build-in Accounts,
- Well-known Accounts, and/or
- Domain User Groups, or
- Specific Users.

to specifically select user context.

Then select if **ALL** conditions must be met. Leave the box unchecked to match **ANY**. You can also specify, if accounts must be enabled to be targeted. This is an important checkbox to set if specific users have been added.



Cloud

For Privilege Manager cloud the **User Context Filter via SID** can be used if (Azure) AD synchronization has not been set up but the SID of the group is known. When creating the filter, enter the

- Group SID, and
- Group Name, to name the group if it does not exist.

New Filter

Filter Details

Platform Windows

Filter Type User Context Filter via SID

Filter Name doctext New User Context Filter

Group SID

Group Name DOMAIN\GROUPNAME

[Back](#) [Create](#)

Filter > DOMAIN\GROUPNAME - User Context Filter

[Details](#) [Related Items](#) [Change History](#)

Details

Name	DOMAIN\GROUPNAME - User Context Filter
Description	Filter to target applications launched by users in the DOMAIN\GROUPNAME user group
Platform	Windows

Settings

Include only files with the owner set to any of the following accounts

Built-in Accounts [+ Add](#) None Selected

Well-known Accounts [+ Add](#) None Selected

Domain User Groups [+ Add](#) None Selected

Specific Users [+ Add](#) None Selected

[Q](#)

- All specified conditions must be met. Uncheck to match any of the specified conditions.
- Require accounts to be enabled.

[Save](#) [Cancel](#)

File Filters

These target specific file information. File Filters can be used to target the file owner of the application, the type of file, the application manifest of the file, or whether the application is present in the signed security catalog (Operating System Files).

The following File Filter type filter topics are available:

- [Application Compatibility Filter](#)
- [Application Manifest Filter](#)
- [File Collection Security Catalog Filter](#)
- [File Existence Filter](#)
- [File Owner Filter](#)
- [File Specification Filter](#)
- [File Type Filter](#)
- [Internet Zone Filter](#)
- [Security Catalog Filter](#)

Application Compatibility Filter

This type of filter identifies the rights or permissions that an application requires to run.

Filter > New Administrative Rights Required Application Compatibility Filter

[Details](#) [Related Items](#)

Details

Name New Administrative Rights Required Application Compatibility Filter

Description This filter tests whether Windows has detected that this executable requires administrative rights

Settings

Perform execution level test: Require Administrator

Perform installer detection test:

- Generic Installer is set
- Specific Installer is not set
- Specific Non Installer is not set

Results should be Included

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#)

Examples

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Type** column enter application compatibility.

Filters

[Add Filter](#)

1 to 5 of 5

NAME	DESCRIPTION	TYPE	MACOS	WINDOWS
Filter	Filter	appid	Any	Any
Administrative Rights Required Application Compatibility Filter	This filter tests whether Windows has detected that this executable requires administrative rights	Application Compatibility File Filter	Not Supported	Supported
Generic Installer Detection Filter	This filter indicates that Windows has detected that an executable is an Application Setup	Application Compatibility File Filter	Not Supported	Supported
Highest Available Application Compatibility Filter	This filter tests whether Windows has detected that this executable required highest available rights	Application Compatibility File Filter	Not Supported	Supported
Specific Installer Detection Filter	This filter indicates that Windows has detected that an executable is an Application Setup	Application Compatibility File Filter	Not Supported	Supported
Specific Non Installer Detection Filter	This filter indicates that an executable has been flagged as not being an Application Setup	Application Compatibility File Filter	Not Supported	Supported

3. Select a filter to view its details and/or create a copy to customize the filter.

Filter > Administrative Rights Required Application Compatibility Filter

i This item is read-only.

[Details](#) [Related Items](#)

Details

Name Administrative Rights Required Application Compatibility Filter

Description This filter tests whether Windows has detected that this executable requires administrative rights

Settings

Perform execution level test: Require Administrator

Perform installer detection test:

- Generic Installer is set
- Specific Installer is not set
- Specific Non Installer is not set

Results should be Included

[Back](#) [Edit](#) [Create a Copy](#)

4. Click **Edit**.
5. Set the needed parameters.

Filter > New Administrative Rights Required Application Compatibility Filter

Details Related Items

Details

Name New Administrative Rights Required Application Compatibility Filter

Description This filter tests whether Windows has detected that this executable requires administrative rights

Settings

Perform execution level test: Require Administrator

Perform installer detection test:

<input checked="" type="checkbox"/> Generic Installer	is	set	▼
<input checked="" type="checkbox"/> Specific Installer	is	not set	▼
<input type="checkbox"/> Specific Non Installer	is	not set	▼

Results should be: Included ▼

Back Edit Create a Copy Delete

6. Click **Save**.

Filter > New Administrative Rights Required Application Compatibility Filter

Details Related Items

Details

Name New Administrative Rights Required Application Compatibility Filter

Description This filter tests whether Windows has detected that this executable requires administrative rights

Settings

Perform execution level test: Require Administrator ▼

Perform installer detection test:

<input checked="" type="checkbox"/> Generic Installer	is	set	▼
<input checked="" type="checkbox"/> Specific Installer	is	not set	▼
<input type="checkbox"/> Specific Non Installer	is	not set	▼

Results should be: Included ▼

Save Cancel

Application Manifest Filter (*Manifest Filter*)

Applications that declare specific rights required via a manifest, such as applications that need administrative privileges.

Filter > new Copy of Manifest Present Filter

Details Related Items

Details

Name new Copy of Manifest Present Filter

Description This filter tests whether an executable has a security manifest

Settings

Presence Only perform presence check

Execution Level Require Administrator

Back Edit Create a Copy Delete

Examples

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Type** column enter application manifest.

Filters

Add Filter

1 to 4 of 4

NAME ^	DESCRIPTION	TYPE	MACOS	WINDOWS
Filter	Filter	manifest filter	Any	Any
Manifest Present Filter	This filter tests whether an executable has a security manifest	Manifest Filter	Not Supported	Supported
new Copy of Manifest Present Filter	This filter tests whether an executable has a security manifest	Manifest Filter	Not Supported	Supported
Require Administrator Rights Manifest Filter	This filter tests whether an executable is marked as requiring Administrative rights	Manifest Filter	Not Supported	Supported
Require Highest Available Rights Manifest Filter	This filter tests whether an executable is marked as requiring highest available rights	Manifest Filter	Not Supported	Supported

3. Select a filter to view its details and/or create a copy to customize the filter.

Filter > Manifest Present Filter

This item is read-only.

Details Related Items

Details

Name Manifest Present Filter

Description This filter tests whether an executable has a security manifest

Settings

Presence Only perform presence check

Execution Level Require Administrator

Back Edit Create a Copy

4. Click **Edit**.

5. Set the needed parameters.

Filter > New Copy of Manifest Present Filter

Details Related Items

Details

Name New Copy of Manifest Present Filter

Description This filter tests whether an executable has a security manifest

Settings

Presence Only perform presence check

Execution Level Highest Available

Save Cancel

6. Click **Save**.

Filter > New Copy of Manifest Present Filter

Details Related Items

Details

Name * New Copy of Manifest Present Filter

Description * This filter tests whether an executable has a security manifest

Settings

Presence Only perform presence check

Execution Level * Highest Available

Save Cancel

File Collection Security Catalog Filter

This is a special collection of files to whitelist or blacklist. This filter type is similar to other Inventory Filters, particularly our Security Catalog Filter. *No out-of-box filters exist in Privilege Manager for this type.*

You can use these filters to target executables found in security catalogs. The built-in filter targets the Signed Security Catalog (`Windows\System32\catroot`) and is typically used to automatically whitelist applications from Microsoft.

New Filter

Filter Details

Platform

Filter Type

Name

Description

File collection

Catalog signing certificate [Select resource...](#)

Timestamp server

Parameters

- File collection, this is the specific catalog you want to use.
- Catalog signing certificate, select the specific certificate from a list.
- Timestamp server, specifies a particular version to be used.

File Existence Filter

This type of filter identifies whether a file exists. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform * Windows

Filter Type * File Existence Filter

Name * New File Existence Filter

Description

File Path

This filter is available for both Windows and macOS systems.

Parameters

- Path, this must be an exact file path. Windows Environment Variables are supported though, %ProgramFiles% for example.

File Owner Filter

This filter identifies files based on ownership.

Filter > new Copy of Manifest Present Filter

Details Related Items

Details

Name new Copy of Manifest Present Filter

Description This filter tests whether an executable has a security manifest

Settings

Presence Only perform presence check

Execution Level Require Administrator

Back Edit Create a Copy Delete

This filter is available for both Windows and macOS systems.

Examples

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Type** column enter File owner.

Filters

Add Filter

1 to 3 of 3

NAME ^	DESCRIPTION	TYPE	MACOS	WINDOWS
Filter	Filter	file owner	Any	Any
System (Wheel) File Owner	Files that are owned by the Wheel group	File Owner Unix	Supported	Not Supported
System File Owner Filter	Filter used to detect files owned by the System account	File Owner	Not Supported	Supported
Trusted Installer File Owner Filter	Filter used to detect files owned by the Trusted File Owner account	File Owner	Not Supported	Supported

3. Select a filter to view its details and/or create a copy to customize the filter.

Filter > System File Owner Filter

This item is read-only.

Details Related Items

Details

Name System File Owner Filter

Description Filter used to detect files owned by the System account

Settings

Include only files with the owner set to any of the following accounts

Built-in Accounts

Well-known Accounts • NT Authority System Account

Domain User Groups

Back Edit Create a Copy

4. Click **Edit**.
5. Set the needed parameters.

Filter > New System File Owner Filter

Details Related Items

Details

Name * New System File Owner Filter

Description Filter used to detect files owned by the System account

Settings

Include only files with the owner set to any of the following accounts

Built-in Accounts + Add None Selected

Well-known Accounts + Add • NT Authority System Account

Domain User Groups + Add None Selected

Save Cancel

6. Click **Save**.

Filter > New System File Owner Filter

Details Related Items

Details

Name * New System File Owner Filter

Description Filter used to detect files owned by the System account

Settings

Include only files with the owner set to any of the following accounts

Built-in Accounts - Add • Server Operators

Type the name of a built-in account...

Well-known Accounts + Add • NT Authority System Account

Domain User Groups + Add None Selected

Save Cancel

File Specification Filter

This filter identifies files based on their file path, or location on a computer.

Filter > New File Specification Filter

Details Related Items Change History

Details

Name New File Specification Filter

Description

Platform Windows

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters

Exclude any filters

Back
Edit
Create a Copy
Delete
View as XML
Export

This filter is available for both Windows and macOS systems. Use this filter for macOS endpoints only to target known scripts or command-line tools; otherwise use the [Default File Specification \(macOS\)](#) filter.

Example

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Type** column enter file specification filter.

NAME ^	DESCRIPTION	TYPE	MACOS	WINDOWS
file	Filter	file specification	Any	Any
Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS.	File Specification Filter	Supported	Not Supported
Default File Specification (All executable types)	Specifies all executable file types in Windows and Program files	File Specification Filter	Not Supported	Supported
Default File Specification (MacOS)	The default filter for discovering executable files on MacOS.	File Specification Filter	Supported	Not Supported
Default File Specification (Windows)	This specifies executables in Windows and Program files	File Specification Filter	Not Supported	Supported
Doc Test File Specification Filter		File Specification Filter	Supported	Not Supported

3. Select a filter to view its details and/or create a copy to customize the filter.

Details Related Items Change History

Details

Name Default File Specification (Windows)
Description This specifies executables in Windows and Program files

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

- Common Executable Folders

Include only filters

- Program File Executables

Exclude any filters

- Temporary Files • Documents and Settings

Back Edit **Create a Copy** View as XML Export

4. Click **Edit**.

5. Set the needed parameters.

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters **+ Add** • Common Executable Folders

Include only filters **+ Add** • Program File Executables

Exclude any filters **+ Add** • Temporary Files • Documents and Settings

6. Click **Save**.

File Type Filter

This filter identifies files based on what type of file it is. *No out-of-box filters exist in Privilege Manager for this type.*

Filter > New File Type Filter

[Details](#) [Related Items](#) [Change History](#)

Details

Name	New File Type Filter
Description	
Platform	Windows

Settings

File Extensions

MIME Types

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [Export](#)

Parameters

- File Extensions
- MIME Types

Internet Zone Filter

This filter identifies what internet zone a computer is connected to on your network, such as Trusted Sites and Local Intranet. *No out-of-box filters exist in Privilege Manager for this type.*

Filter > Test Internet Zone Filter

Details Related Items Change History

Details

Name	Test Internet Zone Filter
Description	
Platform	Windows

Settings

Existence of any zone information

Standard zone:

Custom zone ID:

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [View as XML](#) [Export](#)

Parameters

- Existence of any zone information
- Standard zone:
 - Local Intranet
 - Trusted Sites
 - Internet
 - Restricted Sites
- Custom Zone IDs

Security Catalog Filter

This is a special collection of files to whitelist or blacklist. For example, the Microsoft Security Catalog is often whitelisted as a trusted catalog.

Filter > Test Security Catalog Filter

[Details](#) [Related Items](#) [Change History](#)

Details

Name	Test Security Catalog Filter
Description	Testing the security catalog filter
Platform	Windows

Settings

Digital Certificates

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [Export](#)

Parameters

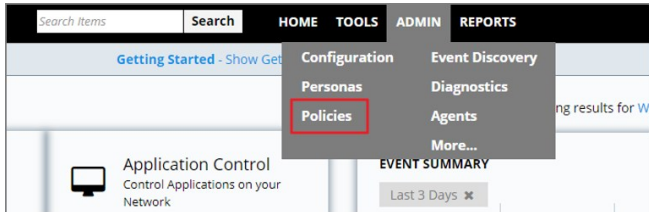
- Digital Certificates

Unable to Access Cortana and Search for Windows 10

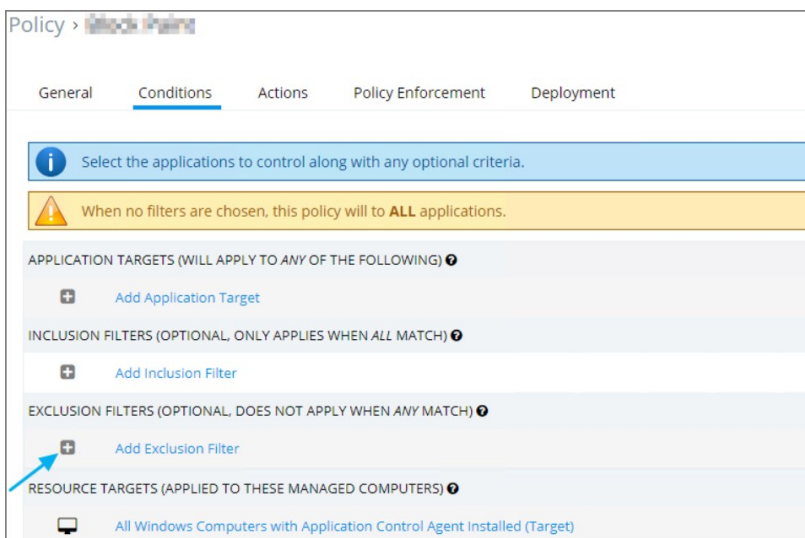
This issue might be due to the **Present In Signed Security Catalog** not being added to the **Exclusion Filters** section in a policy.

How to Resolve

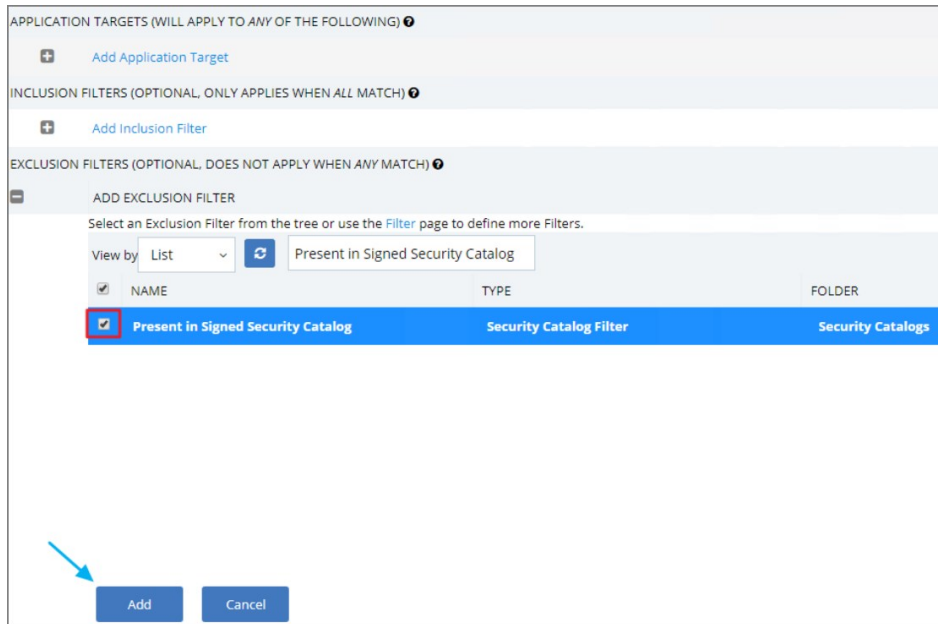
1. Launch **Privilege Manager**
2. Click **ADMIN | Policies**



3. Click on a previously created policy.
4. Click **Edit**.
5. Click on the **Conditions** tab | **Add Exclusion Filter**.

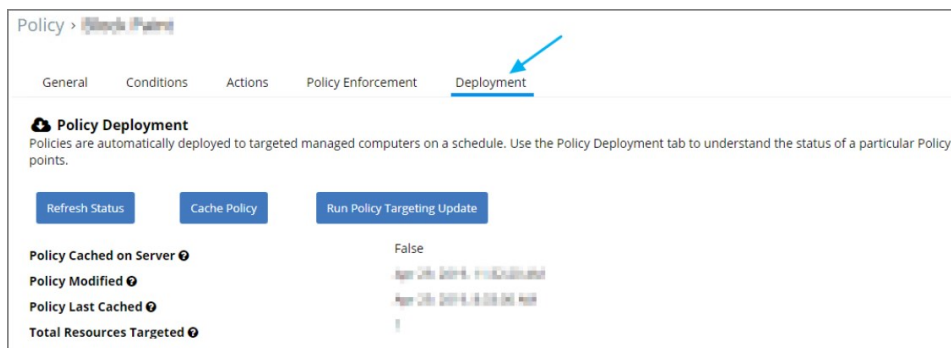


6. Search for **Present In Signed Security Catalog**.
7. Select the check box for **Present In Signed Security** filter | click **Add**.



8. Click **Save**.

9. Click on the **Deployment** tab.



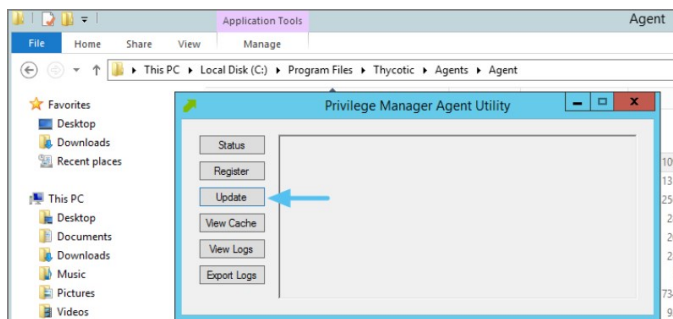
10. Click **Cache Policy** / **Run Policy Targeting Update**.

Note: Once the agents check back into the web console which by default occurs every 30 minutes, the machines will get the new policy changes. However if you would like to test the policy update on a specific machine, please continue to step 11.

11. Go to the Machine(s) where you want to update the policy and open the Agent Utility.

e.g., C:\Program Files\Thycotic\Agents\Agent

12. Click **Update**.



Inventory Filters

These depend on file inventory data, meaning they generally apply to already discovered applications or files pulled in by Privilege Manager tasks. For example, after running an inventory task on a specific computer or group of computers, Privilege Manager can glean through the list of file inventory that is reported and target those files.

Note: No out-of-box filters exist in Privilege Manager for this type of filter category

The following Inventory Filter type filter topics are available:

- [File Collection from List of Sha1 Hashes Filter](#)
- [File Scan Results Filter - Computer](#)
- [File Scan Results Filter - Policy](#)
- [MSI File Contents Filter](#)
- [MSI Package Contents Filter](#)
- [Package Contents Filter](#)
- [Security Catalog Contents Filter](#)
- [Virtual Disk File Contents Filter](#)
- [Virtual Disk Package Contents Filter](#)

File Collection from List of Sha1 Hashes Filter

This type of filter identifies file inventory based on Secure Hash Algorithms. *No out-of-box filters exist in Privilege Manager for this type.*

When creating this filter the target hashes need to be entered as a comma-separated list:

New Filter

Filter Details

Platform * Windows

Filter Type * File Collection from List of SHA1 Hashes Filter

Name * Test File Collection of Hashes Filter

Description Test filter for collection from list of SHA1 hashes

Comma-separated SHA1 Hashes * 520C662A9ECD030AC20028629056EF770D4D2BA4.91D9980C81139290AC289A43FA91509A183D91B1.0032A3D8878ADD5CB2AB3A809A1F59018096E5AF

This filter is available for both Windows and macOS systems.

Parameters

Once the filter is created, the following settings can be edited:

- Data Source:
 - Hash Based Query (do not change the data source)
- Results will be:
 - Included (default)
 - Excluded

File Parameter Collection Filter > New File Collection of Hashes Filter

Details Membership Related Items Change History

Details

Name New File Collection of Hashes Filter

Description

Platform Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source Hash Based Query

Results Will Be Included

Under the Membership tab various reports can be viewed:

- All Files Picker Report
- Win32 File Picker Report
- Default Resource Picker Report

Details **Membership** Related Items Change History

i This collection was last updated on Oct 29, 2019, 3:11:34 PM. To force an immediate update, click Update Membership

View All Files Picker Report

File Name	Product Name	Version	Header Type
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

No records available.

◀ ◻ 10 items per page 0 - 0 of 0 items

Total: 0 items

Example showing the Default Resource Picker Report view:

Details **Membership** Related Items Change History

i This collection was last updated at Oct 29, 2019, 3:26:14 PM. To force an immediate update, click Update

Update Membership

View Default Resource Picker Report

Name	Resource Type
Default Resource Picker Report	
New Loaded Resource - kDKj2leK3VyyzqAmh9ZAYCW5a8= - Created via Sha1 Filter	File
New Loaded Resource - kdmYDIETkpCskJpD+pQmHg9kbE= - Created via Sha1 Filter	File
New Loaded Resource - UgxmKp7NAwrCACChkFbvdw1NK6Q= - Created via Sha1 Filter	File

10 items per page

File Scan Results Filter (Computer)

This type of filter identifies file inventory based on another computer's file scan results. This allows for one computer that has been setup properly to be used as a source for this filter. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform * Windows

Filter Type * File Scan Results Filter (Computer)

Name * TestFile Scan Results (Computer) File Filter

Description Specifies files reported by the specified file scan reporting filters by the specified computers

[Back](#) [Create](#)

This filter is available for both Windows and macOS systems.

Parameters

Once the filter is created the following settings can be edited:

- Data Source, this should not be edited. The information here is specific to the task of the File Scan Results Filter for computers.
- Computer, this is the actual computer resource that has to be selected for the scan.
- Reporting Filter
- Results will be either excluded (default) or included.

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source * File Scan Results Query - Computer

Computer

View Parameters

*Select resource...

Select	Name	Resource T...	SystemType	Domain	Manufacturer	Model	IpAddress	CreatedDate
<input type="checkbox"/>	ResourceCom...	Computer	x64-based PC	WORKGROUP	Microsoft Corporation	Virtual Machine	::1	5/31/19, 12:24 PM

10 items per page 1 - 1 of 1 items

[Close](#) [Clear](#)

Reporting Filter * Type the name of a item...

Results Will Be

Included

Excluded

File Scan Results Filter (Policy)

This type of filter identifies file inventory based on Privilege Manager Policies. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform	Windows
Filter Type	File Scan Results Filter (Policy)
Name	Test File Scan Results File Filter - Policy
Description	Specifies files reported by the specified file scan reporting filters by the specified policy

[Back](#) [Create](#)

Parameters

Once the filter is created the following settings can be edited:

- Data Source, this should not be edited, it is the File Scan Policy Results Query.
- Specifies the File Scan Policy, this is the actual Policy resource that has to be selected for the scan.
- Reporting Filter
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test File Scan Results File Filter - Policy

Details Membership Related Items Change History

Details

Name	Test File Scan Results File Filter - Policy
Description	Specifies files reported by the specified file scan reporting filters by the specified policy
Platform	Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	File Scan Policy Results Query
Specifies the File Scan policy	Type the name of a item...
Reporting Filter	Type the name of a item...
Results Will Be	<input type="radio"/> Included <input checked="" type="radio"/> Excluded

MSI File Contents Filter

This type of filter identifies file inventory based on .MSI file contents, i.e. specific Windows package installers. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform

Filter Type

Name

Description

Parameters

Once the filter is created the following settings can be edited:

- Data Source, (do not edit) this is the MSI File Contents Query.
- File:
 - Parameters (these are required)
 - Win32 Executable
 - Product Name
 - Select Resource, this is the actual MSI file resource that has to be selected for the scan.
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test MSI File Contents Filter

Details Membership Related Items Change History

Details

Name

Description

Platform

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source

File [View Parameters](#)
[Select resource...](#)

Results Will Be Included Excluded

Viewing and Editing the Parameters

File Parameters [Hide](#)

Win32 Executable

Product Name

Viewing and Adding the Resource(s)

File

View Parameters

Select resource...

Select	File Name	Product Name	Version	Header Type
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Agent Utility.exe	Privilege Manager Agent Utility	10.6.1080.0	Coff
<input type="checkbox"/>	AgentService.exe	Microsoft® Windows® Operating System	10.0.14393.1737	Coff
<input type="checkbox"/>	AJRouter.dll	Microsoft® Windows® Operating System	10.0.14393.0	Coff
<input type="checkbox"/>	alg.exe	Microsoft® Windows® Operating System	10.0.14393.0	Coff
<input type="checkbox"/>	AppHostRegistrationVerfier....	Microsoft® Windows® Operating System	10.0.14393.0	Coff
<input type="checkbox"/>	apphostsvc.dll	Internet Information Services	10.0.14393.0	Coff
<input type="checkbox"/>	appidsvc.dll	Microsoft® Windows® Operating System	10.0.14393.2214	Coff
<input type="checkbox"/>	ApplicationFrameHost.exe	Microsoft® Windows® Operating System	10.0.14393.0	Coff

MSI Package Contents Filter

This type of filter identifies file inventory based on MSI package contents. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform * Windows

Filter Type * MSI Package Contents Filter

Name * Test MSI Package Contents Filter

Description Filters executable files contained in the specified MSI package

[Back](#) [Create](#)

Parameters

Once the filter is created the following settings can be edited:

- Data Source, (do not edit) this is the MSI Package Contents Query.
- Package:
 - Parameters:
 - Scope by Organizational Group
 - Search text
 - Maximum rows returned, this is a required parameter and the default is 10000.
 - Select Resource, this is the actual MSI package resource that has to be selected for the query.
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test MSI Package Contents Filter

Details Membership Related Items Change History

Details

Name * Test MSI Package Contents Filter

Description Filters executable files contained in the specified MSI package

Platform Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source * MSI Package Contents Query

[View Parameters](#)

Package * Select resource...

Results Will Be Included Excluded

Viewing and Editing the Parameters

Package

Parameters [Hide](#)

Scope by Organizational Group All Resources

Search text

Maximum rows returned * 10000

[Search](#)

Viewing and Adding the Resource(s)

Package

[View Parameters](#)

◆ Select resource...

Select	Name	Resource Type	Description	CreateDate
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	month/day/ye... <input type="text"/>
<input checked="" type="checkbox"/>	UNC File Inventory Package for \\filesahre1\TP\	Package		8/7/19, 3:39 PM
<input checked="" type="checkbox"/>	UNC File Inventory Package for \\path-to\share\	Package		8/8/19, 9:47 AM

◀ 1 ▶ 10 items per page 1 - 2 of 2 Items

Package Contents Filter

This type of filter identifies file inventory based on package contents. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform * Windows

Filter Type * Package Contents Filter

Name * Test Package Contents Filter

Description Filters files contained in the specified package

[Back](#) [Create](#)

Parameters

Once the filter is created the following settings can be edited:

- Data Source, (do not edit) this is the Package Contents Query.
- Package:
 - Parameters:
 - Scope by Organizational Group
 - Search text
 - Maximum rows returned, this is a required parameter and the default is 10000.
 - Select Resource, this is the actual package resource that has to be selected for the query.
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test Package Contents Filter

Details Membership Related Items Change History

Details

Name * Test Package Contents Filter

Description Filters files contained in the specified package

Platform Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source * Package Contents Query

Package [View Parameters](#)
* [Select resource...](#)

Results Will Be Included Excluded

Viewing and Editing the Parameters

Package **Parameters** [Hide](#)

Scope by Organizational Group All Resources

Search text

Maximum rows returned * 10000

[Search](#)

Viewing and Adding the Resource(s)

Package

[View Parameters](#)

◆ Select resource...

Select	Name	Resource Type	Description	CreateDate
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	month/day/ye... <input type="text"/>
<input checked="" type="checkbox"/>	UNC File Inventory Package for \\filesahre1\TP\	Package		8/7/19, 3:39 PM
<input checked="" type="checkbox"/>	UNC File Inventory Package for \\path-to\share\	Package		8/8/19, 9:47 AM

◀ 1 ▶ 10 items per page 1 - 2 of 2 Items

Security Catalog Contents Filter

This is a special collection of files to whitelist or blacklist. This filter type is similar to other Inventory Filters, particularly our Security Catalog Filter. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform	* Windows
Filter Type	* Security Catalog Contents Filter
Name	* Test Security Catalog File Filter
Description	Filters a list of files contained in Security Catalogs that were inventoried by the specified file scan reporting filters by the specified computers.

[Back](#) [Create](#)

Parameters

Once the filter is created the following settings can be edited:

- Data Source
- Computer Filter
- Computers
- Reporting Filter
- Resource Targets
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test Security Catalog File Filter

Details Membership Related Items Change History

Details

Name	* Test Security Catalog File Filter
Description	Filters a list of files contained in Security Catalogs that were inventoried by the specified file scan reporting filters by the specified computers.
Platform	Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source	* <input type="text" value="Type the name of a data source..."/>
Computer Filter	* 00000000-0000-0000-0000-000000000000
Computers	* 00000000-0000-0000-0000-000000000000
Reporting Filter	* 00000000-0000-0000-0000-000000000000
Resource Targets	* 00000000-0000-0000-0000-000000000000
Results Will Be	<input type="radio"/> Included <input checked="" type="radio"/> Excluded

Virtual Disk File Contents Filter

The Virtual Disk File Contents Filter filters files contained in the specified virtual disk file. *No out-of-box filters exist in Privilege Manager for this type.*

New Filter

Filter Details

Platform * Windows

Filter Type * Virtual Disk File Contents Filter

Name * Test Virtual Disk File Contents Filter

Description Filters files contained in the specified virtual disk file

[Back](#) [Create](#)

Parameters

Once the filter is created the following settings can be edited:

- Data Source, (do not edit) this is the MSI File Contents Query.
- File:
 - Parameters (these are required)
 - Win32 Executable
 - Product Name
 - Select Resource, this is the actual MSI file resource that has to be selected for the scan.
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test Virtual Disk File Contents Filter

[Details](#) [Membership](#) [Related Items](#) [Change History](#)

Details

Name * Test Virtual Disk File Contents Filter

Description Filters files contained in the specified virtual disk file

Platform Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source * Virtual Disk File Contents Query

File [View Parameters](#)
* Select resource...

Results Will Be Included Excluded

Viewing and Editing the Parameters

Data Source * Virtual Disk File Contents Query

File [Parameters](#) [Hide](#)

Win32 Executable * %

Product Name * %

[Search](#)

Viewing and Adding the Resource(s)

Data Source * Virtual Disk File Contents Query

File [View Parameters](#)
[Select resource...](#)

Select	File Name	Product Name	Version	Header Type
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Agent Utility.exe	Privilege Manager Agent Utility	10.6.1080.0	Coff
<input type="checkbox"/>	AgentService.exe	Microsoft® Windows® Operating System	10.0.14393.1737	Coff
<input type="checkbox"/>	AJRouter.dll	Microsoft® Windows® Operating System	10.0.14393.0	Coff
<input type="checkbox"/>	alg.exe	Microsoft® Windows® Operating System	10.0.14393.0	Coff
<input type="checkbox"/>	AppHostRegistrationVerifier.exe	Microsoft® Windows® Operating System	10.0.14393.0	Coff
<input type="checkbox"/>	apphostsvc.dll	Internet Information Services	10.0.14393.0	Coff
<input type="checkbox"/>	appidsvc.dll	Microsoft® Windows® Operating System	10.0.14393.2214	Coff

Virtual Disk Package Contents Filter

Filters files contained in the specified virtual disk package. *No out-of-box filters exist in Privilege Manager for this type.*

Parameters

Once the filter is created the following settings can be edited:

- Data Source, (do not edit) this is the Virtual Disk Package Contents Query.
- Package:
 - Parameters:
 - Scope by Organizational Group
 - Search text
 - Maximum rows returned, this is a required parameter and the default is 10000.
 - Select Resource, this is the actual package resource that has to be selected for the query.
- Results will be either excluded (default) or included.

File Parameter Collection Filter > Test Virtual Disk Package Contents Filter

[Details](#) | [Membership](#) | [Related Items](#) | [Change History](#)

Details

Name * Test Virtual Disk Package Contents Filter

Description Filters files contained in the specified virtual disk package

Platform Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source * Virtual Disk Package Contents Query

Package [View Parameters](#)
* [Select resource...](#)

Results Will Be Included Excluded

Viewing and Editing the Parameters

Data Source * Virtual Disk Package Contents Query

Package [View Parameters](#)

Parameters [Hide](#)

Scope by Organizational Group All Resources

Search text

Maximum rows returned * 10000

Viewing and Adding the Resource(s)

Package [View Parameters](#)
* [Select resource...](#)

Select	Name	Resource Type	Description	CreatedDate
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	month/day/year ... <input type="text"/>
<input checked="" type="checkbox"/>	UNC File Inventory Package for \\fileshare\TTP\	Package		8/7/19, 3:39 PM
<input checked="" type="checkbox"/>	UNC File Inventory Package for \\path-to\share\	Package		8/8/19, 9:47 AM

◀ 1 ▶ 10 items per page 1 - 2 of 2 items

MacOS Specific Filters

Most of the Application and File type filters apply to Windows as much as macOS platforms. There are some macOS specific filters that are covered in this section.

This is the default drop-down list when adding a new filter for macOS:

The screenshot shows a 'New Filter' dialog box with a 'Filter Details' section. The 'Platform' dropdown is set to 'Mac OS'. The 'Filter Type' dropdown is open, showing a list of filter types. The list is divided into two sections: 'Application Filters (MacOS)' and 'File Filters (MacOS)'. The 'Application Filters (MacOS)' section includes: Commandline Filter, Download Source Filter, Parent Process Filter, Secondary File Filter, Security Rating Filter, Signed File Filter, Time Of Day Filter, and User Context Filter. The 'File Filters (MacOS)' section includes: Application Bundle Filter, File Collection from List of SHA1 Hashes Filter, File Existence Filter, File Owner Filter, File Scan Results Filter (Computer), and File Specification Filter.

List of MacOS Filters

The following filters are available based on type from a quick select drop-down menu, after choosing macOS as the platform.

Application Filter Types

- [Commandline Filter](#)
- [Download Source Filter](#)
- [Parent Process Filter](#)
- [Secondary File Filter](#)
- [Security Rating Filter](#)
- [Signed File Filter](#)
- [Time Of Day Filter](#)
- [User Context Filter](#)

File Filter Types

- [Application Bundle Filter](#)
- [File Collection from List of SHA1 Hashes Filter](#)
- [File Existence Filter](#)
- [File Owner Filter](#)
- [File Scan Results Filter \(Computer\)](#)
- [File Specification Filter](#)

List of Default Filters for Event Discovery

The following filters are the default filters used during inventory event discovery on macOS endpoints:

- [Default File Specification \(MacOS\)](#)
 - [Default Applications Folder \(MacOS\)](#)
 - [System Applications Folder \(MacOS\)](#)
- [Default App Bundles File Specification Filter](#)
 - [Default Application Bundles Filter \(MacOS\)](#)
 - [System Application Bundles Filter \(MacOS\)](#)

Available Preference Pane Filters

- [Date and Time Preference Pane filter](#)
- [Energy Saver Preference Pane filter](#)
- [Network Preference Pane filter](#)

App Bundle Filter

This type of filter identifies app bundles for macOS systems.

Filter > Test Application Bundle Filter (MacOS)

Details Related Items Change History

Details

Name	Test Application Bundle Filter (MacOS)
Description	
Platform	Mac OS

Settings

Bundle Name

Bundle Path Include subdirectories

Match the following property list values:

- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File
- Info String
- Min System Version

Prior to Privilege Manager 10.7.1, the value of the Bundle Name field requires the inclusion of the .app extension (e.g. Console.app). The Bundle Name field should have an entry like **console.app** or **photos.app** to correctly apply the filter. If it is not present, the filter will fail to properly match. With Privilege Manager 10.7.1, the presence of the .app extension is properly calculated during policy processing.

Pre-10.7.1 Example

The bundle name should appear when creating the filter.

Settings

Bundle Name

Bundle Path

Include subdirectories

Parameters

- Bundle Name
- Bundle Path
 - Include subdirectories

The following bundle properties can be used to identify an application bundle in an Application Bundle filter. These properties are found in the info.plist for the application on macOS systems.

- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File
- Info String
- Min System Version

Note: The **Bundle Name** field is separate from the Bundle Name in the property list. If you have the Bundle Name field populated and it doesn't match the binary being executed, the filter will fail to match and not process the property list values in the Info.plist file. If an app is discovered as a new loaded resource and assigned to a policy, a filter is created and pre-populated based on the information pulled from the info.plist file.

Filter > Wizard Generated App Bundle Filter for 'Photos'

Details Related Items Change History

Details

Name * Wizard Generated App Bundle Filter for 'Photos'

Description

Platform Mac OS

Settings

Bundle Name

Bundle Path

Include subdirectories

Match the following property list values:

App Category is equal to public.app-category.photography

Bundle Identifier is equal to com.apple.Photos

Bundle Name is equal to Photos

Bundle Version

Bundle Version (short)

Executable File is equal to Photos

Info String

Min System Version

Save Cancel Export

Info.plist Example for Photos

```

<key>CFBundleExecutable</key>
<string>Photos</string>
<key>CFBundleHelpBookFolder</key>
<string>Photos.help</string>
<key>CFBundleHelpBookName</key>
<string>com.apple.Photos.help</string>
<key>CFBundleIconFile</key>
<string>AppIcon</string>
<key>CFBundleIconName</key>
<key>CFBundleIdentifier</key>
<string>com.apple.Photos</string>
<key>CFBundleInfoDictionaryVersion</key>
<string>6.0</string>

```

Default App Bundles File Specification Filter

This type of filter identifies application bundles for macOS systems. With this application bundles filter in place, macOS application bundles are inventoried regardless of their installation path in either /Applications or /System/Applications) on all versions of macOS.

Details
Related Items
Change History

Details

Name Default App Bundles File Specification Filter

Description The default filter for discovering app bundles on MacOS.

Platform Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters • Default Application Bundles Filter (MacOS) • System Application Bundles Filter (MacOS)

Include only filters

Exclude any filters

Back
Edit
Create a Copy
View as XML
Export

By default this is a read-only filter which uses the following Additional Filters:

- File filters:
 - [Default Application Bundles Filter \(MacOS\)](#)
 - [System Application Bundles Filter \(MacOS\)](#)

The option to include subdirectories is enabled by default.

Example

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Name** column, search for default.

Filters

1 to 4 of 4

NAME ^	DESCRIPTION	TYPE	MACOS	WINDOWS
default	Filter	Filter	Supported	Any
Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS.	File Specification Filter	Supported	Not Supported
Default Application Bundles Filter (MacOS)	Default Application Bundles Filter (MacOS)	App Bundle Filter	Supported	Not Supported
Default Applications Folder (MacOS)	The default filter for discovering executable files in /Applications on MacOS.	File Specification Filter	Supported	Not Supported
Default File Specification (MacOS)	The default filter for discovering executable files on MacOS.	File Specification Filter	Supported	Not Supported

3. Select the **Default App Bundles File Specification Filter** filter to view its details and/or create a copy to customize the filter.
4. Click **Edit**
5. Set the needed parameters.

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters • Default Application Bundles Filter (MacOS) • System Application Bundles Filter (MacOS)

Include only filters None Selected

Exclude any filters None Selected

6. Click **Save**.

Default File Specification (MacOS)

This filter identifies files based on their file path or location on a computer.

Details
Related Items
Change History

Details

Name Default File Specification (MacOS)

Description The default filter for discovering executable files on MacOS.

Platform Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters • System Applications Folder (MacOS) • Default Applications Folder (MacOS)

Include only filters • macOS Executables

Exclude any filters

Back
Edit
Create a Copy
View as XML
Export

This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:

- File filters:
 - [System Applications Folder \(MacOS\)](#)
 - [Default Applications Folder \(MacOS\)](#)
- Include only filters:
 - [macOS Executables](#)

The option to include subdirectories is enabled by default.

Example

1. Navigate to **Admin | More...** and select **Filters**.
2. In the search field for the **Name** column, search for default.

Filters

1 to 4 of 4

Add Filter

NAME ^	DESCRIPTION	TYPE	MACOS	WINDOWS
default	Filter	Filter	Supported	Any
Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS.	File Specification Filter	Supported	Not Supported
Default Application Bundles Filter (MacOS)	Default Application Bundles Filter (MacOS)	App Bundle Filter	Supported	Not Supported
Default Applications Folder (MacOS)	The default filter for discovering executable files in /Applications on MacOS.	File Specification Filter	Supported	Not Supported
Default File Specification (MacOS)	The default filter for discovering executable files on MacOS.	File Specification Filter	Supported	Not Supported

3. Select the **Default File Specification (MacOS)** filter to view its details and/or create a copy to customize the filter.

4. Click **Edit**.

5. Set the needed parameters.

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters • System Applications Folder (MacOS) • Default Applications Folder (MacOS)

Include only filters • macOS Executables

Exclude any filters None Selected

6. Click **Save**.

Preference Pane Filters

The following Preference Pane Filters are supported for targeting in run as root type policies triggering justification and approval type interactive user dialogs:

- [Date and Time Preference Pane filter](#)
- [Energy Saver Preference Pane filter](#)
- [Network Preference Pane filter](#)

For the following list of default preference pane filters, Thycotic recommends to only target the preference pane in basic deny access policies:

- App Store Preference Pane
- Parental Controls Preference Pane
- Printers and Scanners Preference Pane
- Security and Privacy Preference Pane
- Sharing Preference Pane
- Time Machine Preference Pane
- Users and Groups Preference Pane

Date and Time Preference Pane Filter

The Date and Time Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.

Filter > Test Date and Time Preference Pane (MacOS)

Details Related Items Change History

Details

Name Test Date and Time Preference Pane (MacOS)

Description Date and Time Preference Pane (MacOS)

Platform Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names com.apple.preference.datetime.remoteservice

Path /System/Library/PreferencePanes/DateAndTime.prefPane/Contents/XPCServices/com.apple.preference.datetime.remoteser

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters + Add None Selected

Include only filters + Add None Selected

Exclude any filters + Add None Selected

Save Cancel Export

As the screen captures show, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Thycotic does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

Energy Saver Preference Pane Filter

The Energy Saver Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.

Filter > Energy Saver Preference Pane (MacOS)

i This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Details

Name	Energy Saver Preference Pane (MacOS)
Description	Energy Saver Preference Pane (MacOS)
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names	com.apple.preference.energysaver.remoteservice
Path	/System/Library/PreferencePanes/EnergySaver.prefPane/Contents/XPCServices/com.apple.preference.energysaver.remoteservice.xpc/Contents/MacOS/
Drive Types	<input type="checkbox"/> Unknown Type <input type="checkbox"/> No Root Directory <input type="checkbox"/> Removable Drive (Floppy/USB) <input type="checkbox"/> Fixed Disk <input type="checkbox"/> Network Drive <input type="checkbox"/> Optical Disk (CD/DVD) <input type="checkbox"/> RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters

Exclude any filters

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

As the screen captures show, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Thycotic does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

Network Preference Pane Filter

The Network Preference Pane Filter is a read-only filter. If you need to customize the filter, create a copy and edit Settings and/or add Additional Filters.

Filter > Network Preference Pane (MacOS)

i This Item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Details

Name	Network Preference Pane (MacOS)
Description	Network Preference Pane (MacOS)
Platform	Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names	com.apple.preference.network.remoteservice
Path	/System/Library/PreferencePanes/Network.prefPane/Contents/XPCServices/com.apple.preference.network.remoteservice.xpc/Contents/MacOS/
Drive Types	<input type="checkbox"/> Unknown Type <input type="checkbox"/> No Root Directory <input type="checkbox"/> Removable Drive (Floppy/USB) <input type="checkbox"/> Fixed Disk <input type="checkbox"/> Network Drive <input type="checkbox"/> Optical Disk (CD/DVD) <input type="checkbox"/> RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters

Exclude any filters

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

As the screen captures show, you can edit the default file names and path details. You can further specify to limit the targeting to specific drive type only based on selection, by default Thycotic does not add any limitations here. Selecting Attributes allows to widen the default scope of the filter.

Default Applications Folder (MacOS)

The default filter for discovering executable files in /Applications on macOS.

Details Related Items Change History

Details

Name Default Applications Folder (MacOS)
Description The default filter for discovering executable files in /Applications on MacOS.
Platform Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path /Applications/

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters • macOS Executables

Exclude any filters

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:

- Include only filters:
 - [macOS Executables](#)

The option to include subdirectories is enabled by default.

System Applications Folder (MacOS)

The default filter for discovering executable files in /System/Applications on macOS endpoints.

Details Related Items Change History

Details

Name System Applications Folder (MacOS)

Description The default filter for discovering executable files in /System/Applications on MacOS.

Platform Mac OS

Settings

Select criterion for this filter. This filter can be based on file names, location and/or extensions and can apply additional file filters.

File Names

Path /System/Applications/

Drive Types

- Unknown Type
- No Root Directory
- Removable Drive (Floppy/USB)
- Fixed Disk
- Network Drive
- Optical Disk (CD/DVD)
- RAM Disk

Attributes

- Include subdirectories
- Include system files
- Include hidden files
- Include reparse points
- Include system reparse points

Additional Filters (optional)

File filters

Include only filters • macOS Executables

Exclude any filters

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

This filter is available for macOS systems.

By default this is a read-only filter which uses the following Additional Filters:


- Include only filters:
 - [macOS Executables](#)

The option to include subdirectories is enabled by default.

Default Applications Bundle Filter (MacOS)

The default filter for discovering application bundles in /Applications on macOS endpoints.

Filter > Default Application Bundles Filter (MacOS)

 This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Details

Name	Default Application Bundles Filter (MacOS)
Description	Default Application Bundles Filter (MacOS)
Platform	Mac OS

Settings

Bundle Name

Bundle Path /Applications/
 Include subdirectories

Match the following property list values:

- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File
- Info String
- Min System Version

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

This filter is available for macOS systems.

The option to include subdirectories is enabled by default.

macOS Executables

The default filter for executable Mach-O files. This filter is available for macOS systems.

Include only files with a Mach-O header marked with attributes set via the filter Settings:

Settings

Include only files with a Mach-O header marked with the following attributes.

Cpu Type	All Cpu Types		
File Type	Demand Paged Executable File		
Flags	<input type="checkbox"/> No Undefined References	is	not set ▾
	<input type="checkbox"/> Incremental Link Output	is	not set ▾
	<input type="checkbox"/> Dynamic Linker Input	is	not set ▾
	<input type="checkbox"/> Dynamic Linker Bound Undefined References	is	not set ▾
	<input type="checkbox"/> Prebound Dynamic Undefined References	is	not set ▾
	<input type="checkbox"/> Split RO And RW Segments	is	not set ▾
	<input type="checkbox"/> Run Lazy Init Routine	is	not set ▾
	<input type="checkbox"/> Two-Level Name Space Bindings	is	not set ▾
	<input type="checkbox"/> Force Flat Name Space Bindings	is	not set ▾
	<input type="checkbox"/> Guarantee No Multiple Defintions	is	not set ▾
	<input type="checkbox"/> No Dylid Notify	is	not set ▾
	<input type="checkbox"/> Prebinding Can Be Redone	is	not set ▾
	<input type="checkbox"/> Binds All Modules	is	not set ▾
	<input type="checkbox"/> Can Divide Sections	is	not set ▾
	<input type="checkbox"/> Canonicalized Binary	is	not set ▾
	<input type="checkbox"/> Contains External Weak Symbols	is	not set ▾
	<input type="checkbox"/> Uses Weak Symbols	is	not set ▾
	<input type="checkbox"/> Stacks Have Stack Execution Privilege	is	not set ▾
	<input type="checkbox"/> Safe For Root Use	is	not set ▾
	<input type="checkbox"/> Safe For issetguid() Processes	is	not set ▾
	<input type="checkbox"/> Do Not Need Examine Dependent Dyllibs	is	not set ▾
	<input type="checkbox"/> Load Random Address	is	not set ▾
	<input type="checkbox"/> Dead Strippable DYLIB	is	not set ▾
	<input type="checkbox"/> Has TLV Descriptors	is	not set ▾
	<input type="checkbox"/> No Heap Execution	is	not set ▾
	<input type="checkbox"/> App Extension Safe	is	not set ▾

Results should be ▾

System Applications Bundle Filter (MacOS)

The default filter for app bundles files in /System/Applications on macOS endpoints.

Filter > System Application Bundles Filter (MacOS)

i This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Details

Name	System Application Bundles Filter (MacOS)
Description	System Application Bundles Filter (MacOS)
Platform	Mac OS

Settings

Bundle Name

Bundle Path /System/Applications/
 Include subdirectories

Match the following property list values:

- App Category
- Bundle Identifier
- Bundle Name
- Bundle Version
- Bundle Version (short)
- Executable File
- Info String
- Min System Version

[Back](#) [Edit](#) [Create a Copy](#) [View as XML](#) [Export](#)

This filter is available for macOS systems.

The option to include subdirectories is enabled by default.

A Resource Target in Privilege Manager is a specified set of computers that meet certain criteria (e.g., type of operating system or location of the computers), meant to be used as targets for policies or scheduled tasks. To make a policy apply to a certain set of computers, you need a resource target comprising that set of computers and assign that resource target to the policy (or, to state it differently, assign the policy to the resource target).

There are several built-in resource targets (for example, "All 64-bit Windows Computers with Application Control Agent Installed") that can be used when defining policies so that users generally do not need to create custom resource targets. However, there are cases when the latter is needed and, toward that end, this article focuses on user defined resource targets.

The article also briefly touches upon collections, a concept related to resource targets.

Resource targets are not the only kind of targets that can be assigned to policies; one could also assign an application filter to a policy to make the policy apply to the application file included in the filter.

User Defined Resource Targets

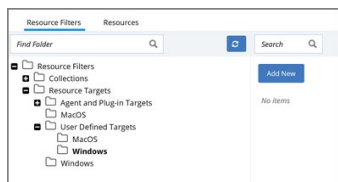
Targets are defined by starting with all known computers and then adding filters to narrow down the set (and after an initial narrowing down, if needed, expand it in some way).

You could create unique targets for all your policies, but if you want to create a target to be reused across multiple policies, it will be more practical to follow the steps in this article.

Interface to View or Create/Modify User Defined Targets

In the Privilege Manager console, navigate to **Admin | More...** and click **Resources**. On the Resources page select the Resource Filters tab, then in the tree go to **Resource Filters | Resource Targets | User Defined Targets**, and select either MacOS or Windows.

If you already created user defined targets, you see them listed here and can modify any of them by clicking the name and then editing the definition.



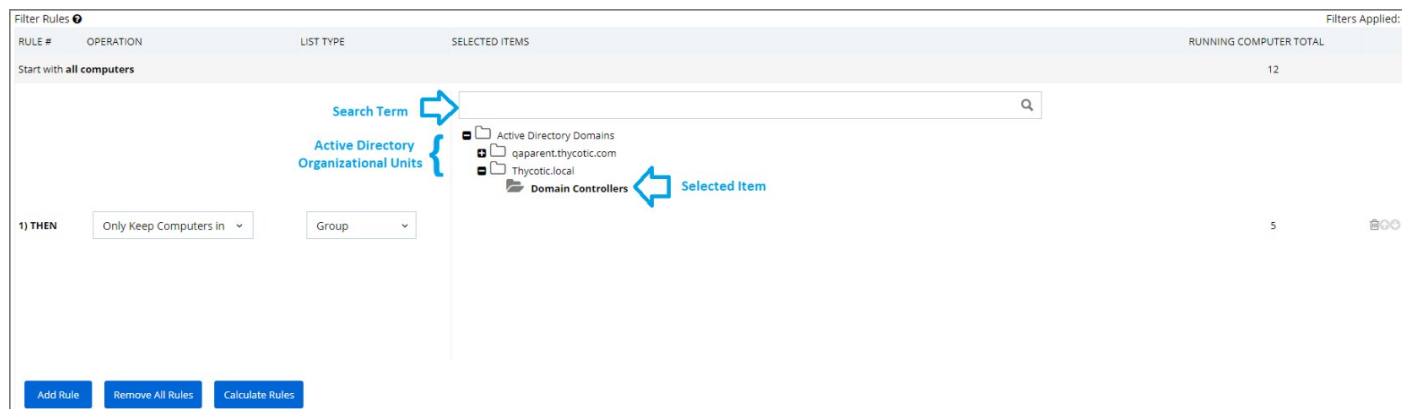
To create a new target, click the Add New button on the right, enter a name and description and then click the Create button.

Note: A Computer Group, like a Resource Target, is also a specified set of computers; you can think of it as another way to refer to Resource Targets. A computer group can be viewed, created, and modified from the Local Security home page. If you create a computer group in Local Security, you will see it listed in the User Defined Targets node of the Resource Filters tree.

Target Definition

After you have clicked the Create button, you will be on the target page (a page that provides an interface for defining the target). On the target page, click Edit and make sure you are on the Filter Rules tab.

Here you will be able to add rules to define the target, using the drop-down fields in the Operation and List Type columns.



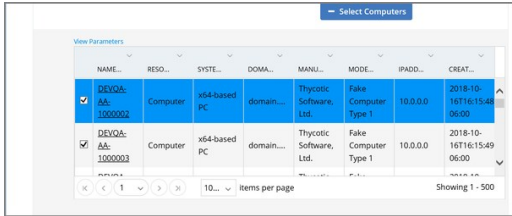
Operation

The idea here is that you are starting with all computers and applying filters to get the desired set. There are several operations that can be applied:

- **Only Keep Computers In:** This is an intersect operation. Only computers in both the current working set and the given list/collection will be kept.
- **Include Computers In:** This is an add operation. The computers in the given list/collection will be added to the current working set.
- **Exclude Computers In:** This is a subtract operation. Any computers in the excluded list/collection will be removed from the current working set.

List Type

- **Collection:** A collection (in the context being discussed here) is a predefined list of computers. (A collection is often meant to act as a filter and hence is also sometimes referred to as a filter.) See the Collections section for more information.
- **Computer List:** This is a fixed list specified for the target being defined. (See the screenshot at the end of this section.)
- **Group:** This is most often used to select a group of computers like an Active Directory Organizational Unit.



You can select "View Parameters" to enter search text to help find a computer.

Filter Rules	OPERATION	LIST TYPE	SELECTED ITEMS	RUNNING COMPUTER TOTAL
Start with	all computers			12
1) THEN	Only Keep Computers in	Group	OU=Domain Controllers,DC=thycotic,DC=local	5

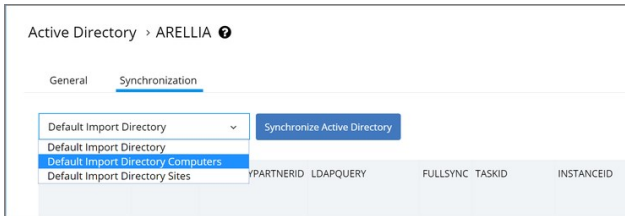
← Distinguished Name of the selected OU

Performance Considerations

Resource Targets are reevaluated when the scheduled task "Collection and Resource Targeting Update" runs. This operation is expensive for large numbers of computers. To keep performance high we suggest that you keep the overall number of targets to a minimum. Also note that targets with simpler definitions are generally less expensive.

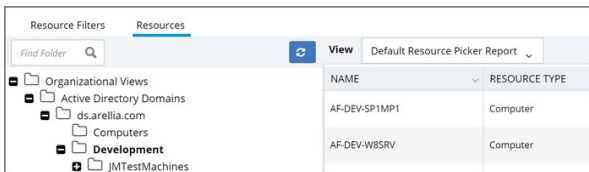
Active Directory as Related to Resource Targets

After you have created an Active Directory (AD) instance in Privilege Manager, you need to import computers (computer records, to be more precise). Go to your Active Directory Instance (by using Admin | Configuration | Foreign Systems, selecting your domain, then clicking your AD name) and select the Synchronization tab. Run the task "Default Import Directory Computers":



Note: Default Import Directory Computers will import computers and also import the Organizational Units (OU) to which they belong. Default Import Directory will import only organization structure and security-related information like users.

After the task completes, go to Admin | More, then select Resources, then Resource tab, then in the tree Organizational Views | Active Directory Domains | (your AD name). You should be able to see your OUs and computers.

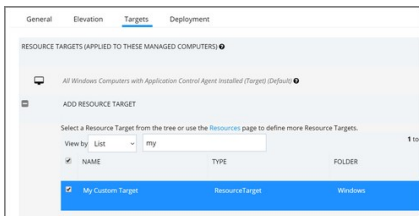


These OUs are what you can select using the "Group" option, for "List Type", when building a target.

Note: Changes made in AD are not immediately reflected in Privilege Manager. Run the Default Import Directory Computers task again to import changes. You can search for "Default Import Directory Computers", edit the task and add a schedule to automatically import updates. The operation can be long-running for large domains, so be careful about the frequency with which you schedule the import.

Assigning Policies to Targets

To assign a policy to your target (or, stated another way, to add your target to a policy), find the policy on the Policies page and click Edit. If you are using the Simple Policy View, find the Targets tab; if using the Advanced Policy View, find the Conditions tab. You can remove existing targets by clicking the trash icon. Select Add Resource Target, find your target, select it, and click the Add button and Save.



Collections

A collection is a predefined list of computers. A collection is often meant to act as a filter and hence is also sometimes referred to as a filter.

Collections are typically defined by an SQL query that returns a list of computer IDs or other resource IDs.

Built-in collections are available in Privilege Manager, for example, "All x64 Windows Computers" and "Domain Controllers."

User defined collections are possible but typically expected to be created by Privilege Manager professional services, on behalf of a user, rather than directly by a user. Users are encouraged to define custom targets using existing (built-in) collections, groups, and fixed lists rather than creating new collections.

This topic provides the Privilege Manager filters catalog for all out-of-the-box filters that are baked into Privilege Manager and can be used to make your policy configuration process easy.

Win32 Executable Filters

Add Hardware Utility (hdwwiz.exe)	Filter used to identify the Device Pairing Wizard that appears when you click Add Device in Windows Vista and Windows 7
AOL Instant Messenger	Filter used to detect AOL Messenger
AppCmd for App Pool Recycling (appcmd.exe)	Filter used to identify the AppCmd executable
Backup and Restore Utility (sdclit.exe)	Filter used to identify the Windows Backup and Restore utility
Chrome	Filter used to detect Google Chrome web browsers
COM Elevation Host Utility (COMElevateHost.exe)	Filter to detect the COMElevateHost. This is used to detect when COM components are being elevated, such as the Network Adapter Properties
Command Processor (cmd.exe)	Filter used to identify the Windows command shell processor
Control Panel Utility (control.exe)	Filter used to identify the process used to launch Control Panel applets
Defragment GUI Utility (dfrgui.exe)	Filter used to identify the disk defragment utility within Windows
Device Pairing Wizard	Filter used to identify the Device Pairing Wizard that appears when you click Add Device in Windows Vista and Windows 7
Eudora	Filter used to detect Eudora email client
Firefox	Filter used to detect Firefox web browsers
Google Talk	Filter used to detect Google Talk
IIS Manager Executable Filter (inetmgr.exe)	Filter used to identify the IIS Manager executable
IIS Reset Executable Filter (iisreset.exe)	Filter used to identify the IIS Reset executable
Internet Explorer	Filter used to detect Internet Explorer web browsers
ISCSI Executable Filter (iscsipl.exe)	Filter used to identify the ISCSI executable
iTunes	Filter used to detect iTunes
Library Loader Utility (rundll32.exe)	Filter used to identify the dynamic library loader utility used by Windows to launch various system configuration applets
Microsoft Installer File Filter	Filter used to detect the Microsoft Installer. This filter can be used in policies with secondary file filters targeting specific MSI files
Microsoft Management Console (mmc.exe)	Filter used to identify the Microsoft Management Console Utility
Microsoft Windows Media Player	Filter used to detect Windows Media Player
MS Access	Filter used to detect Microsoft Access
MS Excel	Filter used to detect Microsoft Excel
MS FrontPage	Filter used to detect Microsoft FrontPage
MS InfoPath	Filter used to detect Microsoft InfoPath
MS Lync	Filter used to detect Microsoft Lync
MS OIS	Filter used to identify the Office Picture Manager Image Viewer
MS Outlook	Filter used to detect Microsoft Outlook
MS Powerpoint	Filter used to detect Microsoft PowerPoint
MS PPTVIEW	Filter used to detect Microsoft PowerPoint Viewer
MS Publisher	Filter used to detect Microsoft Publisher
MS Visio	Filter used to detect Microsoft Visio
MS VPreview	Filter used to detect Microsoft VPreview
MS Word	Filter used to detect Microsoft Word
MSN Messenger	Filter used to detect MSN Messenger
NLB executable Filter (nlbmgr.exe)	Filter used to identify the NLB Manager executable
ODBC Executable Filter (odbcad32.exe)	Filter used to identify the ODBC executable
Opera	Filter used to detect the Opera Browser
Outlook Express	Filter used to detect Microsoft Outlook Express

Performance Monitor Utility (perfmon.exe)	Filter used to identify the Performance Monitor launcher stub utility within Windows
Powershell (powershell.exe)	Filter used to identify the Windows Powershell command processor
Printer Control Utility (printui.exe)	Filter used to identify the printer management applet launcher within Windows
QuickTime	Filter used to detect QuickTime
RealPlayer	Filter used to detect RealPlayer
Resource Monitor (resmon.exe)	Filter used to identify the Windows Resource Monitor application
Safari	Filter used to detect Apple Safari on Windows
Scripting Host (cscript.exe)	Filter used to identify the Windows Scripting Host command-line utility
Scripting Host (wscript.exe)	Filter used to identify the Windows Scripting Host commandline utility
Setup Display Languages Utility (lpksetup.exe)	Filter used to identify the Install/Uninstall of Display Languages setup utility for Windows
ShareX	This filter targets the ShareX application
Skype	Filter used to detect Skype
Trillian	Filter used to detect the Trillian application
User's Temp Directory Win32 Executable Filter	Filter used to target any executable (exe) in a user's temp directory
Win32 Executables Discovered in the Last Week	This filter is limited to applications discovered on the endpoint within the last week
Winamp	Filter used to detect Winamp application
Windows Firewall (netsh.exe)	Filter used to identify the Windows Firewall netsh.exe
Windows Messenger	Filter used to detect Windows Messenger
Yahoo! Messenger	Filter used to detect Yahoo Messenger

Commandline Filters

Filter | Description | ----- | Add Printer Commandline Arguments | Filter used to identify the Add Printer UI applet | Azman.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Authorization Manager | Backup and Restore Commandline Arguments | Filter used to identify the Backup and Restore component, used as a commandline argument to a process | Certmgr.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Certificate Manager | Ciadv.msc Commandline Filter for MMC Snap-In | Filter used to detect Indexing Service Management | Compmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Computer Management | Dfragmgt.msc Commandline Filter for MMC Snap-In | Filter used to detect the MMC Snap-in used to defragment disks in Windows XP | Devmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Device Manager | Dhcpmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect DHCP Management | Diskmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Disk Management | Dnsmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect DNS Management | Eventvwr.msc Commandline Filter for MMC Snap-In | Filter used to detect Event Viewer | Fsmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect Shared Folders Management | Fsmgmt.msc Commandline Filter for MMC Snap-In | Filter used to detect File Resource Manager | Gpedit.msc Commandline Filter for MMC Snap-In | Filter used to detect Group Policy Editor | Hardware Wizard Applet | Filter used to identify a commandline argument referring to the Control Panel applet used to add new hardware | Lusrmgr.msc Commandline Filter for MMC Snap-In | Filter used to detect Local User and Group Management | Napclfcfg.msc Commandline Filter for MMC Snap-In | Filter used to detect NAP Client Configuration | Network Adapter Elevate Attempt | Filter used to detect when a user right-clicks on a network adapter and selects Properties | Ntmsmgr.msc Commandline Filter for MMC Snap-In | Filter used to detect Removable Storage Manager | Performance Monitor Component (perfmon.msc) | Filter used to detect Performance Monitor | Printmanagement.msc Commandline Filter for MMC Snap-In | Filter used to detect Print Management | Recycle App Pool Commandline | Filter used to identify the recycle command for application pools | Rsop.msc Commandline Filter for MMC Snap-In | Filter used to detect Resultant Set of Policy | Secpol.msc Commandline Filter for MMC Snap-In | Filter used to detect Local Security Settings Manager | Services.msc Commandline Filter for MMC Snap-In | Filter used to detect Services Manager | Sqlservermanager12.msc Commandline Filter for MMC Snap-In | Filter used to detect SQL Server Manager | System Control Panel Applet | Filter used to identify a commandline argument referring to the Control Panel applet used to change the system time and date settings | Tpm.msc Commandline Filter for MMC Snap-In | Filter used to detect Trusted Platform Module Management | Wbadmin.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Server Backup | Wf.msc Commandline Filter for MMC Snap-In | Filter used to detect Windows Firewall Management | Wmiingmt.msc Commandline Filter for MMC Snap-In | Filter used to detect WMI Management |

Environment Filters

Manual Application Compatibility Setting	Detects whether an application is being run with manual override options
User Access Control Consent Dialog Detected	This filter will match when an application that requires User Access Control consent is launched
User Requested Run As Administrator	Detects whether a user has right-clicked on an application and used Thycotic's custom 'Request Run as Administrator' option

Network Location Filters

Disconnected from Network	Filter used to detect when the computer is not attached to a network
Domain Network Location Filter	Filter used to detect when the computer is attached to a network classified as domain
Private Network Location Filter	Filter used to detect when the computer is attached to a network classified as private
Public Network Location Filter	Filter used to detect when the computer is attached to a network classified as public

Parent Process Filters

Thycotic Copy/Installer Helper Parent Process Filter	Filter used to detect when a user attempts to copy a file using the Privilege Manager copy helper
---	---

Secondary File Filters

Application Signed By Certificates Secondary Filter for policy: New Whitelist Signed Applications Policy	Filter used to capture secondary files (such as MSI or scripts) for policy: 'New Whitelist Signed Applications Policy'. This policy will add administrator rights to applications signed by the chosen certificates
Application Signed By Certificates Secondary Filter for policy: Whitelist Microsoft Security Catalog Applications	Filter to capture secondary files (such as MSI or scripts) for policy: 'Whitelist Microsoft Security Catalog Applications'. This policy will add administrator rights to applications signed by the chosen certificates
Target MSI and Scripts executed from the User's Temp Directory	Filter used to target MSI and Scripts executed from the User's Temp Directory

Security Rating Filters

VirusTotal	This filter will target VirusTotal for Reputation Checking
VirusTotal-Bad Rating	This filter will target VirusTotal for Reputation Checking
VirusTotal-Clean Rating	This filter will target VirusTotal for Reputation Checking
VirusTotal-Suspect Rating	This filter will target VirusTotal for Reputation Checking

VirusTotal Filters based on configuring VirusTotal integration in Privilege Manager. For steps to do this, see our [VirusTotal Integration Guide here](#)

Time of Day Filters

Business Hours (8:30AM to 5:30PM)	This filter is limited to 8AM to 6PM weekdays
Business Hours (8AM to 6PM)	This filter is limited to 8AM to 6PM weekdays
Business Hours (9AM to 5PM)	This filter is limited to 9AM to 5PM weekdays
Weekends	This filter is limited to weekends

User Context Filters

Administrators	Detects when an application is running with elevated (administrator) permissions
Administrators (Include Disabled)	Detects when an application has an administrator user token

File Filters

Application Compatibility File Filters

Administrative Rights Required Application Compatibility Filter	This filter tests whether Windows has detected that this executable requires administrative rights
Generic Installer Detection Filter	This filter indicates that Windows has detected that an executable is an Application Setup
Highest Available Application Compatibility Filter	This filter tests whether Windows has detected that this executable required highest available rights
Specific Installer Detection Filter	This filter indicates that Windows has detected that an executable is an Application Setup
Specific Non Installer Detection Filter	This filter indicates that an executable has been flagged as not being an Application Setup

Manifest Filters

Require Administrator Rights Manifest Filter	This filter tests whether an executable is marked as requiring Administrative rights
Require Highest Available Rights Manifest Filter	This filter tests whether an executable is marked as requiring highest available rights
Manifest Present Filter	This filter tests whether an executable has a security manifest

File Owner Filters

System (Wheel) File Owner	Files that are owned by the Wheel Group (Unix)
System File Owner Filter	Filter used to detect files owned by the System account

Trusted Installer File Owner Filter Filter used to detect files owned by the Trusted File Owner account

File Specification Filters

Any Package (MacOS)	Target .pkg and .mpkg files
App Store Preference Pane (MacOS)	Filter used to detect App Store Preference Pane in Mac
Common Executable Folders	Filter used to detect files in common executable directories, such as C:\Windows, C:\Program Files, and C:\Program Files(x86)
Date and Time Preference Pane (MacOS)	Date and Time Preference Pane (MacOS)
Default App Bundles File Specification Filter	The default filter for discovering app bundles on MacOS
Default File Specification (All executable types)	Specifies all executable file types in Windows and Program files
Default File Specification (MacOS)	The default filter for discovering executable files on MacOS
Default File Specification (Windows)	This specifies executables in Windows and Program files
Documents and Settings	Filter used to detect files in the Downloaded Program Files directory
Drivers	Filter used to detect files in the C:\Windows\System32\drivers directory
Energy Saver Preference Pane (MacOS)	Filter used to detect the Energy Saver Preference Pane in Mac
Executables in Windows Directories	This specifies executables in Windows directories
Executables in Windows Directories (All executable types)	Specifies all executable file types in Windows directories that are not present in a signed security catalog
Mac OS/Users/File Specification	The default filter for files in the /Users/ directory on MacOS
Network Drive Filter	Specifies files present on network file systems
Optical Drive Filter (CD/DVD)	Specifies files present on optical drives (CD/DVD)
Parental Controls Preference Pane (MacOS)	Filter used to detect the Parental Controls Preference Pane in Mac
Printers and Scanners Preference Pane (MacOS)	Filter used to detect the Printers and Scanners Preference Pane in Mac
Program Data	Filter used to detect files in the C:\ProgramData\ directory
Program Files	Filter used to detect files in the C:\Program Files\ directory
Program Files (x64 on Win32)	Filter used to detect files in the C:\Program Files\ directory
Program Files (x86)	Filter used to detect files in the C:\Program Files(x86)\ directory
Removable Drive Filter	Filters files present on removable drives such as Floppy Drives and USB devices
Security and Privacy Preference Pane (MacOS)	Filter used to detect Security and Privacy Preference Pane in Mac
Sharing Preference Pane (MacOS)	Filter used to detect the Sharing Preference Pane in Mac
System Catalog Folder	Filter used to detect files in the CatRoot directory
System Preferences (MacOS)	Filter used to detect the System Preferences Preference Pane in Mac
Temporary ASP.NET 1.0 Files	Filter used to detect files in the .NET 1 Temp directory
Temporary ASP.NET 1.1 Files	Filter used to detect files in the .NET 1.1 Temp directory
Temporary ASP.NET 2.0 Files	Filter used to detect files in the .NET 2 Temp directory
Temporary Files	Filter used to detect files in the C:\Windows\Temp directory
Thycotic Copy/Installer Helper Application	Filter used to detect usage of the Privilege Manager copy helper
Time Machine Preference Pane (MacOS)	Filter used to detect the Time Machine Preference Pane in Mac
Uncommon Executables Folders	Filter used to detect files in the Uncommon directories
Users and Groups Preference Pane (MacOS)	Filter used to detect the Users and Groups Preference Pane in Mac
User's Directory Collection File Specification Filter	Used to target any file in the user's temp directory
User's Downloads Directory File Specification Filter	Used to target any file in the user's temp directory
User's Temp Directory File Specification Filter	Used to target any file in the user's temp directory
Windows Directory	Filter used to detect files in the C:\Windows directory
Windows Directory (Include Subdirectories)	Filter used to detect files in the C:\Windows\ directory

Windows Dll Cache	Filter used to detect files in the C:\Windows\System32\dlldata directory
Windows Side By Side	Filter used to detect files in the C:\Windows\WinSxS\ directory
Windows Software Distribution	Filter used to detect files in the Windows Software Distribution directory
Windows\System32	Filter used to detect files in the C:\Windows\System32 directory
Windows\System32 (Include Subdirectories)	Filter used to detect files in the C:\Windows\System32\ directory
Windows\SysWOW64	Filter used to detect files in the SysWOW64 directory
Windows\SysWOW64 (Include Subdirectories)	Filter used to detect files in the SysWOW64\ directory

Security Catalog Filters

Present In Signed Security Catalog	Filter used to detect Operating System Files and other trusted files dynamically on each system by using that machine's Signed Security Catalog. This filter does not need to be modified on the server
---	---

Miscellaneous Filters

App Bundle Filters

All Application Bundles Filter (MacOS)	Filter used to detect All Applications Bundles
---	--

Coff Header Filters

32-bit Executables	Filter used to detect files with the 32-bit executable machine type header set
All Executable Types	This filter includes all executable types
Commandline Executables	Filter used to detect files with the Windows console subsystem header set
GUI Executables	Filter used to detect files with the GUI header set
Native Executables	Filter used to detect files with the executable header set
Windows CE Executables	Filter used to detect files with the Windows CE Subtype header set
Program File Executables	Filter used to detect files with the executable or DLL header set
Posix Executables	Filter used to detect files with the POSIX header set
X64 Executables	Filter used to detect files with x64 machine type header set

File Parameter Collections

All Blacklist Security Rated Applications	This collection contains all applications that have been blacklisted by applying a security rating
All Executables Discovered in Last 2 Weeks	Filter used to detect files that have been discovered by the server in the past 2 weeks
All Executables Discovered in Last Day	Filter used to detect files that have been discovered by the server in the past day
All Executables Discovered in Last Week	Filter used to detect files that have been discovered by the server in the past week
All Executables Discovered in Last Month	Filter used to detect files that have been discovered by the server in the past month
All Greylist Security Rated Applications	This collection contains all applications that have been greylisted
All Unclassified Applications	This collection contains all applications that have not been classified by a security rating
All Whitelist Security Rated Applications	This collection contains all applications that have been whitelisted by applying a security rating

Mach-O Header Filters

macOS DyLib	Identifies dynamic library (dylib) files according to their embedded Mach-O header (not specifically according to file name)
macOS Executables	Identifies files marked as executables according to their Mach-O header (not file mode changes via chmod)

In Privilege Manager, taking action is the name of the Application Control game. Once you know how to accurately identify events via filters, the next crucial step in policy creation is to make stuff happen by applying specific actions to your filtered targets. This begs the question: what actions are possible to perform in Privilege Manager?

The most popular and well-known action categories in Application Control include:

- **Blocking Actions** - Blocking an application simply means: deny it, or prevent it from running.
- **Monitoring Actions** - This is a category of actions that can be applied to unknown applications that attempt to run. Sandboxing is another term often linked to monitoring, because you can create policies that link to reputation checking tools (like VirusTotal) to perform smart actions once an unknown file's reputation has been verified.
- **Elevation Actions** - Allowing an application to run (Whitelisting) is good and well for trusted programs, but many trusted applications also require a higher credential set than your end users normally have access to. The elevation action category will allow an application to run with elevated permissions so any user can, for example, install that trusted HP printer on your network without taking time out of a HelpDesk employee's day. Implementing elevation policies allow "Least Privilege" to be implemented by your organization, eliminating the need for local users to have full administrator access on their computer.
- **Workflow Actions** - Some actions explicitly enforce an organization's workflow system. The big example here is the "Request Access" action that will prompt a user for the reason they are trying to access an application for verification purposes and auditing.
- **Display Message Actions** - Display messages are paired with one of the action types listed above. Display Message Actions are customizable and serve to tell the end user what is happening and why.

For a more complete (and more specific) list of all out-of-the-box Privilege Manager actions and types of actions, see the [List of Default Actions](#) topic.

Creating a New Action Manually

Navigate to **Admin | Actions** in Privilege Manager and click **Add Action**. Under Action Details, select a platform type and then choose an action type from the dropdowns (see our Actions' Catalog for descriptions of action types).

- Windows:

The screenshot shows the 'New Action' dialog box with the 'Action Details' section. The 'Platform' dropdown is set to 'Windows'. The 'Action Type' dropdown is open, showing a list of available actions: ActiveX Installer, Adjust Process Rights, Application Classification, Apply Application Compatibility Fix Action, Deny File Access, Deny Windows Hooking, Display Advanced Message, Display User Message, Encrypt Application Files, Enhanced Mitigation (EMET) Action, Execute Application, Sandbox Action, Set Environment Variable Action, and Set Process Security Descriptor Action. There are 'Back' and 'Create' buttons at the bottom left of the dialog.

- macOS:

The screenshot shows the 'New Action' dialog box with the 'Action Details' section. The 'Platform' dropdown is set to 'Mac OS'. The 'Action Type' dropdown is open, showing a list of available actions: Allow Copy Action (MacOS), Display Advanced User Message (MacOS), and Display User Message. There are 'Back' and 'Create' buttons at the bottom left of the dialog.

Name your new action and type a Description, then click **Create**.

Editing options for this action will depend on the type of was action selected from the drop-down.

Message Actions

Messages are the most common application action used in Privilege Manager. These messages are presented for end users on their endpoints. There are two kinds of messages:

- Basic, these display as smaller pop-ups directly from the taskbar area. They display and fade automatically. From the Action Type drop-down these are the [Display User Message](#) actions for both Windows and macOS.
- Advanced, these messages display as a user dialog, requiring users to justify access to a certain application or to warn the user. Most of these messages require user interaction, but some can be set to fade in and out for the end user. From the Action Type drop down these are the [Display Advanced Message](#) for Windows and [Display Advanced User Message \(MacOS\)](#) for macOS endpoints.

Both basic and advanced messages are useful for providing feedback to users that an application is being blocked, usage of the application is being logged, or any message that the end user should see.

Basic vs. Advanced Messages

Basic messages briefly pop up from the end user's task bar. They display like other Windows notifications, are shown on the screen, and then disappear without any user interaction required.

Basic messages do not include custom branding or logos. It is easiest to edit basic messages via Privilege Manager's UI. However, the default message may suffice for some use. Basic messages only display a message. These messages do not perform an action. For example, the basic Deny Execute Message should be used in conjunction with the Deny Execute action.

Advanced messages display as a new dialog, typically in the center of the screen, and usually require an interactive action from the end user - entering a justification, enter credentials, waiting for approval, selecting a continue or cancel button, etc.

Advanced message actions are used for justification and approval policies. The 'Application Denied Notification Action' is the only default advanced message that does not require an interactive action from the end user. While this message has a cancel button to remove the message, this message will fade from the user's screen after a short period of time.

Advanced messages include branding, which can be customized. Some fields are recommended to edit in the XML instead of the UI. These details are expanded in the section on Customizing Advanced Messages.

Types of Advanced Message Actions

There are three categories of advanced messages:

- Advanced Feedback Messages - require information from the end user.
- Approval Request Messages - require information from the end user and approval from the application support team.
- No Required Input Messages - display information to the end user, but do not require information from the end user. May require a button push to clear the message.

Advanced Feedback Messages

Advanced feedback messages require users to justify their need to use an application.

Authentication Justification Message Action

This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application.

The screenshot shows a dialog box titled 'Application Notice: msiexec' with a yellow header and a 'thycotic' logo. The main text reads: 'This application has **not been approved** for use according to [corporate policy](#). Please discontinue use or enter your justification to continue.' Below this, it says 'Application: msiexec' and 'Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.' There is a text input field labeled 'Reason (required):'. At the bottom, there are fields for 'User name: MPT-WINPC01\Administrator' and 'Password (required):', along with 'Continue' and 'Cancel' buttons.

Group Member Authenticated Message Action

This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member. This process is also known as an over-the-shoulder request, meaning that the end-user will have to get their boss or a member of a specific domain user group to approve the request.

The screenshot shows a dialog box titled 'Application Notice: msiexec' with a yellow header and a 'thycotic' logo. The main text reads: 'This application has **not been approved** for use according to [corporate policy](#).' Below this, it says 'Application: msiexec' and 'Date: 11/4/2019 4:22:53 PM'. A blue information box contains the text: 'This process requires authentication by a member of the following group. Group name: Please have a member of this group authorize this request to continue.' Below this, there are fields for 'User name: MPT-WINPC01\Administrator' and 'Password (required):', along with 'Continue' and 'Cancel' buttons.

Justify Application Elevation Action

This action will display a justification prompt to the user before allowing the application to run. The Justify Application Elevation Action is to be used with the User Requested Run As Administrator filter in an application control policy. This action collects information from users and creates reports on the server for approval requests.

Application Elevation: msixec

Application Elevation

Please provide a reason as to why you require this application to be run with elevated rights.

Application: **msixec**
User: **MPT-WINPC01\Administrator**

Type a brief explanation describing why this application is necessary. This explanation **will be recorded** and may be reviewed by the IT staff for consideration into corporate policy.

Reason (required):

Continue Cancel

Justify Application Message Action

This action will display a justification prompt to the user before allowing the application to run. It is used to collect information from users and create reports on the server with reasons why a user was running an application that hasn't been approved or denied yet.

Application Elevation: msixec

Application Elevation

Please provide a reason as to why you require this application to be run with elevated rights.

Application: **msixec**
User: **MPT-WINPC01\Administrator**

Type a brief explanation describing why this application is necessary. This explanation **will be recorded** and may be reviewed by the IT staff for consideration into corporate policy.

Reason (required):

Continue Cancel

Approval Request Messages

The approval request messages are similar to the justification messages because they both gather feedback from end users and report it in the Privilege Manager console. Approval request messages also allow for end-users to see a waiting screen until their request has been either approved or denied.

Approval Request Form Action

This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application.

Application Notice: msixec

Application Notice

This application has **not been approved** for use according to [corporate policy](#). Please discontinue use or enter your justification to continue.

Application: **msixec**
User: **MPT-WINPC01\Administrator**

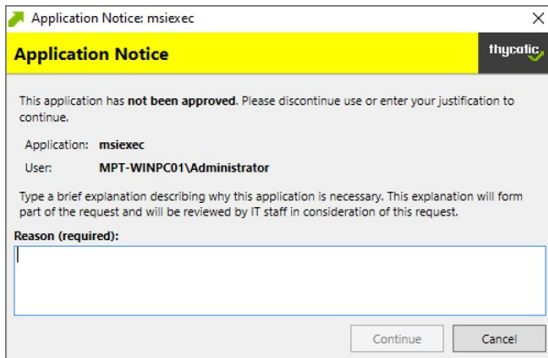
Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.

Reason (required):

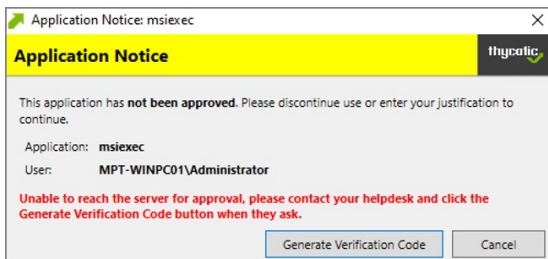
Continue Cancel

Approval Request (with Offline Fallback) Form Action

This action displays an approval request form before allowing the application to run. These messages will then show a waiting screen until the request is either approved or denied by the appropriate Privilege Manager user/admin. With this advanced message, the same dialogue box as the Approval Request Form Action will appear:



If the machine is offline or can't connect to Privilege Manager to upload the request, another dialogue box will then appear to prompt the end user to contact the helpdesk and generate a verification code:

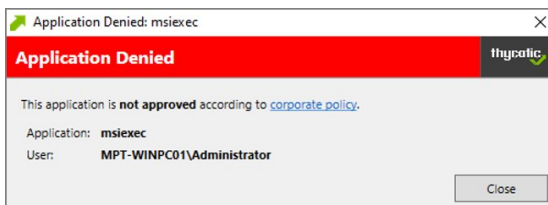


No Required Input Messages

No required input messages differ from the advanced feedback message actions because they do not require a justification to continue. End users need only acknowledge the displayed message. This feature requires that the Microsoft .Net Framework is installed on client machines.

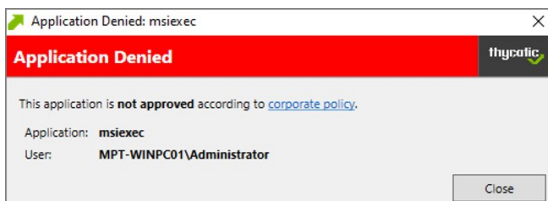
Application Denied Message Action

This action stops an application from being launched and will display a notification of denial to the user attempting to run a process controlled by a policy.



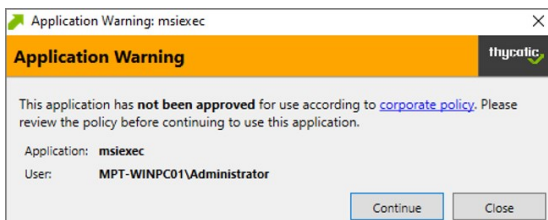
Application Denied Notification Action

This action will display a notification to the user that the process has been denied by a policy. The notification window fades in and out automatically and will close after a defined period of time.



Application Warning Message Action

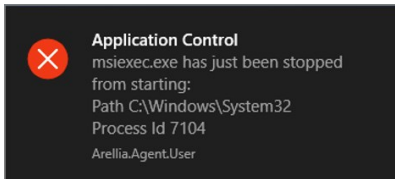
This action will display a warning to the user before allowing the application to run.



Types of Basic Messages

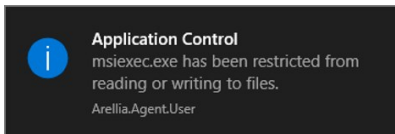
Deny Execute Message

This action displays a message to the user informing that an application has been denied execution. The Deny Execute Action needs to be used with this message.



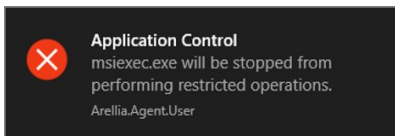
Deny Files Read and Write Access Message

This action displays a message to the user informing that an application will be restricted from certain file access. The Deny Read/Write Access to Microsoft Office Document Files Action needs to be used with this message.



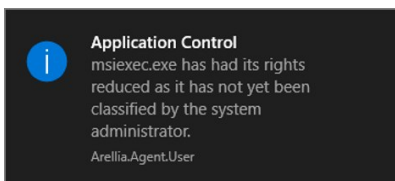
Windows Hooking Message

The action displays a message to the user informing them that an application will be stopped from interacting with other applications. The Deny Windows Hooking Action should be used with this message.



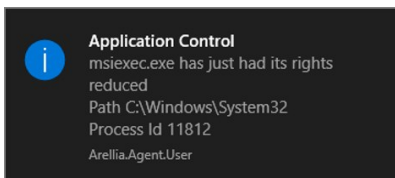
Limit Process Rights for New Applications Message

This action displays a message to the user informing that an application has had its rights reduced. The Remove Administrator Rights or Remove Advanced Privileges Action needs to be used with this message.



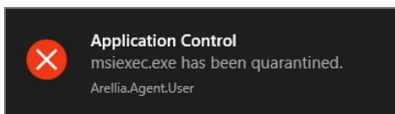
Remove Rights Message

This action displays a message to the user informing them of an associated action. The Remove Administrative Rights Action or Remove Advanced Privileges Action should be used with this message.



Quarantine Message

This action displays a message to the user informing that an application has been quarantined. The File Quarantine Action should be used with this message.



Display User Message Action

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

Action > Test Display User Message Action

Details Related Items Change History

Details

Name	* Test Display User Message Action
Description	Testing Display User Message action
Platform	Windows

Display User Message Settings

Title	*
Message	*
Icon type	* Information ▾
Display Timeout	* 3 Second(s) ▾

This action is available for both Windows and macOS systems.

Parameters

The following Display User Message Settings can be specified:

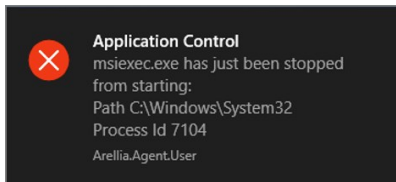
- Title
- Message
- Icon type, which can be specified as Information, Warning, Error, Thycotic, or Program.
- Display timeout setting, which can be specified in Seconds, Minutes, Hours, Days, or Weeks.

Examples

- [Deny Execute Message](#)

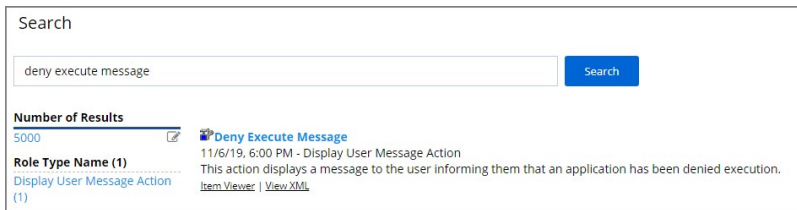
Deny Execute Message

The Deny Execute Message does not include company branding and is easy to edit in the Privilege Manager console. The default of this basis user message action is displayed like this:

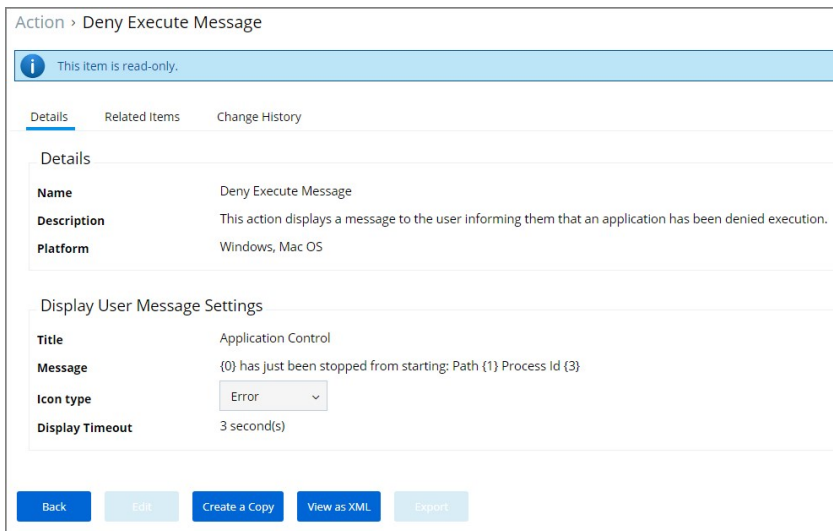


Customization

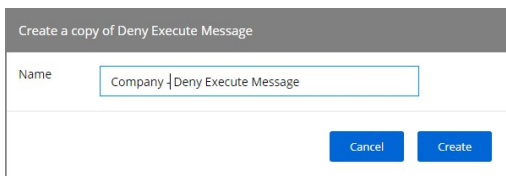
1. In Privilege Manager, search for the default message that will be customized. In this example, we search for the default **Deny Execute Message**.
2. Select the item from the search results.



3. This is a read-only action, to customize the default message, users need to use the **Create a Copy** option.



4. Click **Create a Copy**.
5. Enter a name for the new message action. It is recommended to use standard naming conventions with your custom items, e.g. beginning custom names with your company name is a great way to differentiate between the default items and your custom items.



6. Click **Create**.
7. Click **Edit**.
8. Customize the Title and Message, use the Icon Type drop-down to specify the type, and set the Display Timeout.

Display User Message Settings

Title	* Application Control
Message	* (0) has just been stopped from starting: Path (1) Process Id (3)
Icon type	* Error
Display Timeout	* 3 Second(s)

Save Cancel Export

9. Click **Save**.

Display Advanced Message Action

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

Action > Test Display Advanced Message Action

Details Related Items Change History

Details

Name Test Display Advanced Message Action

Description This action will display a customized message to the user, allowing for feedback before running an application.

Platform Windows

Settings

Require authentication:

- By the interactive end-user
- By a member of the group:

Wait for message prompt to complete before running application

Window Design

Parameters

The following Display Advanced Message Settings can be specified:

- Require authentication.
 - By the interactive end-user
 - By a member of the group
 - Wait for message prompt to complete before running application

Further the Window Design parameters can be set. Those settings include customization of company logo for branding, label, status, button, instruction, prompt, and reason texts just to name a view.

Window Design

Message prompt logo

Application label Application:

Approval status label Approval status:

Approval status section A previous request for this application has been submitted for review.

Cancel button text Cancel

Continue button text Continue

Information section This application has not been approved for use according to corporate policy. Please discontinue use or enter your justification to continue.

Instruction section Type a brief explanation describing why this application is necessary. This explanation will form part of the request and will be reviewed by IT staff in consideration of this request.

Prompt title Application Notice

Reason label Reason (required):

Refresh button text Refresh

Title Prefix Administrator

User label User:

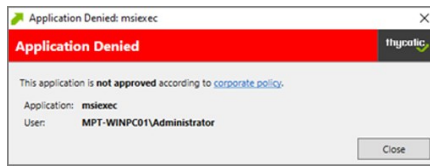
Examples

- [Create Custom Notifications](#)

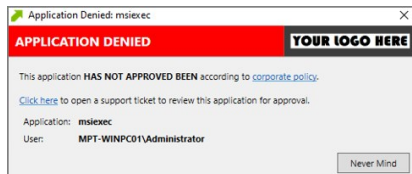
Create Custom Notifications

The default Application Denied Notification Action can be edited/replaced by a customized notification action to better suite a specific customer need.

Example of Default Notification:



Example of Custom Notification:



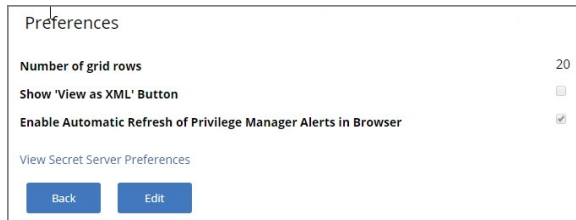
Enable View as XML

To edit the message text the **View as XML** button has to be enabled in your console.

1. Hover (do not click) over your user icon, click **Preferences**.



2. Verify the **Show 'View as XML' Button** checkbox is enabled. If the checkbox is not selected, click **Edit**.



3. Select the checkbox and click **Save**.

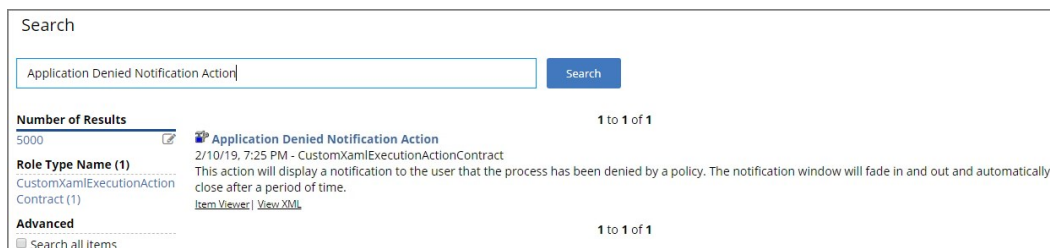
Customizing the Application Denied Notification Action

Default Actions shouldn't be edited directly, however Privilege Manager default items can be copied for customization purposes.

1. In the top Search box enter Application Denied Notification Action.



The search results are displayed.



2. Click on the name of the Action **Application Denied Notification Action**.

Action > Application Denied Notification Action

i This item is read-only.

Details Related Items

Details

Name Application Denied Notification Action

Description This action will display a notification to the user that the process has been denied by a policy. The notification window will fade in and out and automatically close after a period of time.


Settings **?**

Require authentication:

- By the interactive end-user
- By a member of the group:

Wait for message prompt to complete before running application

Window Design

Message prompt logo 

Application label Application:

Information section This application is not approved according to corporate policy.

Prompt title Application Denied

Title Prefix Application Denied

User label User:

Back Edit Create a Copy View as XML

3. Click **Create a Copy**.

4. Enter a customized and meaningful name for the action. It is recommended to use standard naming conventions with your custom items. Beginning custom names with your company name is a great way to differentiate between the default items and your custom items.

Create a copy of Application Denied Message Action

Name

5. Click **Create**. Once you click Create, the new action page opens.

6. Click **Edit**.

7. To upload a custom image file click **Choose File**. You can upload a custom logo, the file size should be under 128 KB and the width should be 500 pixels or less with a maximum height of 34 pixels.


Name * CompanyName Application Denied Notification Action

Description
This action will display a notification to the user that the process has been denied by a policy. The notification window will fade in and out and automatically close after a period of time.

Settings ⓘ

Require authentication:
 By the interactive end-user
 By a member of the group:
 Wait for message prompt to complete before running application

Window Design

Message prompt logo

 No file chosen

Application label
Application:

Information section
This application is not approved according to corporate policy.

Prompt title
Application Denied

Title Prefix
Application Denied

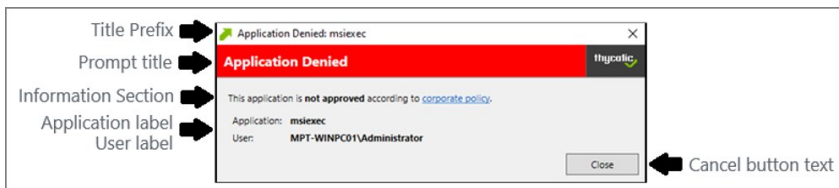
User label
User:

The logo that is uploaded should NOT be a high-resolution image. This image will be delivered to every endpoint with every message in which it's used. The smaller the image, the better, for sending the message to the endpoints and for the endpoint to load the message.

8. Click **Save**.

Editing the Text in the UI

Privilege Manager makes it very easy to edit the text of a message. The fields are listed in alphabetical order on the item's view page. Compare each field to this overview image:



Most of the lines do not include individualized stylings per line. Editing the text in the UI will simply edit the text as required. The **Information Section** field includes html formatting for the hyperlink to the corporate policy. That hyperlink will be removed if the text is edited on the message's edit page.

Window Design

Message prompt logo
YOUR LOGO HERE
 No file chosen

Application label
Application:

Cancel button text
Never Mind

Information section
This application HAS NOT APPROVED BEEN according to corporate policy.
[Click here to open a support ticket to review this application for approval.](#)

Prompt title
APPLICATION DENIED

Title Prefix
Application Denied

User label
User:

Note: It is NOT recommended to edit the Information Section directly on the message's edit page. Instead, editing the Information Section via XML retains the html formatting for this line. If no changes are made to the Information Section, the html formatting is retained. All other fields can be changed except the Information Section and the html formatting for the Information Section is retained.

Editing the Text via XML

1. Click **View as XML**.

Import Items

CompanyName Application Denied Notification Action

```

1 <CustomXamlExecutionActionContract xmlns:adc="http://schemas.arellic.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays"
2 <adc:Attributes>NoReplication System</adc:Attributes>
3 <adc:Description>This action will display a notification to the user that the process has been denied by a policy. The notification window will
4 <adc:FolderId>c602777a-86b3-4450-b5af-1dcbce252071</adc:FolderId>
5 <adc:ItemId>787334b6-00b5-480a-a805-604879cd57cf</adc:ItemId>
6 <adc:Name>CompanyName Application Denied Notification Action</adc:Name>
7 <adc:ProductId>27be0b9a-d037-4d53-b748-bc6651461fe4</adc:ProductId>
8 <adc:State i:type="adc:ItemState">
9 <adc:CreatedById>2dee6e6e-5098-44ac-ad36-6aae8fefa7</adc:CreatedById>
10 <adc:CreateDate>
11 <dc:DateTime>2019-03-01T22:07:36.5405815Z</dc:DateTime>
12 <dc:OffsetMinutes>-480</dc:OffsetMinutes>
13 </adc:CreateDate>
14 <adc:EffectiveSecuredId>01117848-22d5-4e76-8989-19470b7a3a64</adc:EffectiveSecuredId>
15 <adc:EffectiveSecuredInheritedId>77cd2974-8c40-4ae6-931e-fe60087781a9</adc:EffectiveSecuredInheritedId>
16 <adc:IsCreated>true</adc:IsCreated>
17 <adc:ModifiedById>adf3fb34-1f5e-5a84-90ae-b3c5aa2f8ad</adc:ModifiedById>
18 <adc:ModifiedDate>
19 <dc:DateTime>2019-03-01T22:07:36.5405815Z</dc:DateTime>
20 <dc:OffsetMinutes>-480</dc:OffsetMinutes>
21 </adc:ModifiedDate>
22 <adc:VisualStateId>785143a9-13f8-5332-ad68-281ea027f96a</adc:VisualStateId>
23 </adc:State>
24 <AdjustSession>false</AdjustSession>
25 <CommandLine />
26 <Executable>.\ArellicDisplayXamlAction.exe</Executable>
27 <TerminateExitCode>0</TerminateExitCode>
28 <WaitOnApplication>true</WaitOnApplication>
29 <ChildAssociations />
30 <OwnsItemIds />
31 <RequireLogon>false</RequireLogon>
32 <UserGroupId i:nil="true" />
33 <Xaml><![CDATA[<window
34 xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
35 xmlns:vc="http://schemas.microsoft.com/winfx/2006/xaml"

```

Back Edit

2. Change the notification text in the XML viewer:

Line 82 has the following:

```
<Paragraph><Run>This application is <Run><Bold><Run>not approved</Run></Bold><Run> according to </Run><Hyperlink TargetName="" blank" NavigateUri="http://www.example.com/policy"><Run>corporate policy</Run></Hyperlink></Run></Paragraph>
```

Edit this space with the URL and the name of the Hyperlink you would like for your pop up Window.

```
<Paragraph><Run>This application HAS NOT BEEN APPROVED according to </Run><Hyperlink TargetName="" blank" NavigateUri="http://www.example.com/policy"><Run>corporate policy.</Run><Run>Click here, </Run><Hyperlink TargetName="" blank"
NavigateUri="http://www.thyctic.com/helpdesk"><Run>to open a support ticket for review this application for approval.</Run></Hyperlink></Run></Paragraph>
```

3. Change the default timeout:

If you wish to change the default time out for how long the Deny Notification stays up (default is 6 seconds), edit Line 299:

```
<Interaction.Triggers>
<EventTrigger EventName="Loaded">
<adc:InvokeCommandWithDelayAction x:Name="CloseAction" Command="{BindingCloseCommand}" Delay="00:00:06" />
</EventTrigger>
</Interaction.Triggers>
```

To change it to 15 seconds, edit this elements delay parameter to 15:

```
<adc:InvokeCommandWithDelayAction x:Name="CloseAction" Command="{BindingCloseCommand}" Delay="00:00:15" />
```

4. Click **Import**. If you get an error, please address your changes. Errors are indicated with a red dot. Save any edits when resolving errors.

Updating the Policy with the new Action

After creating a custom notification action, the policy using the default notification needs to be updated.




1. Navigate to **Admin I Policies** and locate the policy that uses the default Notification.
2. Go to the **Actions** tab.
3. Click **Edit**.

Policy > Global Deny

General Conditions **Actions** Policy Enforcement Deployment

Send policy feedback

Actions to apply to the application

TYPE	ACTION NAME
	Application Denied Notification Action 
	Add Action

4. To the right of the current default action click the trash can.
5. Click Confirm Remove.

Privilege Manager

Are you sure that you want to remove this action?

Application Denied Notification Action

[Confirm Remove](#) [Cancel](#)

6. Click **Add Action**.

Policy > Global Deny

General Conditions **Actions** Policy Enforcement Deployment

Send policy feedback ⓘ

Actions to apply to the application

TYPE	ACTION NAME
+	Add Action

7. Search for the name of your Custom Action. If it does not show up, click the Refresh icon to reload the Actions into the cache.

Actions to apply to the application

TYPE	ACTION NAME	
+	ADD ACTION	
View by	List <input type="text" value="comp"/> ↻	
<input type="checkbox"/>	NAME	TYPE
<input type="checkbox"/>	Application Compatibility Testing	ApplicationVerifierLuaContract
<input checked="" type="checkbox"/>	CompanyName Application Denied Notification Action	CustomXamlExecutionActionContract
<input type="checkbox"/>	ForceAdminAccess Application Compatibility Fix	ApplicationCompatibilityContract

8. Check the box next to the custom action, click Add.

Actions to apply to the application

TYPE	ACTION NAME	
+	ADD ACTION	
View by	List <input type="text" value="comp"/> ↻	
<input type="checkbox"/>	NAME	TYPE
<input type="checkbox"/>	Application Compatibility Testing	ApplicationVerifie
<input checked="" type="checkbox"/>	CompanyName Application Denied Notification Acti...	CustomXamlExe
<input type="checkbox"/>	ForceAdminAccess Application Compatibility Fix	ApplicationCompe

[Add](#) [Cancel](#)

9. Click **Save**.

Policy changes are automatically propagated to the endpoints. Note, that this might not be instantaneous based on the refresh cycle.

For Privilege Manager Versions Prior to 10.7

If you are on a system version **prior to 10.7**, navigate to the Deployment Tab on the Policy and click **Cache Policy**.

Policy > Global Deny

General Conditions Actions Policy Enforcement Deployment

Policy Deployment

Policies are automatically deployed to targeted managed computers on a schedule. Use the Policy Deployment tab to understand

[Refresh Status](#) [Cache Policy](#) [Run Policy Targeting Update](#)

Policy Cached on Server	False
Policy Modified	Mar 6, 2019, 10:46:02 AM
Policy Last Cached	Mar 6, 2019, 10:41:44 AM
Total Resources Targeted	8
Resources with Policy	8
Resources with Latest Version	0

[Back](#) [Edit](#) [Simple Policy View](#) [Create a Copy](#) [Delete](#) [View as XML](#) [See Events](#)

You can then go to your test endpoint and open the **Thycotic Agent Utility** and click **Update** to get the new Action on the test endpoint.

Display Advanced User Message Action (MacOS)

Display messages are paired with another action type. They are customizable and serve to tell the end user what is happening and why. Advanced messages pop up in the middle of the screen, whereas Basic User messages appear as smaller pop-ups directly from the taskbar area.

Action > Test Display Advanced User Message Action (MacOS)

Details Related Items Change History

Details

Name Test Display Advanced User Message Action (MacOS)

Description

Platform Mac OS

Settings

Title

Message Type

Message 1

- Deny Application Message
- Deny Application Message**
- Warning Message
- Justify Application Usage
- Deny Application with justification
- Approval Request Message

Parameters

The following Display Advanced Message Settings can be specified:

- Title
- Message Type, such as deny, justify, warn, etc.
- Message, which is the actual text of the message displayed to the user.

This topic explains the Adjust Process Rights Action and Unrestricted Tokens in Privilege Manager.

When elevating process rights with Application Control Solution (ACS) on Windows, there are times when the rights given by ACS appear to be insufficient. The process still doesn't work as it does when the user is logged in as Administrator, accepts the UAC box, or the process is run with the right-click Run As Administrator option. Sometimes an error is returned stating insufficient rights to access.

Microsoft with the release of Windows Vista introduced changes to security which included creating two tokens for users when they log in. For more information refer to the [Microsoft Documentation on Restricted Tokens](#).

The lower privilege token is the one always used unless the user goes through UAC or other processes. ACS allows administrators to choose which token should be used to elevate certain processes. The lower privilege token, if it works, is the better option as it has fewer privileges and thus protects the system better. But if necessary, the higher-privilege token can be used by ACS when manipulating the process's security configuration.

The following are the Privilege Manager default Adjust Process Rights Actions. As with all actions delivered with Privilege Manager, these actions cannot be modified. They can be copied and then customized and as many actions as necessary can be created for a custom implementation:

- Add Administrative Rights
- Add Administrative Rights - Unrestricted
- Adjust Process Rights for Resource Monitor
- Remove Administrative Rights
- Remove Advanced Privileges Action

Each of those actions has by default Related Items associated, which need to be considered when customizing an action.

Adjust Process Rights Action Settings Explained

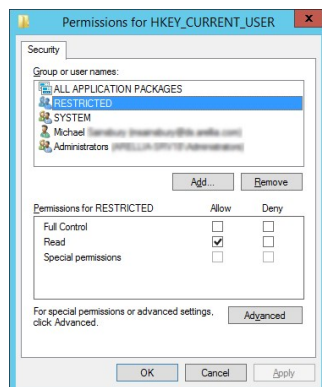
The application action elevates or restricts the permissions and/or privileges held by a process security token. By default, each process inherits the user's security token.

The four main areas to customize are:

- Selecting an **Action Type**, which can either Elevate Rights or Restrict Rights. When the adjustment is a rights restriction, there is an advanced feature that allows you to apply restricted Security Identifiers (SIDs), which further restricts access to securable objects. More about this under the [What is a Restricted SID](#) topic.
- Adding or Removing **Windows Privileges**, these come prepopulated with a set of default recommendations for each out of the box Action. To learn more about these Windows Privileges visit [Microsoft's Documentation about User Rights Assignment](#).
- Adding or Removing **Build-in Roles**, these are the roles that provide file level access to a system and they are based on group membership.
- Adding or Removing **Well-known Accounts**, these are specifying the integrity levels at which processes can run. Also refer to [Microsoft's Documentation about Mandatory Integrity Control](#).

What is a Restricted SID?

A restricted ID is an access token that modifies a user's access to securable objects and controls a user's ability to perform various system-related operations on the local computer.



When a restricted process or thread tries to access a securable object, the system performs two access checks, using the

- token's enabled SIDs, and
- the list of restricted SIDs.

Access is granted only if both access checks allow the requested access rights.

When to use restricted ID

Use a restricted SID to further restrict the applications in the sandbox, which you can use as another method of graylisting. In other words, this is a way to protect yourself against unknown applications if you don't want to implement blacklisting.

The restricted SID will allow only Read access to the user registry but not to the local machine registry. Also, restricted processes do not have rights to open any network-based resource, such as file servers. As a result, the restricted SID will be able to do very little and apps may not work correctly under this model. Ultimately, apps in the sandbox that have restricted SID applied to them will be severely locked down.

Using Apply Restricted SID

When you select Restrict Rights and then Apply Restricted SID, you add the Restricted SID to the process. When evaluating security for any operation, when there is any Restricted SID specified then not only does the Security Descriptor need to allow access to the user, but explicitly to the Restricted SID.

How to Add Windows Permissions

Windows permissions are specific OS based permissions to perform actions, like changing system time or taking ownership of a files vs. accessing securable resources. To learn more about these Windows Privileges visit [Microsoft's Documentation about User Rights Assignment](#).

How to Use Well-known Accounts

In this area you will most likely specify either of the following:

- High Mandatory Level
- Low Integrity Level

- Medium Integrity Level
- Medium Plus Integrity Level
- Restricted Code Well Known Group
- System Integrity Level
- Untrusted Mandatory Level

These integrity levels determine who else can use a specific process. Processes launched by a standard user are by default medium integrity. Any process that gets launched via an elevated policy has a high integrity level assigned by default.

Processes need to have level parity to be able to utilize each other. This means, if a process is running at a high integrity level and wants to inject code into another process, it can do so if that other process is running at high, medium, or low integrity levels, but it cannot inject code into system level processes. Processes that run at low integrity levels can be utilized by pretty much any other process, but they cannot reach out to other processes.

New processes are always created with the minimum of the user integrity and file integrity levels. This guarantees that a new process never executes with higher integrity than the executable file.

Example Scenario

In Privilege Manager we can use these Well-known Accounts to set or remove level integrity independent of or in combination with any assigned elevation or blocking policies.

For example, Adobe applications are generally part of elevation policies in an organization. As mentioned before an elevation policy defaults to a high integrity level. Due to Adobe interoperability requirements within their product suites and with processes launched by standard users, it requires medium integrity levels for all Adobe products.

Any elevation policy pertaining to Adobe products, needs an **Adjust Process Rights Action** that sets the **Well-known Accounts** setting to **Medium Integrity Level**.

Additional Options Explained

Under Additional Options customers can select to **Use User's Unrestricted Token** and **Disallow changes to the process rights after applying changes**.

The use of the unrestricted token option is another level of available customization beyond what can be enabled or disabled via the Adjust Process Rights Settings. Enabling this token presents the user with extra levels of access rights over the process. If changes to the process rights are disallowed, the user's unrestricted token is valid as long as the pertaining process is running.

For example if you have a standard user policy for a certain process to run at medium integrity level, but you want to enable more rights without fully elevating and granting the process a high integrity level, you can use the unrestricted access token to fine tune.

Enabling Unrestricted Token Use

To set the unrestricted token, follow these steps:

1. Select the action of type **Adjust Process Rights Action** that best fits your specific business need.
2. Create a copy of that action.
3. Select the **Use User's Unrestricted Token** checkbox on the copied action and save the action with a new name (for example "Unrestricted Token - Add Admin Rights").
4. Add the new action to new policies or change existing policies and remove the old action.
5. Add the new action and save the changes.
6. Then update the agent client policies.
7. The ACS agent must retrieve the details of the new action from the server via the ACS web service.
8. The change may take a few minutes to reach the client machine after the client policies have updated depending on how busy the server is.

Adjust Process Right for Resource Monitor

The following image shows the default action. To customize make a copy to change any of the default items.

Action > Adjust Process Rights for Resource Monitor

Details Related Items

Details

Name Adjust Process Rights for Resource Monitor

Description This actions will adjust process rights necessary to run Resource Monitor.

Platform Windows

Adjust Process Rights Settings

i This application action elevates or restricts the permissions and/or privileges held by a process security token. By default each process inherits the user's security token.

Action Type

- Elevate Rights
- Restrict Rights
- Apply Restricted SID (advanced)

Windows Privileges

- Act as part of the operating system • Impersonate a client after authentication
- Create a pagefile • Load and unload device drivers • Replace a process-level token
- Create Global Objects • Change the system time • Take ownership of files or other objects
- Debug programs • Profile system performance • Create a token object
- Bypass traverse checking

Built-in Roles

- Administrators

Well-known Accounts


Additional Options (requires Windows Vista or greater)


- User user's unrestricted token
- Disallow changes to the process rights after applying changes

Related Item - Policy


The following image shows the default related item policy for the above action. To customize make a copy to change any of the default items.

Policy > Client Option - Elevate Resource and Performance Monitoring


 This policy is not enabled. Managed computers won't receive this policy until it is enabled.

 This Policy is used by the Client System Settings. Changes to this policy should be made by choosing Admin / Policies / Client System Settings tab.
Client System Settings

General Conditions **Actions** Policy Enforcement Deployment

Send policy feedback 

Actions to apply to the application


TYPE	ACTION NAME
	Adjust Process Rights for Resource Monitor

Actions to apply to the child applications

Use the same actions as the parent
No actions are currently being applied.

[Back](#) [Edit](#) [Enable](#) [Create a Copy](#) [See Events](#)

This type of action is a specific use-case for older Windows systems (Windows XP and Windows Server 2003). The ActiveX installer action allows or denies an application to enable standard users to install approved ActiveX components. If you don't know what ActiveX means, you won't need to use this type of action.

Details	
Name	* Test ActiveX Installer
Description	Testing ActiveX Installer action
Platform	Windows
 This action is only supported on Windows XP and Windows Server 2003 operating systems.	
ActiveX Installer Settings	
Deny ActiveX Components	View Parameters Select resource...
Elevated Installation	View Parameters Select resource...
Silent Elevated Installation	View Parameters Select resource...

Parameters

The following details can be set on the ActiveX action:

- Deny ActiveX Components, or
- Elevated Installation, or
- Silent Elevated Installation

For those actions for ActiveX, these parameters can be specified:

- Scope by Organization Group
- Search text
- Maximum rows returned
- Resources (use the column filter function to locate a resource and click **Add**)

Action to allow copying of application on macOS systems.

Action > Test Allow Copy Action (MacOS)

Details Related Items Change History

Details

Name	Test Allow Copy Action (MacOS)
Description	
Platform	Mac OS

Settings

Path	
-------------	--

Parameters

The following Allow Copy Action Settings can be specified:

- Path

This type of action will restrict applications from modifying certain items and will enforce standard Windows ACLs when the targeted application accesses restricted files, folders, registry keys, or services on a computer.

Details	Related Items	Change History
Details		
Name	* Test Application Classification Action	
Description	Testing Application Classification action	
Platform	Windows	
Application Classification Settings		
Application Classification	* Classification	

This type of action will allow old applications that must be run via compatibility mode to execute without manual compatibility adjustments.

Details

Name * Test Application Compatibility Fix

Description This action will apply the specified application compatibility fix

Platform Windows

Compatibility Layer Settings

Standard Layer [Select layer...](#)

Custom Layer

Layer Name *

Shims **Flags**

[Add Shim](#)

NAME	PARAMETER
No shims defined	


Parameters

The following Compatibility Layer Settings can be set on the Apply Application Compatibility Fix action:

- Custom vs. Standard Layer, which lets users select a layer either x86 and x64, x86 only, or x64 only.
- Shims
- Flags

This action stops specific application from executing. It is a default action without any configurable settings. It is a read-only item.

Action > Deny Execute

 This item is read-only.

[Details](#) [Related Items](#) [Change History](#)

Details

Name	Deny Execute
Description	This action stops specified applications from executing.
Platform	Windows, Mac OS

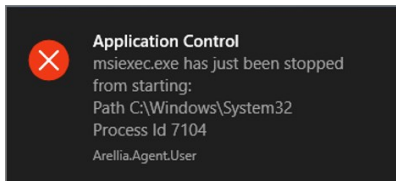
Settings

There are no configurable settings for this item.

[Back](#) [Edit](#) [View as XML](#) [Export](#)

Deny Execute Message

This action displays a message to the user informing that an application has been denied execution. The Deny Execute Action needs to be used with this message.



As the name suggests, this type of action will prevent applications from reading or writing (or both) to certain directories or to certain file types.

Details	
Name	Test Deny File Access Action
Description	Testing Deny File Access action
Platform	Windows
Deny File Access Settings	
Deny Access	<input type="checkbox"/> Deny Read <input type="checkbox"/> Deny Write
Deny File Access Settings	
Path	<input type="text"/>
	<input type="checkbox"/> Include subdirectories
File Extensions	<input type="button" value="+ Add"/> None Selected
MIME Types	<input type="button" value="+ Add"/> None Selected

Parameters

The following Deny File Access Settings can be specified:

- Deny Access to read and/or write operations.
- Path and possibly subdirectory locations.
- Specific file extensions.
- MIME types.

Deny Files Read and Write Access Message

This action displays a message to the user informing that an application will be restricted from certain file access. The Deny Read/Write Access to Microsoft Office Document Files Action needs to be used with this message.

□

This type of action will limit specified applications from interacting in malicious ways with other applications.

Action > Test Deny Windows Hooking Action

Details Related Items Change History

Details

Name Test Deny Windows Hooking Action

Description Testing Deny Windows Hooking action

Platform Windows

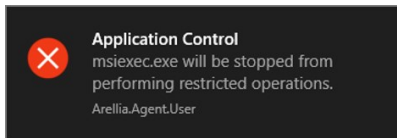
Settings

There are no configurable settings for this item.

This action does not have any configurable parameters.

Windows Hooking Message

The action displays a message to the user informing them that an application will be stopped from interacting with other applications. The Deny Windows Hooking Action should be used with this message.



This type of action will force applications to use Microsoft encryption when saving a file.

Action > Test Encrypt Application Files Action

Details Related Items Change History

Details

Name	Test Encrypt Application Files Action
Description	Testing Encrypt Application Files action
Platform	Windows

Encrypt File Settings

Path Include subdirectories

File Extensions

MIME Types

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [View as XML](#) [Export](#)

Parameters

The following Encrypt Application Files Settings can be specified:

- Path and the option to include subdirectories.
- File Extensions.
- MIME Types.

This type of action will execute another application and (optionally) wait on that process to complete before the original process can execute.

Action > Test Execute Application Action

Details Related Items Change History

Details

Name	Test Execute Application Action
Description	This action will execute the specified application.
Platform	Windows

Executable Application Settings

Executable	
Command Line	
<input type="checkbox"/> Wait for executable to complete before allowing process to run	
<input type="checkbox"/> Terminate process if exit code: <input type="text"/> is returned from this executable	

Parameters

The following Execute Application Settings can be specified:

- an executable
- command line arguments

This type of action will limit the environments in which certain code can execute. The sandbox runs a process in a job object that limits its ability to interact with other processes, as well as limiting some specific types of interactions with the operating system.

Action > Test Sandbox Action

Details Related Items Change History

Details

Name	Test Sandbox Action
Description	Testing Sandbox action
Platform	Windows

Settings

Restrictions

- Limit Desktop
- Limit Global Atoms
- Limit Display Settings
- Limit System Parameters
- Limit Write Clipboard
- Limit Handles
- Limit Exit Windows
- Limit Read Clipboard

This type of action sets an environment variable for processes that could change the behavior of an application, or be caught by an Environment Variable filter in another policy.

Action > Test Set Environment Variable Action

Details Related Items Change History

Details

Name	Test Set Environment Variable Action
Description	This action will set the specified environment variable.
Platform	Windows

Environment Variable Settings

Name	<input type="text"/>
Value	<input type="text"/>

Parameters

The parameters for the Set Environment Variable action are setting the name and value of the environment variable.

Adjusting Process Security allows a process to be protected from most tampering by users. For example, adjusting process security can restrict who can stop a process from the task manager.


Action > Test Set Process Security Descriptor

Details Related Items Change History

Details

Name	Test Set Process Security Descriptor
Description	This action will apply the specified security descriptor to the process
Platform	Windows

Process Security Details

 Alters the process security using the specified Security Descriptor

Process Security Descriptor

Parameters

The parameters for the Set Process Security Descriptor action are done via resource selection from a list of available security descriptors.

This topic describes the out-of-the-box actions that are available in Privilege Manager and can be used to make your policy configuration process easy.

Actions Catalog

Here is the complete list of Actions that come with Privilege Manager out-of-the-box, according to category type:

Adjust Effective Process Rights Action

Run as Root	Adjust the process rights of the application to run as the root user (MacOS)
--------------------	--

Adjust Process Rights Action

Add Administrative Rights	This action adds basic administrative rights needed to install and run specified applications
Add Administrator Rights – Unrestricted	This action adds administrative rights at a higher integrity level for specified applications. Usually you will only need to use this type of action if an application or installer needs to create a global object, such as a service, or if system changes require unrestricted administrator rights
Remove Administrator Rights	This action removes administrative rights for specified applications
Remove Advanced Privileges Action	This action removes advanced privileges for specified applications from the process token

Allow Copy Action

Allow Copy to/Applications/Directory	This action is used by policies that allow users to run the package installer elevated
---	--

Application Verifier Action

Application Compatibility Testing	This action triggers application compatibility testing while the process runs and sends the results to the server
--	---

Apply SVS Layer Action

Workspace Virtualization Global Layer	This action places specified applications in a common Workspace Virtualization global layer
Workspace Virtualization Isolation Layer	This action places specified applications in a common Workspace Virtualization isolation layer

Advanced Message (Windows)

Application Denied Message Action	This action will display a modal denial notification message to the user and prevent application execution on Windows
Application Denied Notification Action	This action will display a notification to the user that the process has been denied by a policy. The notification window will fade in and out and automatically close after a period of time
Approval Request Form Action	This action will display an approval request form for approval before allowing application to run
Authenticated Justification Message Action	This action will display a customized message to the user, allowing for feedback and requiring authentication before running an application
Group Member Authenticated Message Action	This action will display a customized message to the user and requires authentication by a member of the specified group if the end-user is not a member
Justify Application Elevation Action	This action will display a justification prompt to the user before continuing to the process controlled by a policy
Justify Application Message Action	This action will display a justification prompt to the user before continuing to the process controlled by a policy

De-elevate Child Processes

De-elevate Child Processes	Ensures that all child processes are created without administrator rights. Forces all new processes created by the targeted application to be launched by a de-elevated token.
-----------------------------------	--

Deny Actions

Deny Execute	This action stops specified applications from executing
Deny Read/Write Access to Microsoft Office Document Files	This action can be used to deny read and write access to Microsoft Office documents
Deny Windows Hooking	This action limits specified applications from interacting in malicious ways with other applications

Deny Write Access to Executable Files	This action can be used to deny write access to common executable files
--	---

Display Advanced Message Actions

Application Approval Request Message Action	Application Approval Request Message Action for Mac OS
Application Justification Message Action	Application Justification Message Action for Mac OS
Application Denied Message Action	This action will display a modal denial notification message to the user and prevent application execution on MacOS
Application Warning Message Action	Application Warning Message Action for Mac OS

Display User Message - Basic

Deny Execute Message	This action displays a message to the user informing them that an application has been denied execution
Deny Files Read and Write Access Message	This action displays a message to the user informing them that an application will be restricted from certain file access
Limit Process Rights for New Applications Message	This action displays a message to the user informing them that an application has had its rights reduced
Quarantine Message	This action displays a message to the user informing them that an application has been quarantined
Remove Rights Message	This action displays a message to the user informing them of an associated action
SWV Global Layer User Message	This action displays a message to the user informing them that an application has been placed in SWV global layer
SWV Isolation Layer User Message	This action displays a message to the user informing them that an application has been placed in SWV isolation layer
Windows Hooking Message	This action displays a message to the user informing them that an application will be stopped from interacting with other applications

Encrypt Application Files

Encrypt Microsoft Office Documents	This action can be used to automatically encrypt common application documents using Windows EFS
---	---

Execute Application Action

Immediate File Inventory	This action will inventory the file being executed
---------------------------------	--

Enable UAC Virtualization

Enable UAC Virtualization	This action will turn on UAC virtualization for the target process.
----------------------------------	---

Meter Application Action

Meter Application Usage	This action meters the usage of the specified applications
--------------------------------	--

Quarantine File Action

File Quarantine	This action can be used to quarantine a file by moving it to the default agent quarantine path
------------------------	--

Restrict File Dialogs

Restrict File Dialogs	This action prevents users from abusing the elevated rights of the application via the file open and save dialogs. This is a recommended action that customers should add to their elevation policies.
------------------------------	--

Set Environment Variable Action

Suppress User Account Control Consent Dialog	This action will prevent the UAC consent dialog from being displayed
---	--

Set Process Security Descriptor

Locked down Service Process Security Descriptor This action applies a restrictive security descriptor disallowing Administrators the right to terminate the process

Application Control requires many operational tasks. Those can be creating reports and emailing them, modifying policies, filters, actions, task parameters, and schedules.

In this section the following topics are covered:

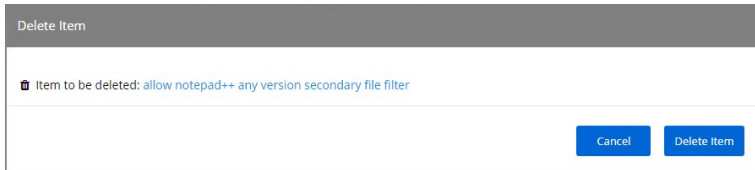
- [Deleting Items](#)

When deleting items there might be dependencies, like a filter is used in a policy. If that filter is then deleted without modifying or also deleting the policy, the policy will stop working without anyone realizing that the filter has been deleted.

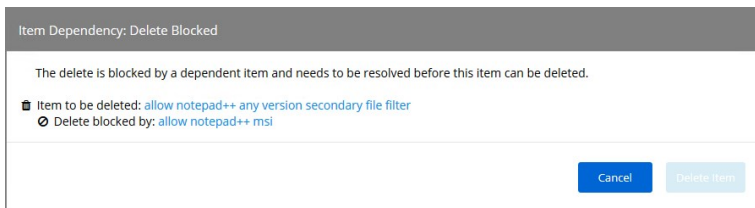
Privilege Manager detects dependencies when items are deleted and alerts the user to

- any dependent items, which block the deletion.
- any child items, which will also be deleted.

When a the **Delete** button is clicked on a filter, in this example the filter is called **allow notepad++ any version secondary file filter** and no dependencies are detected, a **Delete Item** modal opens. The user can proceed by clicking the **Delete Item** button.

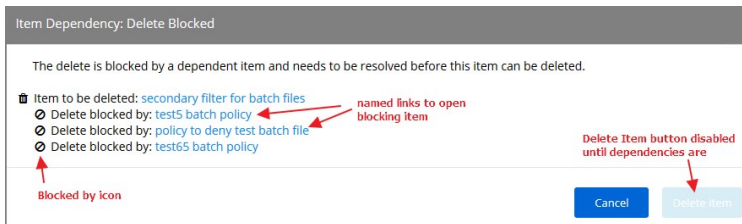


If that filter is part of a policy and the **Delete** button is clicked, the **Item Dependency: Delete Blocked** modal opens.

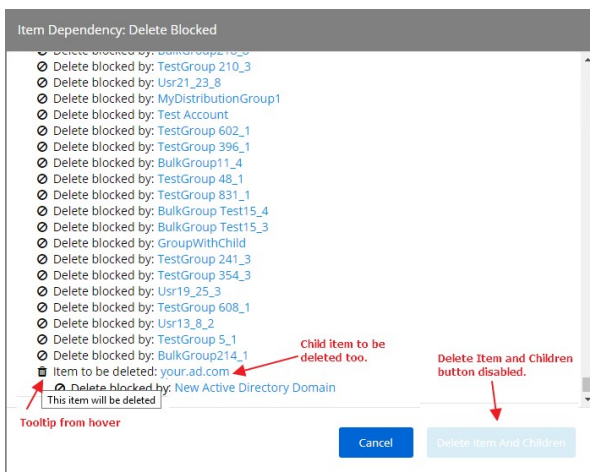


From the modal the user can see that the delete is blocked by a dependent item. A tool tip is shown when hovering the mouse pointer over the icons.

The trash can icon informs about which item was selected to be deleted. The blocked icon informs which items are blocking the deletion.



While there are blocking items, the **Delete Item** or **Delete Item and Children** buttons are disabled. The delete button is dynamic and will only display **Delete Item and Children** if both of those are dependencies, otherwise it will only display **Delete Item**.



Blocking dependent items can be accessed and deleted by clicking on the named item link. This opens the dependent item in another browser tab, where it can be viewed and deleted.

Tasks

In Privilege Manager tasks are activities that can be run on demand or regularly scheduled. If they are regularly scheduled, the schedule triggers the execution of a task instance, which performs specific actions based on set parameters.

Remote Scheduled Client Command type tasks that are considered agent-side require policies to be applied on the agent endpoints, the ones that are considered server-side do not require policies to be executed.

Tasks are set-up via **Admin I More** and then selecting the Tasks link. They are categorized as following:

- [Client Tasks](#)
- [Server Tasks](#)
- [HelpDesk Tasks](#)
- [Infrastructure Scheduled Activities](#)

The following general task topics are available:

- [Agent Hardening](#)
- [Maintenance tasks details](#)
- [Other tasks to schedule](#)
 - [Emailing Reports](#)
- [Reset Licensing](#)
- [Tasks Launching Executables without User Context](#)

Client Tasks are used to run or schedule activities at the endpoints, like:

- Basic Inventory, which triggers the agent to immediately report basic inventory back to the server. The information can be viewed for a computer under Known Data. Data sets are different based on endpoint operating system.
- Resource Discovery Client Task, which populates agent-side data for any resources that have been discovered but lack detailed information.
- Update Applicable Policies, which triggers policy updates at the endpoints.

Note: All default enabled client tasks are **read-only items** and if any customization to the schedule is required, create a copy to add, save, and apply changes. Schedule changes can be added on the Triggers page when clicking the existing schedule and then **Show Advanced**.

Details for each task are provided under the following topics:

- [Basic Inventory](#)
- [Cleanup Agent Inventory Transfer](#)
- [COM Inventory Policy](#)
- [Cleanup Sent Privilege Manager Event](#)
- [Configure PM Remove Programs](#)
- [Default File Inventory Policy](#)
- [Ensure UAC Override Setting](#)
- [Local User Inventory Policy](#)
- [Perform Resource Discovery](#)
- [Retry Errored TMS Events](#)
- [Set Agent Log Size](#)
- [Scheduled Check for Pending Tasks](#)
- [Shared Folder Inventory Policy](#)
- [Scheduled Registration](#)
- [Update Agent Commands](#)
- [Update Applicable Policies](#)
- [User Logon Inventory Policy](#)
- [Update Provisioned Resource Client Items](#)
- [Windows Server Inventory Policy](#)

Basic Inventory (Initial, Windows) and (Initial, Mac OS) are scheduled to run at a client's initial start-up after the agent is installed. The cause of the policy's trigger is the task creation.

The common Basic Inventory is scheduled to run daily at 8 am.

For Windows systems the policies instruct the agent on the client system to report the following WMI classes to the server:

- Win32_ComputerSystem,
- Win32_ComputerSystemProduct
- Win32_OperatingSystem WMI

Basic Inventory (Initial, Windows)

Default Active	Yes
Command	Perform WMI Basic Inventory (Windows)
Parameters	WMI classes: ROOT\CIMV2:WIN32_ComputerSystemProduct, ROOT\CIMV2:Win32_ComputerSystem, ROOT\CIMV2:Win32_OperatingSystem
Triggers	Daily at 10:00:00 AM Upon task creation/modification
Targets	All Windows Managed Computers - No Basic Inventory (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	250 KB
Agent Received Size	n/a
Restrictions	none

Basic Inventory (Windows)

Default Active	Yes
Command	Perform WMI Basic Inventory (Windows)
Parameters	WMI classes: ROOT\CIMV2:WIN32_ComputerSystemProduct, ROOT\CIMV2:Win32_ComputerSystem, ROOT\CIMV2:Win32_OperatingSystem
Triggers	Daily at 8:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (Initial, Mac OS)

Default Active	Yes
Command	Perform Basic Inventory (MacOS)
Triggers	Daily at 10:00:00 AM

	Upon task creation/modification
Targets	All MacOS Managed Computers - No Basic Inventory (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Basic Inventory (Mac OS)

Default Active	Yes
Command	Perform Basic Inventory (MacOS)
Triggers	Daily at 10:00:00 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 5 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	

Completes and cleans BITS transfers and temporary files used by the TMS Agent Inventory Helper.

Cleanup Agent Inventory Transfers (Windows)

Default Active	Yes
Command	Cleanup Agent Inventory Transfers
Triggers	Daily at 2:00:02 AM
Targets	All Windows Computers with Application Control Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of failed file transfers
Agent Received Size	n/a
Restrictions	none

Purges Agent events that have been successfully transmitted from managed endpoints to reclaim disk space.

Cleanup sent Privilege Manager Events (Windows)

Default Active	Yes
Command	Remove sent TMS Client Events (Windows)
Triggers	Daily at 2:00:02 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

Cleanup sent Privilege Manager Events (Mac OS)

Default Active	Yes
Command	Remove sent TMS Client Events (MacOS)
Triggers	Daily at 2:30:02 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 30 minutes.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

The purpose of this policy is to inventory COM+ and DCOM packages installed on the client. The inventory of these package

COM+ (Component Object Model) and DCOM (Distributed Component Object Model) utilize RPC calls for component communication and access to the object's methods and data. Running an inventory on those packages on a client is beneficial, if apps using those packages require elevation or should be denied.

Default Active	No
Command	Local Security COM Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of COM+ and DCOM packages
Agent Received Size	n/a
Restrictions	none

Configure the [Privilege Manager Remove Programs](#) behavior.

For standard users the utility by default,

- adds all programs to the Control Panel.
- hides repair options for all installers.
- shows the blocked installer list.
- prevents Thycotic software from being uninstalled.

Default Active	Yes
Command	Configure Remove Programs Application
Parameters	selected: Add to Control Panel, Hide Repair for All Installers, Show Blocked Installers in List, Vendor software that can't be Uninstalled: Thycotic.
Triggers	Daily at 10:00:00 PM (repeating every 2 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

The purpose of this policy is to inventory software programs running on the managed computer.

These policies use their respective OS based File Specification filters, which in turn have a set of optional additional filters to identify the programs to be inventoried.

Default File Inventory Policy (Windows)

Default Active	Yes
Command	File Inventory Command
Parameters	Default File Specification (Windows)
Triggers	Weekly on Sun at 3:00:00 AM
Targets	All Windows Computers with File Inventory Agent Installed (Target)
Conditions	Idle: None specified by default Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of programs to inventory
Agent Received Size	n/a
Restrictions	none

Default File Inventory Policy (MacOS)

Default Active	Yes
Command	File Inventory Command
Parameters	Default File Specification (MacOS), Default App Bundles File Specification Filter
Triggers	Weekly on Sun at 3:00:00 AM
Targets	All Mac OS Computers with File Inventory Agent Installed (Target)
Conditions	Idle: None specified by default Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of programs to inventory
Agent Received Size	n/a
Restrictions	none

Ensures that the UAC Override Registry Key is set.

Default Active	Yes
Command	Ensure UAC Override Registry Key
Parameters	Default File Specification (Windows)
Triggers	Daily at 12:00:00 AM
	At startup
Targets	All Windows Computers with Application Control Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
	Stop the task if it run for longer than 15 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

The purpose of this policy is to inventory Local User accounts, groups and group membership on the client. This policy can also be used to inventory specific account privileges.

Local User Inventory Policy

Default Active	Yes
Command	Local Security Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of users and groups
Agent Received Size	n/a
Restrictions	GPO - Audit Account Management enabled does not use Security Event Log

Local User Inventory Policy (MacOS)

Default Active	Yes
Command	Local Security Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s) - not set by default.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of users and groups
Agent Received Size	n/a
Restrictions	none

Schedule on which agents check with server to determine, if any local resources require discovery.

After any type of resource discovery, it might be possible that the server does not have all the details required to correctly identify what was initially provided by the agent. The agent periodically checks in with the server, if any additional information needs to be discovered. The sever then sends information back to the agent about any pending item clarifications.

Perform Resource Discovery (Windows)

Default Active	Yes
Command	Resource Discovery Command
Triggers	Daily at 12:00:00 AM (repeating every 4 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour.
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on server request
Agent Received Size	depends on request volume and the number of items pending on server for clarification
Restrictions	none

Perform Resource Discovery (Mac OS)

Default Active	Yes
Command	Resource Discovery Command
Triggers	Daily at 3:00:00 AM (repeating every 4 hours for a duration of 24 hours)
	Upon task creation/modification
Targets	MacOS Computers
Conditions	Idle: None specified by default Power: Start the task only if the computer is on AC power, Stop if the computer switches to battery power
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 3 day(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on server request
Agent Received Size	depends on request volume and the number of items pending on server for clarification
Restrictions	none

Scan Agent queue for any events that require retransmission.

Retry errored TMS Events (Windows)

Default Active	Yes
Command	Retry errored TMS Client Events (Windows)
Parameters	Force Resending (incl. transient errors)
Triggers	Daily at 2:00:02 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of items that require retransmission
Agent Received Size	n/a
Restrictions	none

Retry errored TMS Events (Mac OS)

Default Active	Yes
Command	Retry errored TMS Client Events (MacOS)
Triggers	Daily at 2:00:02 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 1 hour(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of items that require retransmission
Agent Received Size	n/a
Restrictions	none

Scheduled Check Pending Client Tasks - Internet Clients (Windows)

Initiate a check for pending client tasks. Used by agents that are unable to receive an incoming connection from the server.

Default Active	Yes
Command	Check Pending TMSClient Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	depends on number of pending items
Restrictions	none

Scheduled Registration (Windows)

Initiate agent registration with server.

Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	none

Scheduled Registration - Internet Clients (Windows)

Initiate agent registration with server less frequently than internal clients.

Default Active	Yes
Command	Check Pending TMS Client Tasks
Triggers	Daily at 2:00:00 AM (repeating every 4 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	none

Scheduled Registration (Mac OS)

When this policy is triggered the Agent will attempt (or re-attempt) to register with the server.

Default Active	Yes
Command	Start TMS Registration
Triggers	Daily at 2:00:00 AM (repeating every 1 hour for a duration of 24 hours)
Targets	All MacOS Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed

(stop)	Stop the task if it run for longer than 5 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	5 KB
Agent Received Size	n/a
Restrictions	none

Configures the size of the Agent Event Log. By default this is set to 1 MB. For most environments it is recommended to increase the Agent Event Log size. This task can be used to override the default setting.

Default Active	No
Command	Set Agent Log Size (Windows)
Parameters	Log Size: 20 MB
Triggers	Daily at 6:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	n/a
Agent Received Size	n/a
Restrictions	none

The purpose of this policy is to inventory shared folders on the client.

Default Active	No
Command	Local Security Shared Folder Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of shared folders on the endpoint
Agent Received Size	n/a
Restrictions	none

Task sends up request for hashes of specific client item types. With Privilege Manager version 10.7 and up returned items are filters based on the last time run the task ran.

Update Agent Commands (Windows)

Instructs Agent to update any agent commands if required.

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Agent Command
Triggers	Daily at 12:00:00 AM
Targets	Windows Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	none

Update Agent Commands (Mac OS)

When this policy is triggered the Agent will update agent command items.

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Agent Command
Triggers	Daily at 12:00:00 AM
Targets	MacOS Computers
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	depends on the number of updated commands
Restrictions	none

Update Applicable Policies (Windows)

Instructs Agent to check with server for policy changes.

Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 30 minutes for a duration of 24 hours)
Targets	All Windows Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	none

Update Applicable Policies - Internet Clients (Windows)

Instructs Agent to check with server for policy changes less frequently than internal clients.

Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 2 hours for a duration of 24 hours)
Targets	All Windows Managed Computers - Internet Client (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	
Restrictions	none

Update Applicable Policies (Mac OS)

When this policy is triggered the Agent will check the server for updated policies.

Default Active	Yes
Command	Update Applicable Policies
Triggers	Daily at 12:00:00 AM (repeating every 30 minutes for a duration of 24 hours)
Targets	All MacOS Managed Computers - Internal Network (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed

(stop)	Stop the task if it run for longer than 10 minute(s).
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	
Agent Received Size	depends on the number of updated policies
Restrictions	none

These policies trigger the Agent to force a Client Item Update for provisioned resources on the specific client system.

Update Provisioned Resource Client Items (Windows)

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Provisioned Resource
Triggers	Daily at 8:00:00 AM starting Sun Apr 07 2013
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on the number of provisioned items
Agent Received Size	n/a
Restrictions	none

Update Provisioned Resource Client Items (MacOS)

Default Active	Yes
Command	Force Client Item Update Command
Parameters	Category: Provisioned Resource
Triggers	Daily at 8:00:00 AM starting Sun Apr 07 2013
Targets	All MacOS Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on the number of provisioned items
Agent Received Size	n/a
Restrictions	none

Updates user logon data based on a given schedule to provide primary user information.

Default Active	Yes
Command	Windows Logon Event Processor
Triggers	Weekly on Sun at 2:00:00 AM
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it run for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of user sessions
Agent Received Size	n/a
Restrictions	none

The purpose of this policy is to inventory Windows Services on the client.

Default Active	Yes
Command	Local Security Service Inventory Command
Triggers	Weekly on Sun at 2:00:00 AM
	Upon task creation/modification
Targets	All Windows Computers with Local Security Agent Installed (Target)
Conditions	None specified by default
Advanced	Allow task to be run on demand
(missed)	Run task as soon as possible after a scheduled start is missed
(stop)	Stop the task if it ran for longer than 0 minute(s). - not set by default
(retry on failure)	not set by default
Rule	Default (Do not start a new instance)
Agent Sent Size	depends on number of installed windows services
Agent Received Size	n/a
Restrictions	none

Component Based List of Default Tasks

Application Control	Get Security Rating for File	Get/update the security rating for the given file.
	Get Security Ratings for Files	Get/update the security ratings for the given files.
	Refresh Security Rating Reports	Refreshes old security rating reports for resources rated by the given provider.
Application Control Cylance		
Directory Services	Default Import AzureAD Users/Groups	Run this task to import/update Azure AD users and groups.
	Default Import Directory	Run this task to import/update directory OUs, users, and containers.
	Default Import Directory Computers	Run this task to import/update directory computer resources.
	Default Import Directory Sites	Run this task to import/update directory sites.
	Import Specific Azure AD Users and Groups	Import specific users and groups from Azure Active Directory.
	Merge Duplicate Account SID Resources	Run this task to merge resources that have a duplicate account SID.
	Synchronize Organizational Unit Server Task	Synchronize Organizational Unit Server Task.
	Update OU Directory Scope Collections Membership	This task updates the membership of Directory Services OU scope collections.
	Update OU Directory Scope Collections Membership 2	This task updates the membership of Directory Services OU scope collections.
Email Tasks	Send Gauge Summary E-mail Task	Send a specific report on a schedule.
File Inventory	Inventory File	Run this task to collect detailed information on the selected file for reports, filters, etc.
	Inventory File Resource	Run this task to update information on an existing file resource for reports, filters, etc.
	Inventory Package	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Package with Exclusions	Run this task to scan the contents of a package and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages	Run this task to scan the contents of a list of packages and report detailed information on files it contains for reports, filters, etc.
	Inventory Packages Referenced in Whitelists	Run this task to collect detailed information for files contained in packages referenced in one or more whitelists.
	Inventory Uploaded File	This task is used internally to collect detailed information from files uploaded remotely to the server. It is visible only for status information and troubleshooting.
Foreign Systems		
	SCCM	Tasks here let you synchronize users, computers, and specific SCCM collection.
	ServiceNow	Creates ServiceNow Approval Request items.
	Symantec Management Platform	Tasks here let you synchronize SMP collections and package(s).
	Syslog	Creates tasks to send events to the configured syslog server based on specific templates.
Local Security	Update Primary User	Updates the primary user for the given computer resource.
	Update Primary User for Collection	Updates the primary user for each computer in the given collection.
Thycotic One Users	Sync users with Thycotic One	Run this task to synchronize PM users with a Thycotic One instance.
Security	Rebuild Item Security Cache	Run this task to mark all entries in the item security cache as invalid, forcing a rebuild.
	Refresh Agent Secrets	Run this task to refresh the agent secrets that were generated before the given max age.
	Revoke Agent Secrets	Run this task to revoke the secrets from one or more agents.
	Revoke Secrets from All Agents	Run this task to revoke the secrets from all agents.
	Set Security Rating	Run this task to manually set the security rating (used in filters) for the selected files.
	Update Security Ratings for Resource	Run this task to update the security ratings (used in filters) for the given resources using the given rating system.
Utility	Delete Item	This task will delete an item, and optionally dependent children.
	Update Server Gauge State	This task will update the state of a server gauge.

By default this folder is empty. Administrators can use it to copy tasks for HelpDesk users to run them. The HelpDesk folder provides security settings on those folders that would grant permissions if someone puts tasks in that area.

These are tasks that pertain to either core functions or to components and subcomponents of Privilege Manager.

Core, no folder at root level	Client Items Update OBSOLETE WITH v 10.7 and higher	Updates client items required by agents.
	Collection and Resource Targeting Update	Updates collections and resource targets.
	Collection Update	Update collections.
	Import Local Group Policy Definitions	Loads Group Policy Definitions from the local machine.
	Import Secret Server Licenses	A scheduled import of licenses from Secret Server.
	Licensing Update	Updates licensing product counts.
	Resource Discovery	Run this task to populate data for resources that have been discovered but lack detailed information.
	Resource Target Update	Use this task to updates resource targeting.
Application Control		
App Control Cylance	Refresh Cylance Security Rating Report	Refreshes Cylance security rating reports on a schedule.
App Control VirusTotal	Recalculate Ratings for VirusTotal Provider	Recalculates security rating levels for resource rated by the given provider.
	Refresh VirusTotal Security Rating Reports	Refreshes VirusTotal security rating reports on a schedule.
Approval	ServiceNow Approval	Initiates a ServiceNow approval process and waits for the result.
Configuration	Reconfigure for System Secret Vault Change	This task is run by the system when the configured system secret vault setting has changed.
Data Feed	Content Tasks	Download Data Feed Entry - Download Data Feed Entity.
		Import Data Feed Entry - Imports data feed entities and their corresponding data feeds, primarily designed to be used by the Setup component.
		Import Product Configuration Package - Download Data Feed Entity.
	Update Tasks	Clear Data Feed Entity Updated - Clear Data Feed Entity.
		Update Data Feed - Updates the Privilege Manager Configuration Feed List
		Update TMS Configuration List Data Feed - Updates the Privilege Manager Configuration Feed List.
Directory Services	Active Directory Merge Computers	Merges computers created by Directory Services.
	Active Directory Merge Single Computer	Merges a single computer during agent registration. Needed if AD Sync has occurred before agent registration.
	Import Secret Server Domains	A scheduled import of AD domains from Secret Server.
	OU Directory Scope Collection Update	This task updates the membership of Directory Services OU scope collections.
	Promote Windows Domains	Promotes any Windows domains to Active Directory domains.
	Update Active Directory Details	Updates Active directory domain details including domain controllers.
File Inventory	Update File Filter Security Catalogs	Updates security catalogs associated with File Collection Security Catalog Filter items.
Import Activities	Import Packages	Imports multiple product packages, data feed entries and performs initial configuration, primarily designed to be used by the Setup component.
	Import Packages v3	Imports multiple product packages, data feed entries and performs initial configuration, primarily designed to be used by the Setup component.
	Install Products V4	This task installs product NuGet packages.
	Install Products V4 (Server Nodes)	This task is used to upgrade binaries for additional server nodes.
	Install Products V5	This task installs product NuGet packages.
	Install Products V5 (Server Nodes)	This task is used to upgrade binaries for additional server nodes.
Local Security	Primary User Update	Updates the primary user for each computer in the given collection.
	User Credentials Data Update	This task ensures that resource credentials match the source user data.
Maintenance Tasks	Assign Orphaned Agent Uploads	This task assigns agent event uploads that have been orphaned.
	Delete Old Performance Counter Events	This task deletes internal performance counter events last updated before the specified time.
	Purge Maintenance - Agent Logs	This server task removes all Agent Log data that is older than the time period specified.

	Purge Maintenance - Application Control Events	Purges the selected Application Control Event types from the database based on the time range specified.
	Purge Maintenance - Audit Events	This task removes audit event records older than the specified time period.
	Purge Maintenance - Completed File Upload Sessions	This task removes completed file upload sessions older than the specified time period.
	Purge Maintenance - Files Undiscovered	Run this task to delete file resources which have not been discovered by File Inventory, and no agent can be identified to collect information for the files.
	Purge Maintenance - Incomplete File Upload Sessions	This task removes incomplete file upload sessions older than the specified time period.
	Purge Maintenance - Message History	This server task removes all Message History data that is older than the number of seconds/minutes/hours/days/weeks specified. Message History data tracks all events received by the Privilege Manager Server and is used for information purposes.
	Purge Old Computers	Remove old computers and gauge data for those old computers.
Monitoring	Check for Available Product Updates	Checks the configured <code>nuget:source:SolutionCentre</code> for available product updates.

In addition to maintenance tasks, there are other tasks that should be scheduled to run regularly by Privilege Manager administrators. It's recommended to run these tasks to determine how long they take to complete in each environment, then schedule appropriately to cover task completion and needs.

AD Import and Synchronization Tasks

Import Active Directory users and groups on demand and based on a set schedule.

Note: Depending on AD structure and size, the tasks should be planned to avoid bulk imports and synchronization of too large of a number of accounts.

Task Parameter Conflicts

When task parameters are set at the task level, they can't be changed when a schedule is created for that task. However, in some circumstances, if you have already defined parameters at the task schedule level and then go back to the task to set the values, you may end up with task schedule parameter conflicts. When there are conflicts with the version currently on the server, the Privilege Manager console shows a modal to resolve the existing conflicts before any schedule modifications can be saved.

Schedule Parameter Conflicts

The following schedules for this task have conflicting parameters.
Please review the conflicting parameters and choose if you would like to either
Keep all conflicting parameters on the schedules
Remove all conflicting parameters from the schedules

[New Task Schedule](#)
▲ MaxRows

[Cancel](#) [Keep](#) [Remove](#)

The user can review the task that introduced the conflict by clicking the linked item, which is opened in a new browser tab.

The options to resolve are

- Keep all conflicting parameters on the schedule - click the **Keep** button.
- Remove all conflicting parameter from the schedule - click the **Remove** button.

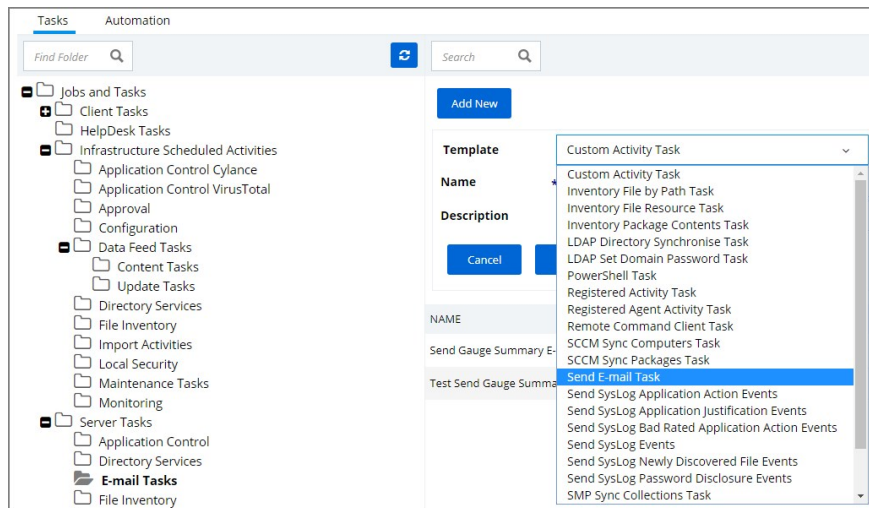
Or cancel if you wish to clean up the conflicts by manually editing task parameters on the conflicting items. However, something indicated as a conflict isn't necessarily a problem. The functionality is implemented so that users have the ability to stop changes on the schedule level by setting something other than default on the task level. If a parameter on the task is a default value, then that parameter will not be in conflict, if it does not match on the schedule.

Whenever there is a deviation from the default value on the task level, even with the parameter on the schedule matching, users are asked to resolve the conflict by keeping the current values.

Any report created in Privilege Manager can be sent to a group of recipients based on a scheduled task.

To set this up, create a new Server task to send emails.

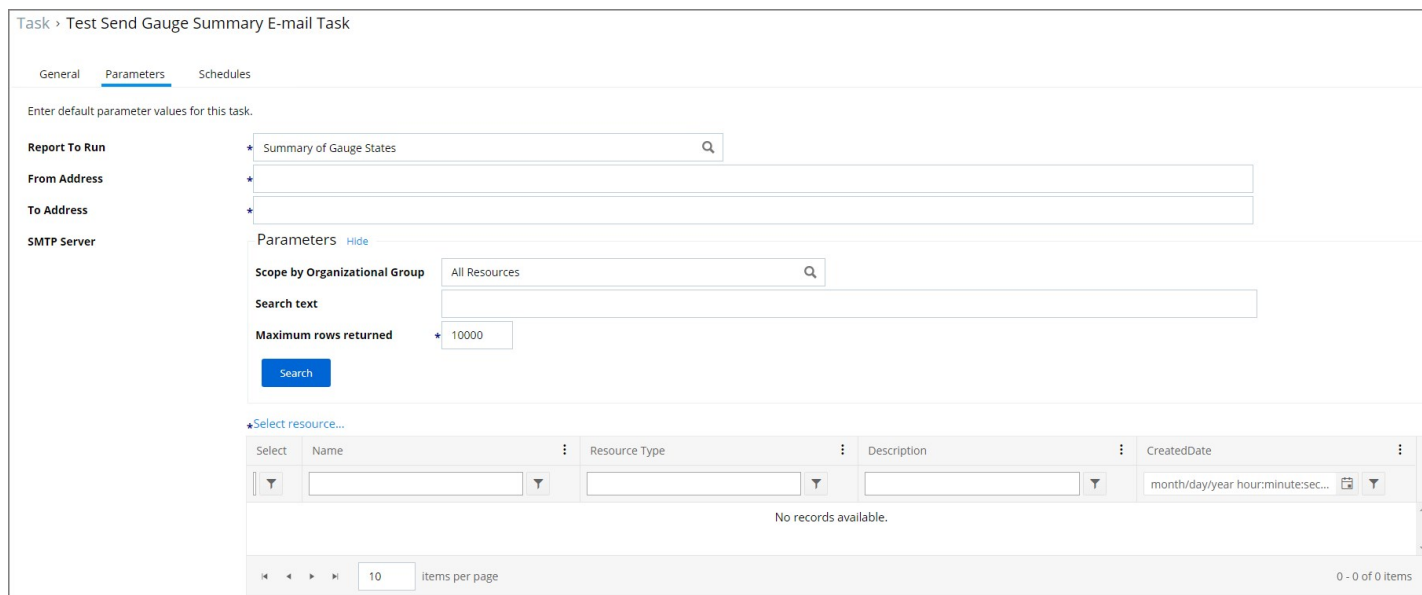
1. Navigate to **ADMIN | Tasks**.
2. In the folder tree open **Server Tasks | E-mail Tasks**.
3. Click **Add New**.



4. From the drop-down select **Send E-mail Task**.
5. Enter the task name and description.
6. For the **SMTP Server**, you can search via Parameters by specifying
 - o Scope by Organizational Group
 - o Search text
 - o Maximum rows returned (default 10000).

Note: This requires a SMTP Server Foreign System set-up.

7. Click **Search**.
8. Click **Select resource...** and select a server from the search results.



9. Click **Create**.
10. Click **Edit**.

11. Go to the Parameters tab.

Task > Test Send Gauge Summary E-mail Task

General Parameters Schedules

Enter default parameter values for this task.

Report To Run * Summary of Gauge States

From Address *

To Address *

SMTP Server [View Parameters](#)
* [Select resource...](#)

SSL Enabled

Note: For cloud environments the SMTP server settings are pulled from an existing configuration and can't be edited via the parameters tab.

1. In the **Report to Run** field enter/search for the report you wish to send.
2. In the **From Address** field enter the sender information you wish to be provided.
3. In the **To Address** field specify the recipient(s) (this can be a comma-separated list of addresses).
4. Select the checkbox for **SSL Enabled**.
5. Click **Save**.
6. Go to the **Schedules** tab.
7. Click **New Schedule**.

Task Schedule > New Task Schedule

Task to run Test Send Gauge Summary E-mail Task

Schedule name * New Task Schedule

Schedule Parameters

At predefined schedule

At date/time

Once

Daily

Weekly

Monthly

[Show Advanced](#)

Starting + 11/2/2019 UTC

Recur every + 1 day(s)

Set up the schedule specifics for this task.

8. Click **Save**.

Tasks Launching Executables

When a task is used to launch executables, but the task does not have an associated user context, the appropriate user token cannot be assigned. This applies to systems with 10.7 and above agents.

A scheduled task launches an executable, which requires elevation, for example running the performance monitor process. That task is then set to run with elevated permissions, however not as a specific user, but rather as a local user group. Such task used in a policy will cause the executable to fail, since a specific user token cannot be associated.

If you don't have a user context to assign to a task for launching an executable, you can use a PowerShell script in combination with the task and policy.

1. Create a PowerShell script to launch the executable.
2. Set the task to launch powershell.exe.
3. Pass in the name of the script.
4. Set the your policy to target that script.

Maintenance

Privilege Manager has many tasks that can be run to ensure that the data in the database is up-to-date and to purge old or unwanted information. This section provides an overview of the maintenance tasks and other schedulable tasks in Privilege Manager.

Determining how often to schedule maintenance tasks depends on the associated items, like events, files, computers, etc. and their build up. These tasks have default **parameters** assigned but are not scheduled to run. Privilege Manager administrators should schedule these tasks based on their needs and system performance.

The primary maintenance tasks that will need to be scheduled to ensure Privilege Manager databases do not grow too excessively are the

- Purge Maintenance - Application Control Events and
- Purge Maintenance - Files Undiscovered tasks and,
- in pre-10.5 systems, the
 - Purge Maintenance - Completed File Upload Sessions and
 - Purge Maintenance - Incomplete File Upload Sessions tasks.

These maintenance tasks can be found at

- **ADMIN | Configuration | General (tab)** or
- **ADMIN | Tasks | Jobs** and
- **Tasks | Infrastructure Scheduled Activities | Maintenance Tasks**

Assign Orphaned Agent Uploads

This task will assign agent event uploads that have been orphaned.

Parameters: Max records [default setting = 2500]

Delete Old Performance Counter Events

This task will delete internal performance counter events last updated before the specified time.

Parameters: Can be set to Seconds, Minutes, Hours, Days, and Weeks. The default is 1 Day.

This maintenance task should be used if [Save Performance Counters](#) is enabled in the general section of the advanced configuration settings.

Initialize Item Change History

This task is run after installs to ensure items with change tracking enabled have initial history entries. This is an automated task to populate initial states of items across updates.

LSS Migration Tasks

For information on the LSS Migration tasks refer to [Migrate Local Security Policies](#).

Purge Agent and Gauge Data for Deleted Computers

This task will delete orphaned data from AgentActivity, AgentRegistration, and GaugeInstanceState.

Notes: This can be helpful to run, to remove unwanted data for computers that have been deleted from Privilege Manager.

Purge Duplicate Computers

Remove duplicate computers.

Notes: When AD sync occurs, Privilege Manager creates a new object in the database for each computer object. When the agent is installed, it references this same object. If the agent is installed before AD sync occurs, there can be 2 different objects in the database for the same machine. This task merges the duplicate objects and is usually only needed when agents are installed before a computer comes in from AD sync.

Purge Maintenance - Agent Logs

This server task will remove all Agent Log data that is older than the time period specified.

Parameters: Can be set to Seconds, Minutes, Hours, Days, and Weeks. The default is 1 Week.

Purge Maintenance - Application Control Events

Purges the selected Application Control Event types from the database either

- manually based on a specified range of time, or
- automatically after reaching a set threshold. Refer to [Maximum Application Event Count](#) time range specified.

Parameters: Event Types to Purge (Application Action Events, Application Justification Events, Application Metering Events, Application Verifier Events). All of these Application Control Events are populated in the various Application Action reports.

Notes: Only Purge Events that belong to specific policies

Purge Application Control Events older than

Notes: Depending on policy settings, Application Control Events can pull a large amount of data into the database. Privilege Manager administrators must setup schedules for this task, as needed, to purge old or excessive data from Application Control policies.

Purge Maintenance - Audit Events

This task will remove audit event records older than the specified time period.

Parameters: Purge events older than [default setting = 30 day(s)]

Notes: The Audit events mainly pertain to and are used in Change History tracking. This task should not need to be scheduled.

Purge Maintenance - Completed File Upload Sessions

This task will remove completed file upload sessions older than the specified time period.

Parameters: Purge completed sessions older than [default setting = 1 day(s)]

Notes: For versions 10.5 and later, the need to run this task should be significantly reduced since they are now cleaned up as file uploads complete.

Purge Maintenance - Files Undiscovered

Run this task to delete file resources which have not been discovered by File Inventory, and no agent can be identified to collect information for the files.

Parameters: Delete Files that have been undiscoverable for longer than [default setting = 1 week(s)]

Notes: This task clears up files with the name "New Loaded Resource" that are older than X days. This can be a helpful task to schedule to remove undiscoverable files from the Event Discovery results (for example, temp files that an installer creates and then deletes).

Purge Maintenance - Incomplete File Upload Sessions

This task will remove incomplete file upload sessions older than the specified time period.

Parameters: Purge incomplete sessions older than [default setting = 2 day(s)]

Notes: For versions 10.5 and later, the need to run this task should be significantly reduced since they are now cleaned up as file uploads complete.

Purge Maintenance - Message History

This server task will remove all Message History data that is older than the time period specified. Message History data tracks all events received by the Privilege Manager Server and is used for informational purposes.

Parameters: Delete Message History older than [default setting = 30 day(s)]

Notes: This task clears the [Ams.Resource].[MessageHistory] table. Use this task to purge that table, if it is excessively large.

Purge Maintenance - Orphaned Local Users and Groups

This task will delete local users and groups that reference a computer as their parent domain (which will block deletes), but are not part of that computers users and groups.

Purge Old Computers

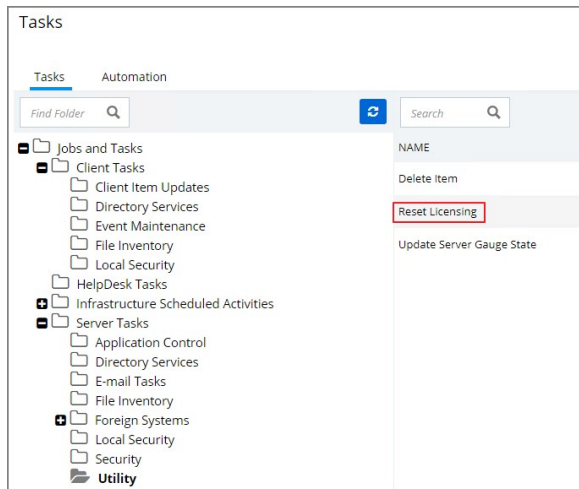
Remove old computers and gauge data for old computers. Remove any agents that have not communicated with the server in a set number of days (default 90), resulting in a critical Agent state.

Reset Licensing

With Privilege Manager 10.7 and up license registrations can be reset. The Reset Licensing task allows upgrading users to remove outdated licenses.

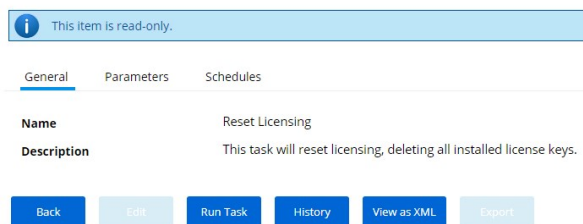
After acknowledging the license reset, all licenses are removed from the Privilege Manager instance. When no licenses can be found, the no product licenses warning banner displays on the top of the console.

1. Navigate to the **Admin | More...** and select **Tasks**.
2. From the Tasks folder tree, select **Server Tasks | Utility**.
3. From the options on the right, select **Reset Licensing**.



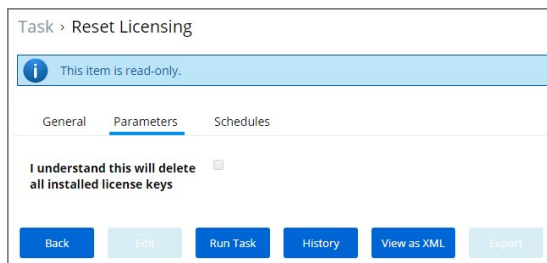
Reset Licensing is a read-only task.

Task > Reset Licensing



However to run it, the user needs to acknowledge the removal of all installed license keys via the Parameters tab.

4. Go to the Parameters tab and select the checkbox **I understand this will delete all installed license keys**.



The task does not run without that acknowledgement and an error is generated.

5. Click **Run Task**

Note: Do not use the scheduling functionality on this task. After a license reset, new licenses should be applied ASAP.

To re-apply licenses refer to the information under [Licensing](#) in the Getting Started section.

Reports

Privilege Manager includes an array of reports. To access reports navigate to the top menu, click the Reports tab for a list of relevant out-of-the-box reports that span a spectrum of system activity and diagnostic information in Privilege Manager.

Click on the name of any of these reports to access details about your system.

Reports

Select Report Options

Actions

- Application Control Event Summary
- Application Justification Summary Details Report
- Summary of Application Actions by Mac Executable
- Summary of Application Actions by Product Name
- Summary of Application Actions by Win32 Executable
- Application Control Event Summary Acknowledgements
- Summary of Application Actions by Computer
- Summary of Application Actions by Operating System
- Summary of Application Actions by Product Version

Agent

- Agent Installation Summary
- Agent Summary by OS
- Managed Operating Systems
- Agent Installations
- Computers Without Agent Installations

Approvals

- Offline Approval Requests
- Summary of Application Approval Requests by Approver
- Summary of Application Approval Requests by User
- Summary of Application Approvals by Date
- Pending Execute Application Approvals
- Summary of Application Approval Requests by Computer
- Summary of Application Approvals and Denials

Detection

- All ActiveX Controls
- All Win32 Executables Report
- Discovered Files not Reported by File Inventory
- Files Pending Agent Discovery with no Discovery Agent
- All Mac OS Executables Report
- Application Verifier Logs
- File Security Rating Details Report

Diagnostic

- Agents missing a policy
- Item Change History
- Product Licenses
- All policies not received by agents
- License Reservations
- Summary of Gauge States

Directory Services

The **Select Report Options** button lets users customize which of the default report options are shown on the landing page.

Users can set the amount of data entries to display per page. The default is 10 rows per report page displayed.

Restore Agent Security Per... CreateFromTemplate Doc-Test-Sys\Administrator 1/23/20, 12:11 PM 686ed5e7-239e-4f27-99f3-9...

10 items per page 1 - 10 of 642 items

Privilege Manager reports can be exported via **CSV** and **PDF** export option buttons.

Reports > Agent Installation Summary

Filter Report Refresh CSV PDF Search

Drag column here for grouping

Computer Name	Last Registered	Application Control ...	File Inventory Agent	OS Name	Service Pack
doc-test-system	1/27/20, 2:59 PM	10.7.2206.48878	10.7.2206.48878	Microsoft Windows Se...	

Once the **CSV** or **PDF** button is clicked, users can choose to

- export the current page or
- export all pages.

Search Items Search HOME TOOLS ADMIN REPORTS

Privilege Manager

Select Export Options

Export Current Page Export All Pages

User Date

Note: Selecting all pages might take some time to complete, depending on the overall size of the data records to export.

Reports and Queries

Each report in Privilege Manager runs a SQL query to return the results. The application does a great job opening the existing queries it uses and generating resolved queries to be used for testing.

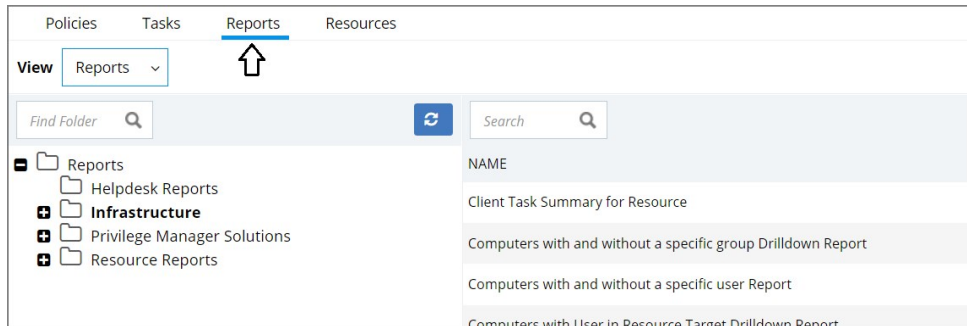
This makes it very easy to run Privilege Manager reports – including custom reports – outside of the application in SQL Server Reporting Services, SQL Server Management Services, or your favorite tool.

This topic gives an overview of finding and using the reports and SQL queries built-in to Privilege Manager.

Most users are probably familiar with the main Reports section of Privilege Manager, which is accessible from the menu at the top of any page. This page includes many common reports. There is a **Select Report Options** button on this page that allows a user to remove reports from this list.

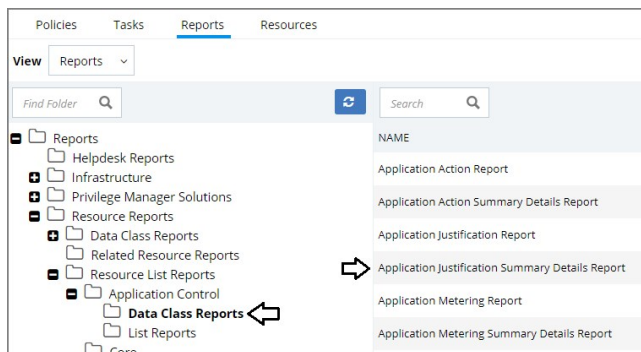
There are many more reports in the product.

To view all the reports in Privilege Manager, navigate to the **ADMIN | Folders | Reports** tab to see all the reports in a folder tree structure.



Expand the folder tree to explore the canned reports.

For example, to access the **Application Justification Summary Details Report**, navigate to **Reports | Resource Reports | Resource List Reports | Application Control | Data Class Reports** and select the **Application Justification Summary Details Report**.



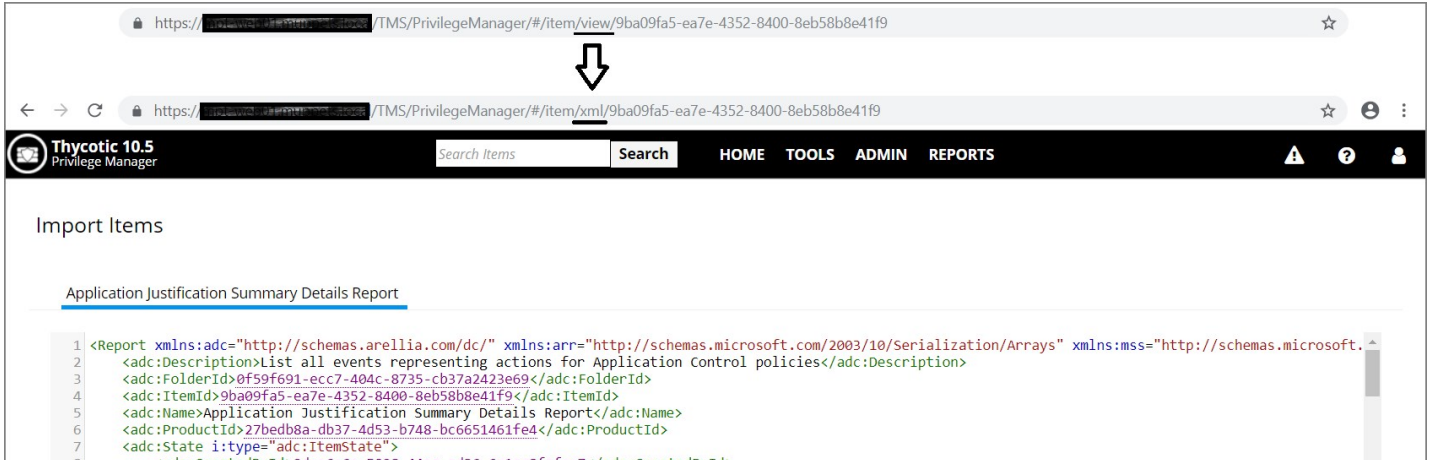
Every report in Privilege Manager is a single XML object and references a separate XML object that contains the SQL query. By viewing the report object's XML, the SQL query object can be determined.

To view the report as an XML object, change the URL from:

[Your_TMS_URL]/PrivilegeManager/#!/item/___view___/9ba09fa5-aa7e-4352-8400-8eb58b8e4119

to:

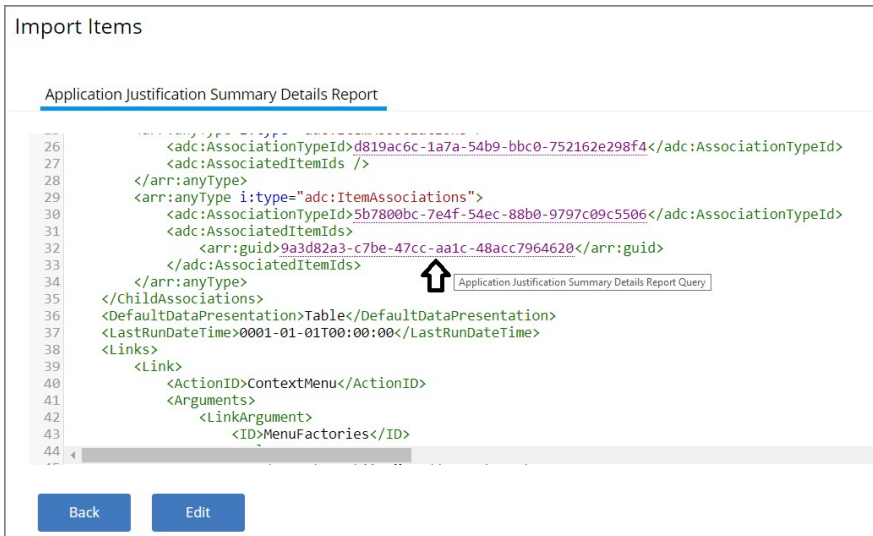
[Your_TMS_URL]/PrivilegeManager/#!/item/___xml___/9ba09fa5-aa7e-4352-8400-8eb58b8e4119



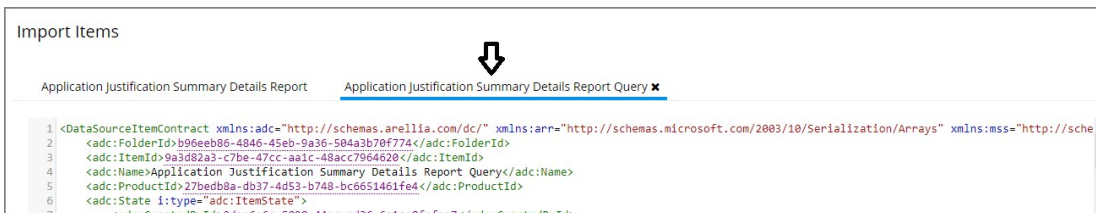
Viewing an item as XML helps in determining what folder it is located in (which will be explained in more detail below). Viewing a report as XML also reveals the XML object for the SQL query.

Use your mouse to hover over the GUIDs in the XML to reveal the name of each GUID's object. Within the section for ChildAssociations, there will be an association for the Report's DataSource. Hovering over the GUID for the AssociatedItem before the Report's DataSource will reveal the report's query.

In the screenshot below, hovering over the GUID is 9a3d82a3-c7be-47cc-aa1c-48acc7964620 identified that item as the **Application Justification Summary Details Report Query**.



Clicking on this GUID will open the XML for the query object in another tab on this same screen:



The XML object for the query includes the direct SQL query that the application runs. However, viewing the query in Privilege Manager will give better query results to work with.

The SQL queries can be viewed in Privilege Manager under **ADMIN | Folders**, but it will be helpful to know the folder in which a specific query is located. In the XML object for query, hover over and click on the GUID for the FolderId.

```

Import Items

Application Justification Summary Details Report  Application Justification Summary Details Report Query x

1 <DataSourceItemContract xmlns:adc="http://schemas.arelia.com/dc/" xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://sche
2 <adc:FolderId>b96eeb86-4846-42eb-9a36-504a3b70f774</adc:FolderId>
3 <adc:ItemId>9a3d82a3-c7be-41a1c-48acc7964620</adc:ItemId>
4 <adc:Name>Application Justification Application Control Bills Report Query</adc:Name>
5 <adc:ProductId>27be0b8a-d875-d875-d748-dc6b514b1fe4</adc:ProductId>
6 </DataSourceItemContract>

```

This will open the XML for the folder in which the query is contained. Click on the FolderId to open the XML for its parent folder, and continue until reaching the root folder – which will not have a FolderId attribute. For the SQL queries, the root folder is Queries.

```

Import Items

Application Justification Summary Details Report  Application Justification Summary Details Report Query x  Application Control x  Report Queries x  Queries x

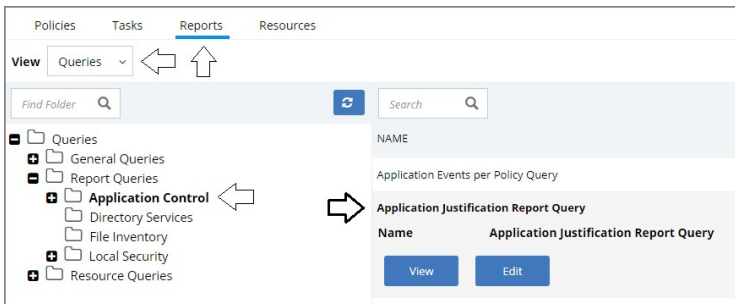
1 <FolderContract xmlns:arr="http://schemas.microsoft.com/2003/10/Serialization/Arrays" xmlns:mss="http://schemas.microsoft.com/2003/10/Serialization/" xmlns:dc="
2 <Attributes>NoModify NoReplication NoDelete NoClone NoExport</Attributes>
3 <DefaultSecuredId>8449e8ae-908b-4205-882b-dc05b57d756</DefaultSecuredId>
4 <ItemId>17969920-3bc4-4a44-89c4-44b62aab01f8</ItemId>
5 <Name>Queries</Name>
6 <ProductId>b409b2ea-d875-4888-9083-ef3c6a26ea52</ProductId>
7 <State>1;Type="FromState">

```

This XML view now shows the full folder location of this specific query: **Queries | Report Queries | Application Control**.

Access the Query from the Folder View

Navigate to **ADMIN | Folders** and select the Reports tab. From the View pull-down, select the Queries View. Then navigate the folder structure determined above: **Queries | Report Queries | Application Control**. Select the Application Justification Report Query from the center pane.

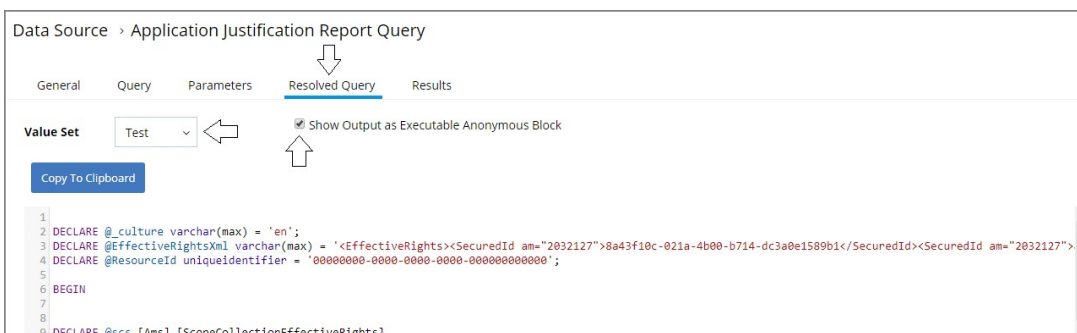


View this query object. The Query tab will show the SQL query that the application runs. This is the same query that appears in the XML of the object.

Obtain a Resolved Query

The Resolved Query tab will give queries that can be used directly on the database to return the similar results that the application receives when it runs the query in the object. This makes it easy to run these queries – or customization of them – in SQL Server Reporting Services.

On the Resolved Query tab, checking the box to **Show Output as Executable Anonymous Block** will assign values to the Parameters the query uses. For the **Value Set** pull-down, select **Test** to assign the Parameters with appropriate values to run this query directly on your database.



Click **Copy To Clipboard** and then paste the resolved query in SSRS, SSMS, or your favorite tool.

Change History Report

Administrators need to be able to look at changes done by other users in Privilege Manager. The need to be able to audit any issue causing changes to configuration settings, policies, filters, and actions. The new **Change History Report** allows Privilege Manager Administrators to track changes and their impact on endpoints.

As part of the audit the following information is recorded:

- User account initiating the change.
- Date/Time of the change.
- Description of the change made.

The following changes are reported:

- Configuration settings to Advanced, Discovery, and Reputation items (new tab on Configuration page)
- Changes to items, like
 - User and Group changes inside Roles
 - Credentials added or existing credentials updated
 - Foreign system added or existing updated
 - Any setting in the Advanced tab
- Changes to conditions of user editable resources.
- Policy, actions, filters, resource target changes, and additions (new tab on policy, actions, filters, resource target pages)
- Editing of task schedules (parameters and schedule of a task) - any change made to the schedule and parameters (New tab on task schedule page for each individual task)
- Imports and Saves of XML - differentiate between import and save

The reporting of any of these changes cannot be turned off and the results can be filtered by categories like Policy, Filter, Action, and Configuration.

Each save creates or adds to the revision history of items. The **Item Change History Report** cannot be used to revert to a previous state.

Reports > Item Change History					
Filter Report Refresh CSV PDF <input type="text" value="Search"/>					
Drag column here for grouping					
Name	Operation	User	Date	Correlation ID	
Test Catch-All Policy	Delete	testing.mydomain.com\ssadmin	11/25/19, 10:08 AM	bf423171-5bf6-4e7d-8	
Test Catch-All Policy	Save	testing.mydomain.com\ssadmin	11/25/19, 9:18 AM	3c54a183-3bb6-47d9-	
Test Catch-All Policy	CreateFromTemplate	testing.mydomain.com\ssadmin	11/25/19, 9:18 AM	bb47a321-139b-4f78-	
Application Entitlements	Save	testing.mydomain.com\ssadmin	11/22/19, 11:32 AM	2bd72239-38f4-4b18-	
Application Entitlements	Save	testing.mydomain.com\ssadmin	11/22/19, 11:02 AM	80952ee3-e7bb-46b3-	
Client Option - Elevate Changing ...	Save	testing.mydomain.com\ssadmin	11/22/19, 10:43 AM	d5d692b3-0009-4394-	
Client Option - Elevate Changing ...	Save	testing.mydomain.com\ssadmin	11/22/19, 10:42 AM	54dd704b-4c76-4b9d-	
New Active-X Group Policy Setting...	Delete	testing.mydomain.com\ssadmin	11/22/19, 8:43 AM	349a7f6f-a740-4eea-9	

Domain Users in Administrator Group

You can get instant reports by clicking the Reports tab. To see which domain users are members of the administrators group, view the domain users as local administrators report.

Local Security

- All Computers with Managed Passwords
- Domain Groups as Local Administrators
- Password Disclosure History
- Summary of Users as Local Administrators

- Disclosure Summary (Local User)
- Local User/Group Summary
- Summary of Domain Users as Local Administrators

Click the Summary of Domain Users as Local Administrators report to view details:

Reports > Summary of Domain Users as Local Administrators

Filter Report
Refresh
CSV
PDF

Drag column here for grouping

Builtin	Account Type	Group Name	User Name	Computers
User Defined	Domain	administrators	krasadmin	1
User Defined	Domain	domain admins	admin	1
User Defined	Domain	domain admins	admin@corp	1
User Defined	Domain	domain admins	anotheradmin	1
User Defined	Domain	domain admins	changepassword	1
User Defined	Domain	domain admins	changepassword1	1
User Defined	Domain	domain admins	test	1
User Defined	Domain	domain admins	test1	1
User Defined	Domain	domain admins	testuser	1
User Defined	Domain	domain admins	jsmith	1

Selecting any of the accounts listed, open the Drilldown report for that specific item:

Reports > Summary of Users as Local Administrators - Drilldown

Filter Report
Refresh
CSV
PDF

Drag column here for grouping

Computer Domain	Computer	Builtin	Account Type	Domain	Group Name	User Name
name.yourdomain.com	GO-TEST-SYS	User Defined	Domain	TESTENV	domain admins	anotheradmin

Logon Session Summary Report

The Summary report for recent Logon Sessions.

1. Navigate to the Privilege Manager Dashboard.
2. In the Search field enter **Logon session**.

Search

Number of Results
5000

Role Type Name (2)
11/12/19, 6:10 AM - Remote Client Task
Collects windows logon events for logon session logging

Report (3)
Remote Client Task (1)
Logon Sessions
11/12/19, 5:50 AM - Report
Basic report for recent Logon Sessions.

Advanced
 Search all items
Logon Session Summary
11/12/19, 5:50 AM - Report
Summary report for recent Logon Sessions.

3. Click on **Logon Session Summary**.
4. The report contains the information for the Computer Name, User Name, total minutes and sessions.

Reports > Logon Session Summary

Drag column here for grouping

Computer Name	User Name	Total Minutes	Sessions
---------------	-----------	---------------	----------

Note: You can also run the **Collect Windows Logon Events Client Task** to get updated windows logon events for logon session logging.

Task > Collect Windows Logon Events Client Task

General Parameters Schedules

Name Collect Windows Logon Events Client Task

Description Collects windows logon events for logon session logging

Command Windows Logon Event Processor

Performance Reporting

Performance Reporting is available for Privilege Manager 10.5 and up. Nightly tasks can collect performance information in the following reports:

- Item Processing Performance
- Processing Performance

1. Navigate to **Admin | Configuration**.
2. Select the **Advanced** tab.
3. Click **Edit** on the bottom of the page.
4. Check the box next to **Save performance counters** under the General tab.
5. Click **Save**.

General

Command Timeout 180

Encryption provider

Max time skew 5

Prevent Legacy Agent Registration (10.4 and older)

Save performance counters

System Secret Vault [Configure](#)

Validate agent event signatures

Note: Once the **Save performance counters** box is checked, find the performance reports by searching for their names ("Item Processing Performance" and "Processing Performance") in the search bar.

Search

performance

Number of Results 5000 1 to 10 of 108

Role Type Name (7)	
Local User Group (100)	<input type="checkbox"/> Item Processing Performance 8/9/18, 10:12 AM - Report
Report (2)	<input type="checkbox"/> Processing Performance 8/9/18, 10:12 AM - Report
Built-in Account (2)	
Windows Privilege (1)	<input checked="" type="checkbox"/> Performance Monitor Users 8/9/18, 10:12 AM - Built-in Account
Commandline Filter (1)	
Show More (all)	
Platform (1)	<input checked="" type="checkbox"/> Performance Log Users 8/9/18, 10:12 AM - Built-in Account
Windows (1)	

Primary User

The primary user is calculated by the data reported from the Logon Session inventory policy. The primary user is considered to be the user with the most minutes on the machine.

1. Enter in the machine name into **Search**.

The screenshot shows a search interface with a text input field containing 'win10' and a 'Search' button. Below the input, it displays 'Number of Results' as 5000 and '1 to 50 of 59'. A table lists results for 'WIN10', including 'Role Type Name (11)', 'Local User Group (19)', and 'Local User (10)'. The first result shows '1/17/19, 10:45 AM - Computer' with links for 'Item Viewer' and 'View XML'.

2. Click on the machine name.

3. Click on **Associations**.

The screenshot shows the 'Resource Explorer > WIN10' interface. The left sidebar has tabs for 'Summary', 'Known Data', 'Events', and 'Associations'. The main area shows details for 'WIN10', including 'Name', 'Created', 'Modified', 'Monitor Resource', and 'Health' (Normal Policy State).

4. This will display the Computer Primary user.

The screenshot shows the 'Resource Explorer > WIN10' interface with the 'Associations' tab selected. A list of associations is shown, with 'Computer Primary User' highlighted. Other items include 'Computer Local Group' and 'Computer Local User'. At the bottom, there are buttons for 'Back', 'View as XML', 'Revoke Agent Trust', and 'Delete'.

The default update primary user for collection task calculates the primary user on a schedule from inventory data.

1. Navigate to **ADMIN | More...**
2. Click on **Tasks**.
3. Expand **Server Tasks**.
4. Click on **Local Security**.
5. From here you can run the **Update Primary User** or the **Update Primary User for Collection Task**.

The screenshot shows the 'Task > Update Primary User for Collection' configuration page. It has tabs for 'General', 'Parameters', and 'Schedules'. The 'General' tab is active, showing the 'Name' as 'Update Primary User for Collection' and the 'Description' as 'Updates the primary user for each computer in the given collection.' At the bottom, there are buttons for 'Back', 'Edit', 'Run Task', 'History', 'Create a Copy', and 'Export'.

Note: The Update Primary User Task only updates the primary user for a given computer resource.

Configuration Feeds

Configuration Feeds are extensions to Privilege Manager. They can be found by navigating to **Admin | More** and then selecting the **Config Feed** link. Configuration feeds allow Thycotic to deliver new components/items to Privilege Manager. Simply click through the options in the Config Feeds page starting with the Select Items button and download anything that might be useful in your environment. Once the item is downloaded, it is immediately available in your Privilege Manager instance.

The main product areas covered are:

- Application Control Solution
- Local Security Solution
- Thycotic Management Server Core

Application Control Solution	Ignoring macOS Updates	Contains the policy to ignore macOS Catalina in the Software Update preference pane.
	Reset ignored macOS Software Updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane.
	AP - Remove Programs Helper	Contains the policies for the Remove Programs Helper Utility. Note: This only pertains to Privilege Manager versions prior to 10.7. In 10.7 and up, the utility is automatically installed and can be enabled via policy .
	AP - UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files.
	AP - UNC Whitelist Policy Template	Contains the UNC Share Whitelist Policy Template to scan a network share and automatically whitelist files in MSI, ISO, ZIP files.
	Browser Lockdown	Contains Configurable Browser Lockdown Settings.
	Secondary File Hash Exclusion Policy	Policy template to exclude non-executable files from the hash process.
Local Security Solution	Local Security Solution - Disclose Password HelpDesk Tab	Adds the helpdesk tab to the Security Manager console.
Thycotic Management Server Core	Maintenance Resources	Contains maintenance gauges, tasks, etc. for optimal TMS performance.
	OU Based Computer Groups	Contains a task to automatically create OU based computers groups and collections.
	SQL CPU Usage Gauge	Contains a gauge and report to monitor SQL CPU usage.
	Windows Server and Desktop Filters	Contains Windows Server and Desktop Filters.

Exclude File Extensions during File Hashing

The Thycotic Application Control Agent collects the file hash of a new process and also the hashes of the child processes it runs. Sometimes non-executable file types cause execution issues during the hashing process. Via the downloadable Configuration Feeds, Thycotic offers a policy template that provides the ability to exclude certain file extensions from the hash process.

If non-executable files like xlsx, xls, mdb, and accdb for example cause execution issues, download the **Secondary Hash Exclusions** policy template. By default .mdb and .accdb are excluded from the file hashing procedure in Privilege Manager. To not overwrite default behavior, make them a part of your exclude list at all times.

Always manually test a new policy deployment on a single endpoint, and only push the solution to all desired endpoints after a successful verification on the test environment.

Note: This feature requires a Thycotic Control Agent version of 10.5 or greater.

1. Navigate to **Admin | More** and then click the **Config Feeds** link.
2. Next to **Privilege Manager Configuration Feeds** click **Select Items**.
3. Next to **Application Control Solution** click **Select Items**.
4. Locate the **Application Control - Secondary Hash Exclusions** and click **Download**.

Data Feeds > Application Control Solution

The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	DOWNLOADED
Application Control - EMET Example Policies	Contains sample Enhanced Mitigation Experience Toolkit (EMET) Application Control policies for common applications.	Mar 13, 2019, 12:24:27 PM	Download
Application Control - Remove Programs Helper	Contains the policies for the Remove Programs Helper Utility	Apr 8, 2019, 4:12:22 PM	Download
Application Control - Secondary Hash Exclusions	Contains the policies for excluding specific extensions from the secondary hash calculations.	Sep 12, 2019, 5:23:27 PM	Download
Application Control - UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files	Mar 13, 2019, 12:24:27 PM	Aug 7, 2019, 10:44:28 AM Download

The policy template is being downloaded and installed.

5. Navigate to **Admin | Policies** and select the **General** tab.
6. Search and select the new policy **Deploy File Hash Exclusion Setting (Windows)**.

Policies

[Add New Policy](#)

Windows Mac OS Client System Settings ActiveX Firewall General

1 to 2 of 2

ENABLED	NAME	FOLDER
Any	h	
Not Enabled	Deploy File Hash Exclusion Setting (Windows)	Windows
Not Enabled	Shared Folder Inventory Policy	Windows

7. Click **Create a Copy**.
8. Click **Edit**, change the Name on the **General** tab and also click the **Enable** checkbox.
9. Go to the **Parameters** tab and add the list of extensions to exclude, for example xlsx, xls, mdb, accdb.

Remote Scheduled Client Command > Copy of Deploy File Hash Exclusion Setting (Windows)

General Parameters Triggers Targets Conditions Advanced Deployment

Enter default parameter values for this task.

File Extensions not to Hash

[Save](#) [Cancel](#)

10. Go to **Triggers** and verify the set schedule works for your environment and edit if changes are required.

Remote Scheduled Client Command > Copy of Deploy File Hash Exclusion Setting (Windows)

General Parameters **Triggers** Targets Conditions Advanced Deployment

TRIGGERS (WHEN TO RUN)

- Daily at 10:00:00 PM starting Tue Jul 31 2018 (repeating every 2 hours for a duration of 24 hours)
- Upon task creation/modification
- Add Trigger

11. Go to the **Targets** tab and specify the targets for the deployment of that list.

Remote Scheduled Client Command > Copy of Deploy File Hash Exclusion Setting (Windows)

General Parameters Triggers **Targets** Conditions Advanced Deployment

RESOURCE TARGETS (APPLIES TO ANY OF THESE MANAGED COMPUTERS)

- Windows Computers
- Add Resource Target

12. On the Conditions tab, you may specify any conditions specific to your environment.
13. Click **Save**.

To create manual secondary extension exceptions to file hash collection, add a registry key to the endpoint.

1. Open Registry Editor (regedit.exe) and navigate to
HKLM:\Software\Policies\Arellia\AMS.
2. Create **New | String Value**
 1. Name: **SecondaryExtensionExclusions**
 2. Value: enter a comma-separated list of extensions to include, i.e. xls,xls,mdb,accdb.
3. Restart the Thycotic services on this machine.

Open a file matching an extension from your inclusion list and test if it works on this endpoint. If it works, create a Policy to push this registry key creation to all desired endpoints.

Ignoring macOS Updates

MacOS has a command-line utility that can be used to ignore specific software updates in the Software Update preference pane. To provide a way in Privilege Manager to ignore or reset ignored OS updates, the following policies are available via configuration feeds.

Data Feeds > Application Control Solution

The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	DOWNLOADED	
Application Control - Ignore macOS Catalina software update	Contains the policy to ignore macOS Catalina in the Software Update preference pane	Jan 8, 2020, 7:01:09 PM	Jan 16, 2020, 6:23:23 AM	Installed
Application Control - Reset ignored macOS software updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane	Jan 8, 2020, 7:01:09 PM	Jan 16, 2020, 6:24:26 AM	Installed
Application Control - Secondary Hash Exclusions	Contains the policies for excluding specific extensions from the secondary hash calculations.	Nov 27, 2019, 9:49:00 AM		Download
Application Control - UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files	Jul 24, 2019, 2:23:53 PM		Download
Application Control - UNC Whitelist Policy Template	Contains the UNC Share Whitelist Policy Template to scan a network share and automatically whitelist files in MSI, ISO, ZIP files	Jul 24, 2019, 2:23:54 PM		Download

[Back](#)

- The Ignore macOS Catalina Software Update (Mac OS) - The Ignore macOS Catalina Software Update (Mac OS) policy uses the Run Shell Script (Mac OS) command. By default, it is triggered to run Daily at 5:00:00 AM starting Fri Dec 20 2019, with default Targets specified as MacOS Computers.
- The Reset ignored macOS Softwares Update (Mac OS) - The Reset ignored macOS Softwares Update (Mac OS), uses the Run Shell Script (Mac OS) command. By default, it is triggered to run Daily at 5:30:00 AM starting Fri Dec 20 2019, with default Targets specified as MacOS Computers.

1. Navigate to **ADMIN | More**.
2. Click on **Config Feeds**.
3. Click on **Select Items** for **Privilege Manager Product Configurations**.

Data Feeds > Data Feeds

The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	
Privilege Manager Product Configuration Feeds	Data feed listing Privilege Manager Product Configuration Feeds	Jan 16, 2020, 6:23:09 AM	Select Items

4. Click on **Select Items** for Application Control Solution.

Data Feeds > Privilege Manager Product Configuration Feeds

The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	
Application Control Solution	Configuration Package Feed	Jan 8, 2020, 7:01:09 PM	Select Items
Local Security Solution	Configuration Package Feed	Jul 24, 2019, 2:23:57 PM	Select Items
Thycotic Management Server Core	Configuration Package Feed	Nov 27, 2019, 9:58:05 AM	Select Items

[Back](#)

5. Click on download for both **Application Control - Ignore macOS Catalina software update** and **Application Control - Reset ignored macOS software updates**.

Data Feeds > Application Control Solution

i The server must have internet access in order to download data feeds.

NAME	DESCRIPTION	LAST UPDATED	DOWNLOADED	
Application Control - Ignore macOS Catalina software update	Contains the policy to ignore macOS Catalina in the Software Update preference pane	Jan 8, 2020, 7:01:09 PM	Jan 16, 2020, 6:23:23 AM	Download
Application Control - Reset ignored macOS software updates	Contains the policy to reset ignored macOS software updates in the Software Update preference pane	Jan 8, 2020, 7:01:09 PM	Jan 16, 2020, 6:24:26 AM	Download
Application Control - Secondary Hash Exclusions	Contains the policies for excluding specific extensions from the secondary hash calculations.	Nov 27, 2019, 9:49:00 AM		Download
Application Control - UNC Elevation Policy Template	Contains the UNC Share Elevation Policy Template to scan a network share and automatically elevate MSI and EXE files	Jul 24, 2019, 2:23:53 PM		Download
Application Control - UNC Whitelist Policy Template	Contains the UNC Share Whitelist Policy Template to scan a network share and automatically whitelist files in MSI, ISO, ZIP files	Jul 24, 2019, 2:23:54 PM		Download

[Back](#)

1. Navigate to **ADMIN I Policies**.
2. Click on the **General Tab**.
3. Click on **Ignore macOS Catalina Software Update (Mac OS)**.

Policies

[Add New Policy](#)

Windows Mac OS Client System Settings ActiveX Firewall **General**

View 10 rows 1 to 10 of 38

ENABLED	NAME	FOLDER
Any	Filter	
Enabled	Cleanup sent Privilege Manager Events (Mac OS)	Mac OS
Enabled	Basic Inventory (Windows)	Windows
Not Enabled	Ignore macOS Catalina Software Update (Mac OS)	Mac OS
Not Enabled	Reset ignored macOS Software Updates (Mac OS)	Mac OS

4. Under the General tab, click **Edit**.

Remote Scheduled Client Command > Ignore macOS Catalina Software Update (Mac OS)

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name Ignore macOS Catalina Software Update (Mac OS)

Description This will ignore the macOS Catalina software update and cause it to be removed from the Software Update preference pane.

Command Run Shell Script (MacOS)

[Back](#) [Edit](#) [Create a Copy](#) [Delete](#) [Export](#)

5. Check the **Enabled** box.
6. Click **Save**.

Policies

[Add New Policy](#)

[Windows](#) [Mac OS](#) [Client System Settings](#) [ActiveX](#) [Firewall](#) [General](#)

View 10 rows 1 to 10 of 38

ENABLED	NAME	FOLDER
Any	<input type="text" value="Filter"/>	
Enabled	Cleanup sent Privilege Manager Events (Mac OS)	Mac OS
Enabled	Basic Inventory (Windows)	Windows
Not Enabled	Ignore macOS Catalina Software Update (Mac OS)	Mac OS
Not Enabled	Reset ignored macOS Software Updates (Mac OS)	Mac OS

7. Repeat steps 1 through 6 for **Reset Ignored macOS Software Updates (Mac OS)** policy.

You can edit when the policy runs by navigating to the **Triggers** tab under the policy and clicking on **Edit**.

Remote Scheduled Client Command > Ignore macOS Catalina Software Update (Mac OS)

[General](#) [Parameters](#) [Triggers](#) [Targets](#) [Conditions](#) [Advanced](#) [Deployment](#)

TRIGGERS (WHEN TO RUN)

Default: Daily at 2:00:00 AM starting Fri Dec 20 2019

[Add Trigger](#)

[Save](#) [Cancel](#) [Export](#)

Note: Once the policies are enabled they do not run immediately. If you would like the policies to run right way you will need to adjust the schedule which you can find under the **Triggers** tab in the policy.

Foreign Systems

Foreign Systems in Privilege Manager are any systems for which a connections or an integration has to be set-up, providing a system URL (network address) and authentication information. Foreign Systems can be Thycotic or third-party products and their basic integration set-up in Privilege Manager is alike.

- [Integration between Privilege Manager and Secret Server](#)

- [Setting Up Azure Active Directory Integration in Privilege Manager](#)

- [Set-up an SMTP Server Connection](#)
- [Set-up a Cylance Connection](#)
- [Set-up a ServiceNow Ticketing Connection](#)
- [Set-up VirusTotal](#)
- [Set-up an SCCM Connection](#)
- [Set-up Syslog](#)

- [Remove RDP Integration](#)

The following topics on integrating Privilege Manager with other Thycotic products are available:

- [Integration between Privilege Manager and Secret Server](#)

Privilege Manager has the ability to use Secret Server as its storage container for credentials. This includes credentials for connecting to integrated systems such as Service Now, as well as credentials for local accounts that are managed by Local Security in Privilege Manager. Customers can choose to integrate with Secret Server only (no Vault setup) or Secret Server and Vault. Either option requires Authentication Data setup for Foreign Systems in Privilege Manager.

The Secret Server Vault integration for 10.7.1 and newer does not require Secret Server to be setup as the authentication provider. Any supported authentication provider can be used, independent from using Secret Server as a Password Vault.

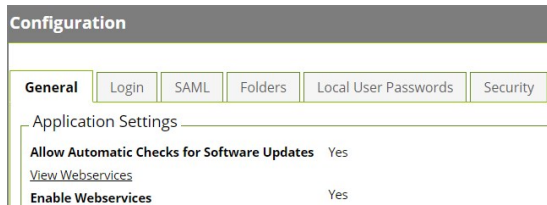
In Secret Server, Privilege Manager credentials are stored as Secrets, and Privilege Manager uses the Secret Server REST API to communicate with Secret Server.

For this the proper license types need to be set-up, as Secret Server Express (free) does not support the integration with Privilege Manager.

Verify Web Services are Enabled in Secret Server

As a prerequisite, you need to make sure that your Secret Server instance has Web Services Enabled.

1. Navigate to **Admin | Configuration | Application Settings**.
2. Verify that under View Webservices the **Enable Webservices** option is reflecting **Yes**.



3. Enter credentials for "Secret Server Default Credential" located at **Admin | Configuration | User Credentials** tab. Edit this account to choose which account will be used by Privilege Manager to connect to Secret Server. This can be a regular Secret Server user or a Secret Server Application account.

Note: The account needs to have a role with ALL of the following permissions.

Add Secret
Administer Configuration
Administer Folders
Administer Licenses
Assign Secret Policy
Create Root Folders
Delete Secret
Edit Secret
Own Secret
View Secret

Setup Authentication Data in Privilege Manager

1. Navigate to **Admin | Configuration**.
2. Click the **Foreign Systems** tab.
3. Select **Secret Server** from the list.
4. In the Name column click on **Default Secret Server**.
5. The Secret Server Foreign System page loads, click the **Edit** button.

6. Under Settings, update the following:

1. **Credential:** This is a Secret Server user (preferably an application account). Refer to required permissions above.
2. **Secret Server Url:** This is the url that end users use to access Secret Server. **HTTPS** is required. Also the validation on this field will reach out to Secret Server using the url provided. If it can't be reached, or if the Secret Server version is lower than 10.6, there will be a 404 not found validation error. The URL needs to be fully qualified ending with a */*.
3. **TMS Url:** This is the url to access TMS itself. It is the url that end users use to access Privilege Manager, minus the PrivilegeManager/ part at the end of the path. This URL also needs to be well formed and fully qualified ending with a */*.

7. Click **Save**.

8. Navigate to the Authentication tab and enable Secret Server as the authentication provider by selecting Secret Server from the drop-down list.

9. Click **Save**.

After these steps the Secret Server Foreign System is ready for use. If you need to enable or disable features for this integration, the Integration Feature list is below the Settings area on the page. Follow any of the links to turn features on and off.

Configure Privilege Manager Credential Vault (optional)

1. In Privilege Manager on the home page select the **Local Security** tile to go to Local Security page.
2. On the top of the Local Security page, click on the suggestion stating **Privilege Manager can store credentials in Secret Server, would you like to configure this now?** For reference, the relative URL for this page is *TMS/PrivilegeManager/#/lss/vault*

Privilege Manager can store credentials in Secret Server, would you like to configure this now? ✕

Show All Computer Groups [Create Computer Group](#)

1 to 2 of 2

NAME	COMPUTERS	USER GROUPS	USERS
MacOS Computers	0	0	0
Windows Computers	0	0	0

The Password Vault Settings configuration page opens.

Password Vault Settings [Edit](#)

Configuring the Password Vault

[Setup Secret Server Foreign System](#)

Use Secret Server No

3. Select **Edit**.

1. Check the box **Use Secret Server** in order to use Secret Server's vault to store credentials.

Password Vault Settings

Configuring the Password Vault

[Setup Secret Server Foreign System](#)

Use Secret Server

Save Changes
Cancel

2. Enter the username and password for the account that will be used to access Secret Server.

Secret Server Foreign System

[Configuration](#) [Change History](#)

Details [Edit](#)

Name Default Secret Server

Description

Settings [Edit](#)

Credential SS Default Secret Server Credential

Secret Server URL <https://myassignedname.secretservercloud.com/>

TMS URL <https://myassignedname.privilegemanagercloud.com/Tms/>

Integration Features

Secret Server Vault Off [Setup Secret Vault](#)

Back

Note: These are the same credentials that will be stored as the Secret Server Default Credential (located at the **Admin | Configuration | User Credentials** tab). If a user already has been entered here, the same account will be auto populated into the configuration page.

4. Back on the **Password Vault Settings** configuration page, click **Save Changes**.

Password Migration

After the vault and authentication set-up, all passwords are migrated from Privilege Manager to Secret Server. This migration process may take time.

Important Notes

The migration will create a root folder in Secret Server named Privilege Manager Secrets. Do NOT delete this folder. The folder, by default only has the sync account user as an owner, with no other permissions. The permissions on this folder can be modified to allow helpdesk users or administrators access to the Secrets. Do NOT remove the sync account user's permissions from the folder.

If desired the folder can be moved or renamed within Secret Server.

Templates

There are two Templates that Privilege Manager uses to store Secrets in Secret Server. These templates must exist with the proper fields and be marked as active.

- **Password (Template Id: 2)**: The following fields need to exist on the template:

- Username
- Password

Do NOT mark any other fields in that template as required!

- **Windows Account (Template Id: 6003)**: The following fields need to exist on the template:

- Machine
- Username
- Password

Do NOT mark any other fields in that template as required!

Note: To troubleshoot or remove the integrated configuration, navigate to the Admin | Configuration | Advanced tab in Privilege Manager and click Edit at the bottom of the page. Locate the "System Secret Vault" setting and click the Select Resource link. Here, a user can manually add and remove the Secret Server vault. If you choose to remove the Secret Server vault, a migration of passwords from Secret Server's vault to Privilege Manager automatically happens.

The following topics are available in the Active Directory (AD) integration section:

- [Setting Up Local Active Directory Synchronization](#)
- [Setting Up Azure Active Directory Integration in Privilege Manager - 10.6 and up](#)
- [10.5 Azure AD Integration with Privilege Manager](#)

Summary

This article explains how to integrate Azure Active Directory (AD) with Privilege Manager 10.5. It is divided into the following sections:

- Introduction
- Part I: Establish Credentials for Privilege Manager to access Azure AD
- Part II: Add Azure AD as a Foreign System in Privilege Manager
- Part III: Complete the Azure AD Integration with Privilege Manager
- Additional Information

Introduction

As a Privilege Manager user, you might want to do Azure AD integration for one or more of the following reasons:

- Import users and groups into Privilege Manager, via Azure AD. This gives you the ability to:
 - Assign one or more Azure AD users to a Privilege Manager role (Administrator or other).
 - Use a User Context filter, in the definition of an Application Control policy, to target applications based on ownership by one of the Azure AD imported users.
- Use Azure AD as an authentication provider, to login into Privilege Manager (for any of the Azure users which have been assigned to a Privilege Manager role).

The procedure for Azure AD integration is outlined below (providing a summary of the steps):

Part I. Establish credentials for Privilege Manager to access your Azure AD

This is done in Privilege Manager from: Admin | Configuration | User Credentials

The steps are:

- Step A: Create a service account in the Azure portal.
- Step B: Add that service account as a User Credential in Privilege Manager.

Part II. Add your Azure AD as a "Foreign System" in Privilege Manager

This is done in Privilege Manager from: Admin | Configuration | Foreign Systems

You will also need to interact with Azure to enter/obtain some data.

Part III: Complete the Azure AD Integration with Privilege Manager

Overall, there are four (sub) steps involved in Part III:

- Step One: Import Users & Groups.
You need to do the following steps, Steps Two to Four, only if you want to use Azure AD as an authentication provider.
- Step Two: Assign Azure User or Group to Role.
- Step Three: Complete Setup.
- Step Four: Set as Authentication Provider.

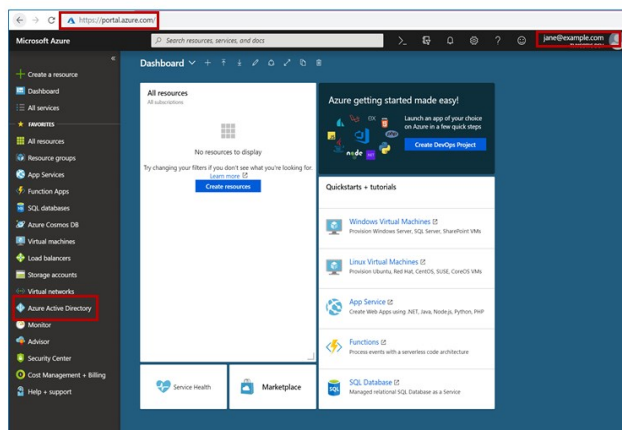
The steps for Part I are:

- Step A: Create a service account in the Azure portal.
- Step B: Add that service account as a User Credential in Privilege Manager.

Part I, Step A: Create a Service Account in the Azure Portal

Note: Please ensure you have a user account in the Azure portal which has permissions to create a new user account (which you intend to set up as a user credential in Privilege Manager for Azure AD access).

- Log in to the Azure portal: <https://portal.azure.com>. Assume you login as: jane@example.com. Make sure you have selected the domain which you want to synch with Privilege Manager. Assume the domain is dev.Thycotic.com.

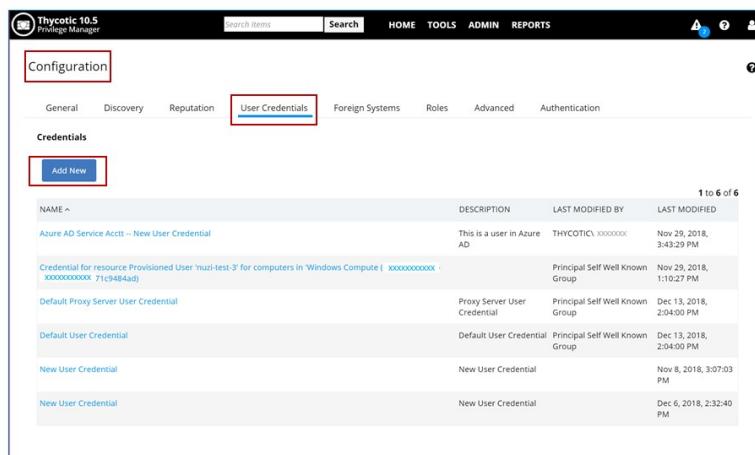


- Click on Azure Active Directory, in the left pane.
- Navigate to: Manage | Users | New User
- Fill in the form to provide data for user name etc. to create the service account. (This account must have permissions to read user and group information in Azure AD.)
- Assume you have created the service account as follows:
 - Name: Azure AD Service Acctt for Privilege Manager
 - User Name: AD-synch-user@example.com

Part I, Step B: Add the Service Account as a User Credential in Privilege Manager

Now you have to add the service account (which you created in the Azure portal) as a User Credential in Privilege Manager.

- Login to Privilege Manager (as an Administrator)
- Navigate to: Admin | Configuration | User Credentials
- Click on "Add New"



You will see a page with two sections; fill them in as follows:

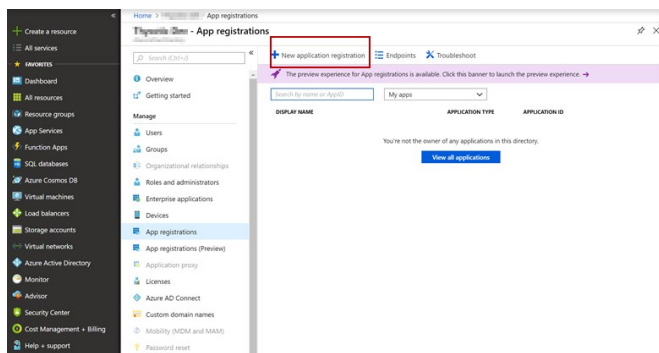
- Details section: Enter the name of the service account you created in the Azure portal (which you want to be used by Privilege Manager to synch with your Azure AD) and, optionally, a description.

- Setting Section: Enter account name and password for the service account.

The screenshot shows the configuration form for a service account in Thycotic 10.5 Privilege Manager. The form is divided into two sections: 'Details' and 'Settings'. In the 'Details' section, the 'Name' field is filled with 'Azure AD Service Acctt for Priv Man' and the 'Description' field contains 'User Credential for Priv Man to Access Azure AD'. In the 'Settings' section, the 'Account Name' field is filled with 'AD-synch-user@example.com', and the 'Password' and 'Confirm Password' fields are filled with masked characters. A 'Save' button is highlighted with a red box at the bottom left of the form.

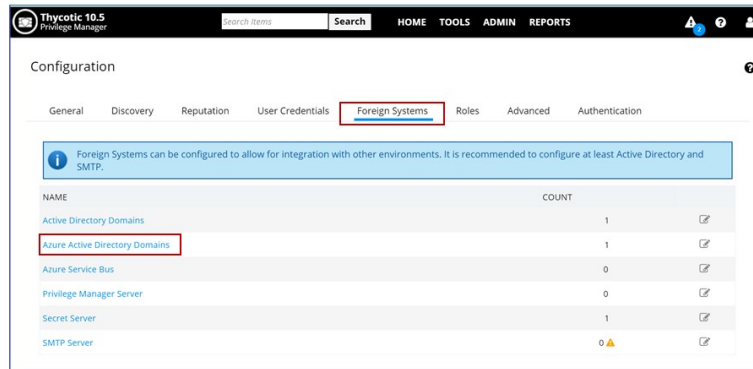
Click the **Save** button.

The name of the service account will now be listed, as a link, in the User Credentials tab.

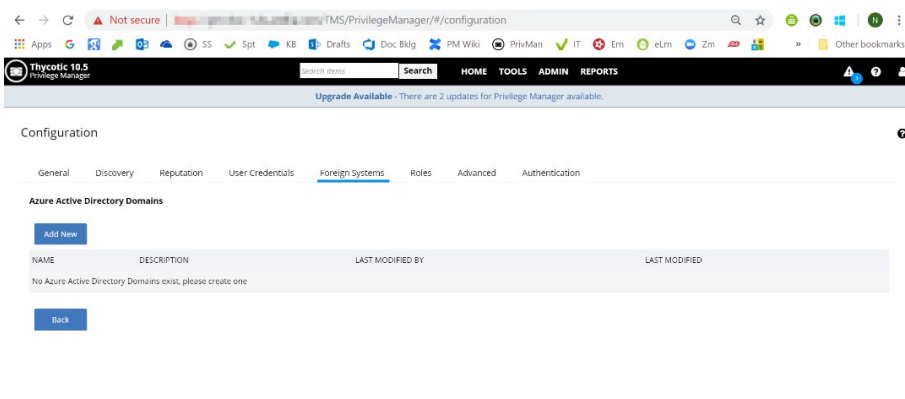


Now you will add your Azure AD as a "Foreign System" in Privilege Manager.

Navigate to: Admin | Configuration | Foreign Systems | Azure Active Directory Domains.

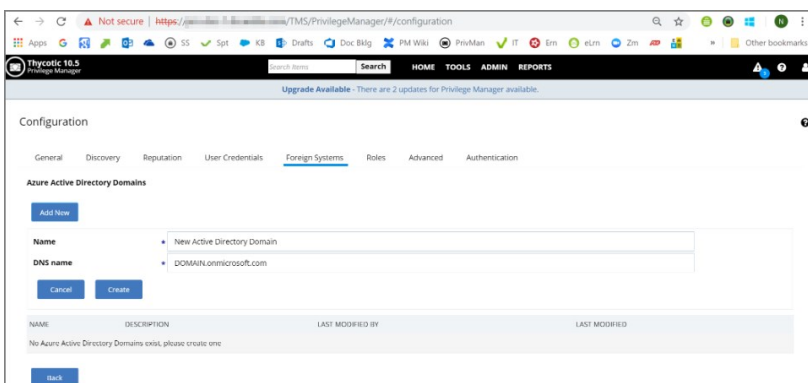


Clicking on Azure Active Directory Domains will take you to a new page. Click the "Add New" button.



On the page for adding a new domain, the fields are to be filled in as follows:

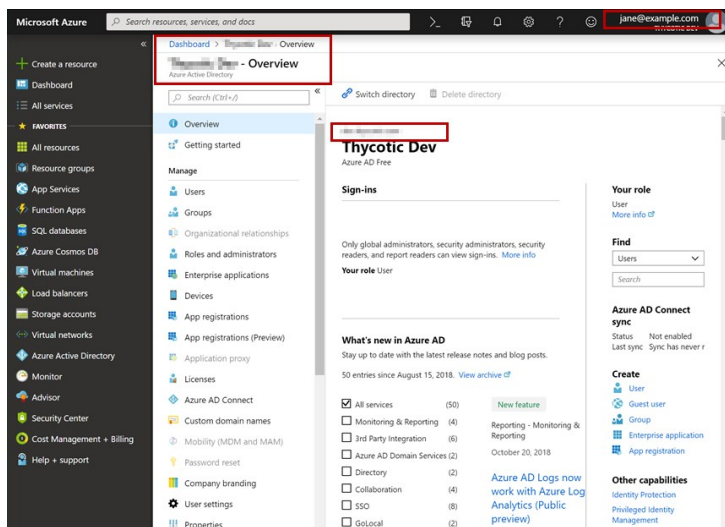
- Name: Any name of your choice.
- DNS Name: The DNS name has to be obtained from the Azure portal; instructions are provided further below (after the screenshot of the page showing these fields).



Now you have to go to the Azure portal to obtain the DNS name.

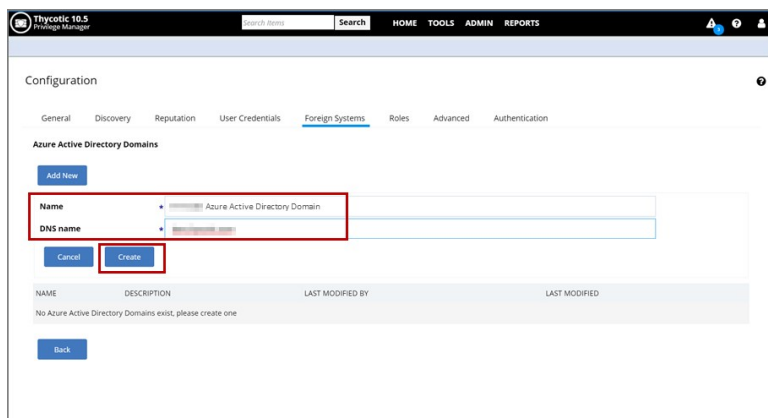
- Login to the Azure portal (selecting the domain which you want to be synced with Privilege Manager).
- The DNS name is the URL found in the Overview pane.

- Copy this URL to be pasted into the DNS name field in Privilege Manager.



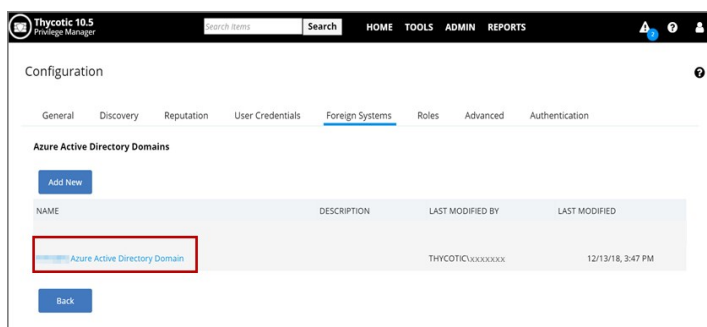
Now back in Privilege Manager, fill in the fields as follows:

- Name: Enter any descriptive name of your choice.



DNS Name: Enter the URL obtained from the Azure portal.

Click the Create button.



The name of the AD domain you just added will now be listed in Azure Active Directory Domains, in the Foreign Systems tab. (You might need to refresh the browser to see it displayed.)

Click on the link for the domain you just added. You will be taken to the Azure Authentication page for Part III of this procedure.

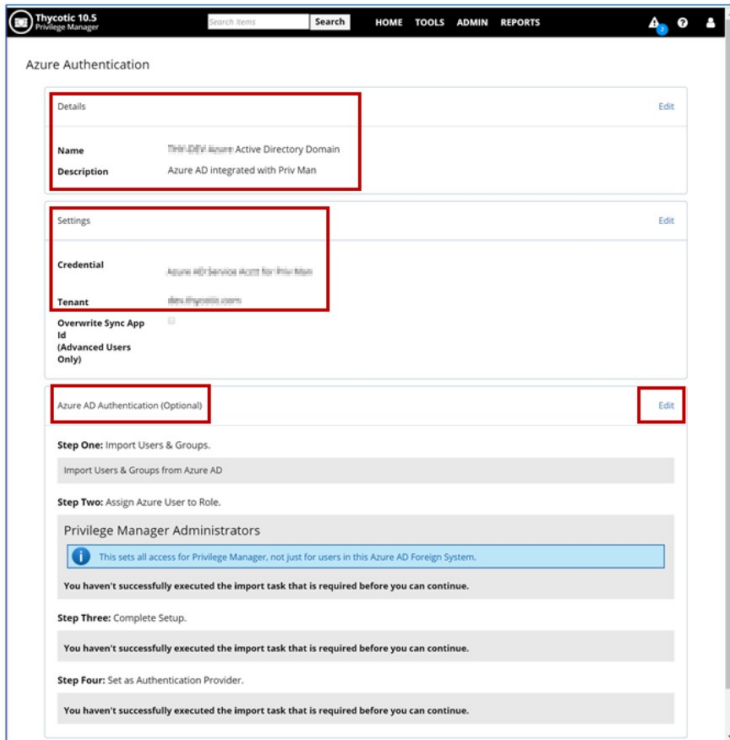
Overview of the Azure Authentication Page

On the Azure Authentication page, there are several sections for filling in data:

- Details

- Settings
- Azure AD Authentication; this has the following sections:
 - Step One: Import Users & Groups.
 - Step Two: Assign Azure User to Role.
 - Step Three: Complete Setup.
 - Step Four: Set as Authentication Provider.

NOTE: Steps Two-Four are needed only if you want to use Azure AD authentication.



Details and Setting Sections

Edit the "Details" section; enter data and save changes.

- Name: will be populated by Privilege Manager.
- Description: enter a description – optional.

The screenshot in the Overview section above shows this as already done.

Then edit the "Settings" section; enter data and save changes.

- Credential: Enter the same service account name that you created in Admin | Configuration | Credentials
(As you start entering the name string, the Search field will start showing results and you can select the name you want.)
- Tenant: This is the same as the DNS name; will be populated by Privilege Manager; if not correctly populated, enter the DNS name.

The screenshot in the Overview section above shows this as already done.

Then click Edit for the "Azure AD Authentication (Optional)" section.

Step One: Import Users & Groups

After the Credential field has been populated (done in the previous section), you will see that you have a link to do an import in the "Step One" section.

Details Edit

Name Privileged Active Directory Domain
Description Azure AD integrated with Priv Man

Settings Edit

Credential Azure AD Service Acct for Priv Man
Tenant [redacted]
Overwrite Sync App Id (Advanced Users Only)

Azure AD Authentication (Optional)

Step One: Import Users & Groups.
[Import Users & Groups from Azure AD](#)

Step Two: Assign Azure User to Role.
Privilege Manager Administrators
 ⓘ This sets all access for Privilege Manager, not just for users in this Azure AD Foreign System.
 You haven't successfully executed the import task that is required before you can continue.

Step Three: Complete Setup.
 You haven't successfully executed the import task that is required before you can continue.

Step Four: Set as Authentication Provider.
 You haven't successfully executed the import task that is required before you can continue.

Save Changes Delete Cancel

Back

- In Step One, click the link to start import.
- A task will run to import all users and groups that exist in your Azure AD domain.
- Then click Refresh to see results.

Physic 10.5
Privilege Manager

Search HOME TOOLS ADMIN REPORTS

Azure Authentication

Details Edit

Name Privileged Active Directory Domain
Description Azure AD integrated with Priv Man

Settings Edit

Credential Azure AD Service Acct for Priv Man
Tenant [redacted]
Overwrite Sync App Id (Advanced Users Only)

Azure AD Authentication (Optional)

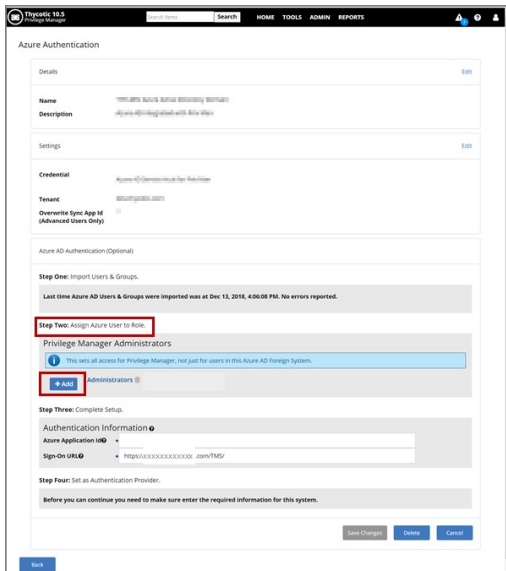
Step One: Import Users & Groups.
 Last time Azure AD Users & Groups were imported was at Dec 13, 2018, 4:06:08 PM. No errors reported.

Step Two: Assign Azure User to Role.
Privilege Manager Administrators
 ⓘ This sets all access for Privilege Manager, not just for users in this Azure AD Foreign System.
 + Add Administrators

Step Three: Complete Setup.
Authentication Information
Azure Application Id [redacted]
Sign-On URL https://[redacted]@privman.com/TMS/

Step Two: Assign Azure User to Role

To start Step Two, click the Add button.

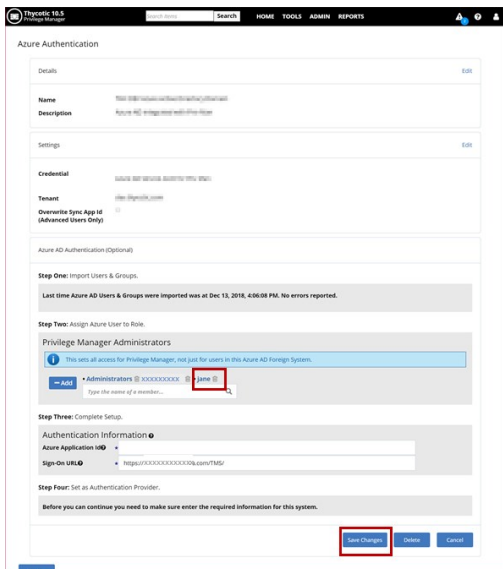


In the text field that opens up, start typing the name of the user account who you wish to add for the Privilege Manager admin role; from the search results drop-down, select the user name.

The user name will be added to the list above the search box.

In the screenshot below, we show the user "jane", whose account name is jane@example.com.

Click "Save Changes".

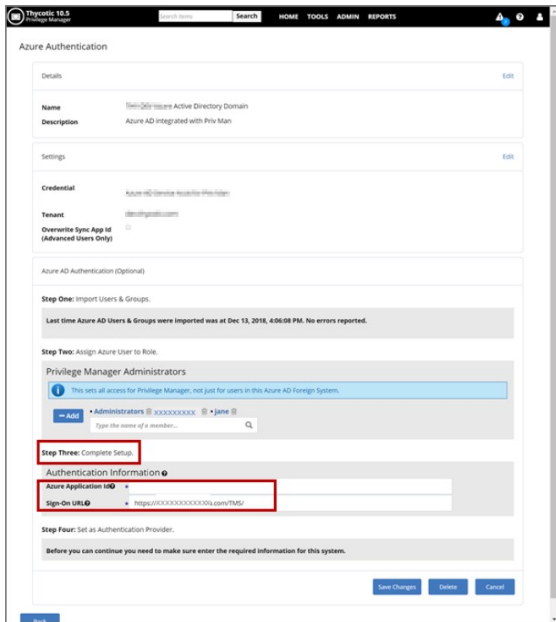


At this point, you have achieved your goal of being able to assign a user imported from Azure AD to the Privilege Manager Admin role.

Step Three: Complete Setup

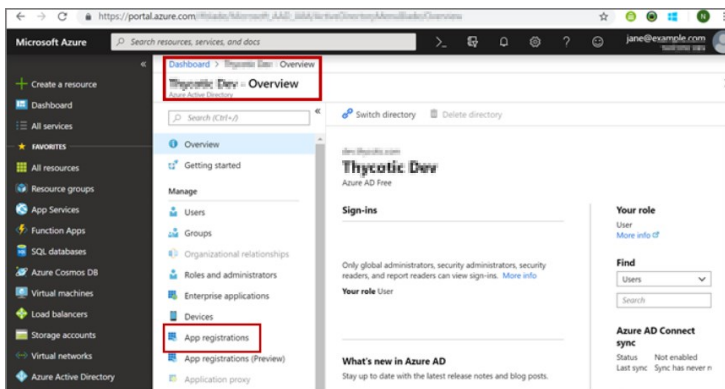
In this step you store the Privilege Manager Azure Application ID which you will obtain from the Azure portal. The fields to fill are:

- Azure Application Id: We need to obtain the value from Azure AD.
- Sign-On URL: Privilege Manager will populate this field. If not, paste here the URL you use for launching Privilege Manager in a browser.

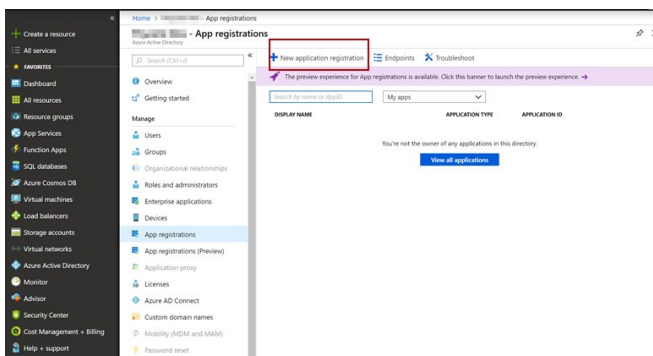


To obtain the Azure Application Id, log into <https://portal.azure.com>. Make sure you are in the correct directory – the one you are trying to synch. You need to do the following on the Azure portal:

- Register Privilege Manager as an application.
- Obtain (copy) the Application ID so we can use it to complete Step Three on the Azure Authentication page of Privilege Manager.

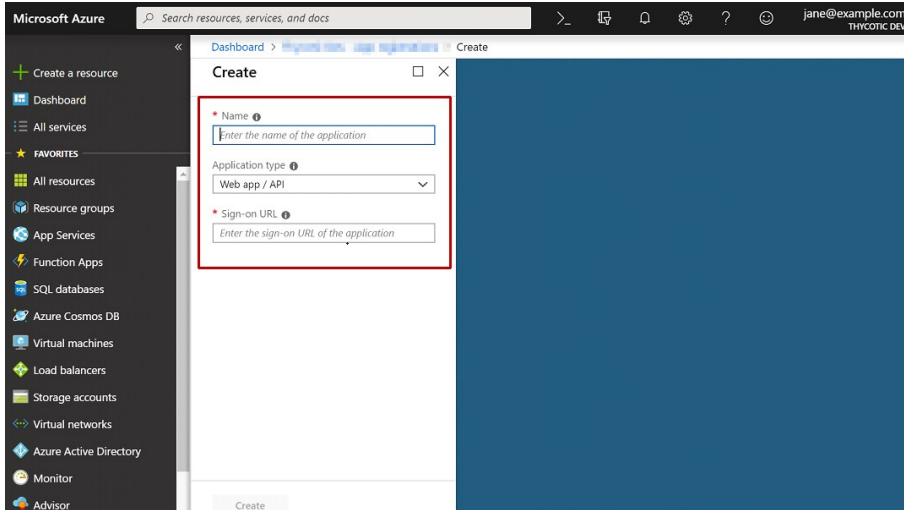


Click on "App registrations".



Click on "New application registration". On the next page, you need to fill out the three fields:

- Name: Enter a name to represent your Privilege Manager instance.
- Application type: Select "Web app / API"

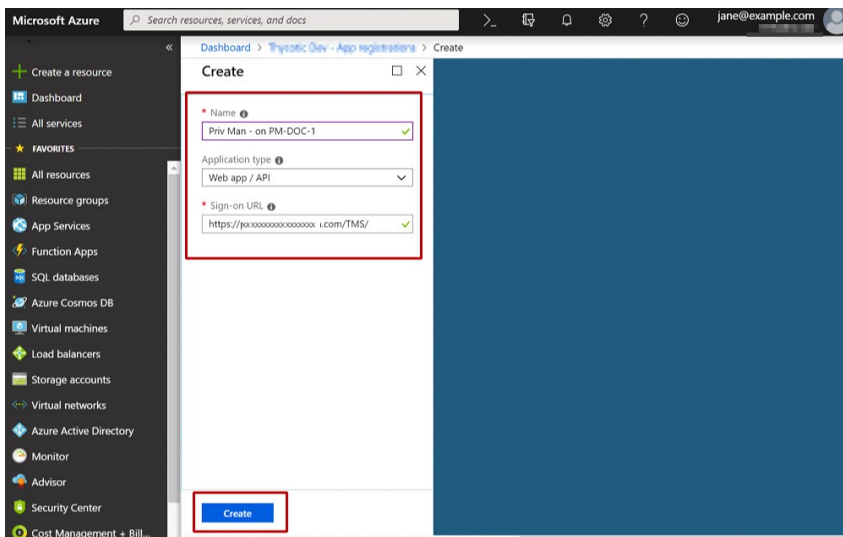


Sign-on URL: Copy this from the Step Three "Sign-On URL" field in Privilege Manager

To get the Sign-on URL:

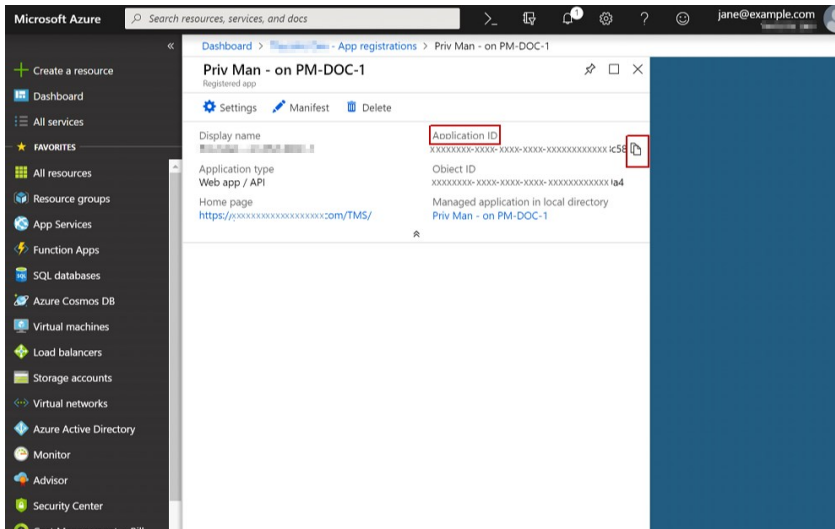
- Navigate to Privilege Manager: Admin | Configuration | Foreign Systems | Azure Active Directory Domains
- Copy the Sign-on URL from Step Three to paste into the Azure form.

The screenshot below shows all three fields populated.



After filling each of the three fields, click Create.

Azure will now provide an Application ID; copy that.



Now back in Privilege Manager:

Paste into the Step Three field, the Application ID you copied from Azure. Save Changes.

Azure AD Authentication (Optional)

Step One: Import Users & Groups.

Last time Azure AD Users & Groups were imported was at Dec 13, 2018, 4:06:08 PM. No errors reported.

Step Two: Assign Azure User to Role.

Privilege Manager Administrators

This sets all access for Privilege Manager, not just for users in this Azure AD Foreign System.

— Add • Administrators [xxxxxxxxxxxx] • jane []

Type the name of a member...

Step Three: Complete Setup.

Authentication Information

Azure Application Id [xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx58]

Sign-On URL [https://xxxxxxxxxxxxxxxx.com/TMS/]

Step Four: Set as Authentication Provider.

Before you can continue you need to make sure enter the required information for this system.

Save Changes Delete Cancel

Back

Step Four: Set as Authentication Provider

In this step, you can set Azure AD as your authentication provider for Privilege Manager.

The informational message in Step Four tells you which provider you are currently using to authentication.

(Advanced Users Only)

Azure AD Authentication (Optional) Edit

Step One: Import Users & Groups.
Last time Azure AD Users & Groups were imported was at Dec 13, 2018, 4:06:08 PM. No errors reported.

Step Two: Assign Azure User to Role.
Privilege Manager Administrators
This sets all access for Privilege Manager, not just for users in this Azure AD Foreign System.
Administrators • xxxxxxxx • Jane

Step Three: Complete Setup.
Authentication Information
Azure Application ID: xxxxxxxxxxxx-xxxxx-xxxxx-xxxxx-xxxxx.c58
Sign-On URL: https://xxxxxxxxxxxxxxxx.com/TMS/

Step Four: Set as Authentication Provider.
You may only use one authentication provider at a time. You are currently using NTLM.
Use as Authentication Provider

Back

Check the box in front of "Use as Authentication Provider". Save Changes.

You will be asked to confirm your changes.

Note: If you do Save, you will then only be able to log back in using the Azure AD account which you assigned in Step Two.

Click **Save**.

Settings Edit

Confirm Authentication Provider

Please confirm that you want to change the authentication provider for Privilege Manager. You will be immediately logged out after you make this change, and you will only be able to log back in using an Azure AD account.

Cancel Save

Credential

Tenant
Overwrite Sync (Advanced Users Only)

Azure AD Authentication (Optional) Edit

Step One: Import Users & Groups.
Last time Azure AD Users & Groups were imported was at Dec 13, 2018, 4:06:08 PM. No errors reported.

Step Two: Assign Azure User to Role.
Privilege Manager Administrators
This sets all access for Privilege Manager, not just for users in this Azure AD Foreign System.

Privilege Manager will log you out since you now need to login using the Azure AD account which you assigned to the Privilege Manager Admin role, in Step Two.

Thycotic 10.5 Privilege Manager Server Setup HOME SETUP ?

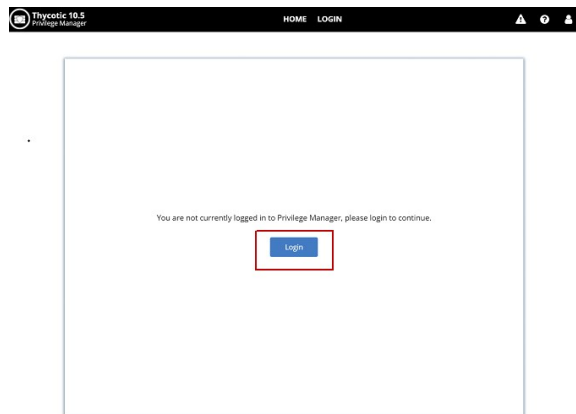
Logout

You have successfully logged out.

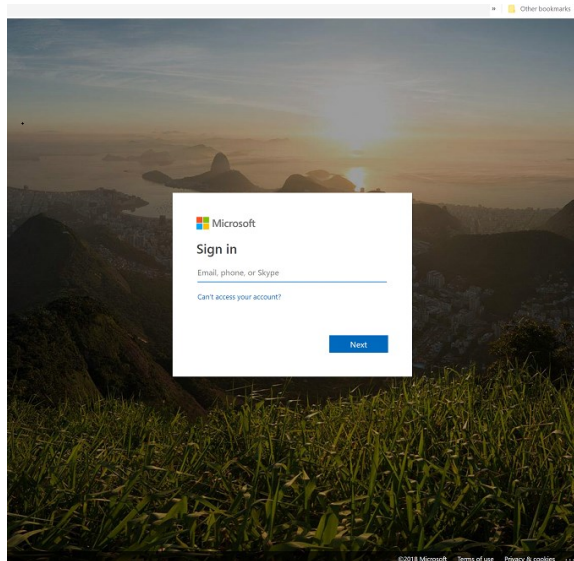
Logging back into Privilege Manager after completion of Step Four

These are the steps for logging back into Privilege Manager after completion of Step Four, "Set as Authentication Provider".

Privilege Manager will prompt you for Login.



You now need to login using the Azure AD account which you assigned to the Privilege Manager Admin role, in Step Two. (In our example, we showed this was jane@example.com.) Sign in with that account name and on the next dialog, accept the permissions requested – to allow Privilege Manager to sign you in and read your profile. Once in Privilege Manager, you will see that you are logged in with your Azure AD account name.



You have now fulfilled your goal of using Azure AD as an authentication provider, to login into Privilege Manager.

Allowing Azure AD Accounts to Login with a Privilege Manager Role

Assumption: you have completed Step Four, or are planning to do so, on the Azure Authentication page.

If you want to add Azure AD users so they will be able to access Privilege Manager, in the Privilege Manager User role, using their Azure credentials:

- Navigate to: Admin | Configuration | Roles | Privilege Manager Users (or whichever role you want)
- Click **Edit | Add**.
- Search for and select any Azure AD user to whom you want to give Privilege Manager User role access to Privilege Manager.
- Save changes.

Options for Activating or De-Activating the Azure AD Authentication Integration

Activating

There are two ways to activate your Azure AD Authentication Integration:

- You can do this via Step Four on the Azure Authentication page, as shown in a previous section of this article.
- Alternatively, you can Activate this integration as follows:
 - Admin | Configuration | Authentication
 - Select your Azure AD Domain from the Authentication Provider dropdown list.
 - Save.

De-Activating

If you activated Azure AD authentication (by any method) and want to switch back to a different auth method, you must do the following:

- Admin | Configuration | Authentication
- Select from the Authentication Provider dropdown list whichever method you prefer.
- Save.

Note: If you try to simply uncheck the Use as Authentication Provider checkbox under Step Four on the Azure Authentication page, the reversal authentication method will NOT take effect.

Deleting Azure AD Domains

To delete an Azure AD Instance:

- Go to: Admin | Configuration | Foreign Systems | Azure Active Directory Domains
- Click the name of the domain you want to delete.
- Click Edit under any of the sections on the Azure Authentication page, then click Delete, and Confirm Delete when prompted by the pop-up dialog.

Locked Out?

Are you accessing Privilege Manager from a Remote Machine?

If you have issues logging into Privilege Manager from a client machine, first try logging in with a local account directly on your Privilege Manager web server.

Have you recently Reset your Azure Account Password?

If you've recently performed a password reset with the Azure account you are using for login, sign into the Azure portal with that account and follow the prompts to create a new password before attempting to access Privilege Manager.

Setting up Azure AD integration with Privilege Manager requires steps in your Azure tenant and in Privilege Manager.

In Privilege Manager the Azure Active Directory Domain Foreign System requires the following from the Azure Portal:

- Tenant (this is the unique identifier of the Azure Active Directory instance)
- Application ID (an application registration in the directory instance)
- Client Secret (this is found in Certificates & Secrets in the Azure portal for the previously created application registration)

Setting up Azure AD Integration in Privilege Manager requires these components independent of On-premises or Cloud:

- User Credential
- An Azure Active Directory Domain Foreign System
- Executing a Privilege Manager Task (Import Users and Groups)
- Creating a Scheduled Task to synchronize the users and groups on a regular basis

Note: You do not need to have an active directory domain before you can sync with an Azure Active Directory. However, there are benefits for synchronizing on-premises Active Directory to Azure AD.

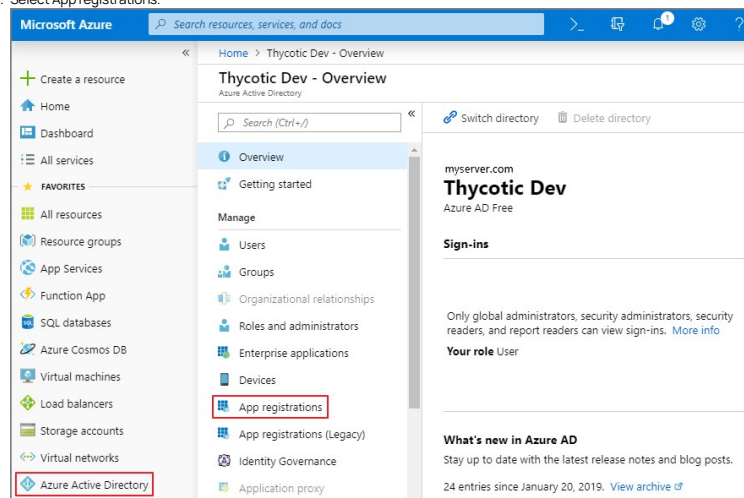
Prerequisites

Assign Azure user(s) to the Privilege Manager Administrators Role. In order for users to authenticate via Azure AD, they need to be members of various roles. There must be at least one member from your Azure Directory to be allowed to login via Azure AD before you can continue. We recommend adding yourself to ensure that you can login after the Authentication Provider is configured.

Setting up Azure AD with Privilege Manager

Steps In the Azure Portal

1. Navigate to your <https://portal.azure.com>
2. In your Azure portal, navigate to and open Azure Active Directory.
3. Verify you are in the right tenant or use the filter to switch.
4. Select App registrations.



5. Select **+ New registration**.
6. Under Register an application, enter
 1. an application **Name**
 2. select **Supported account types** based on your business requirements
 3. specify the following Redirect URI values using the URI of your Privilege Manager server: <https://myserver.example.com/TMS/>

Note: This URI does not need to be a publicly visible address. It is only used in redirecting the browser back to the Privilege Manager web application after authentication. For Privilege Manager Cloud subscriptions, the URI should be pointed to the URI that was set up for you, for example: <https://myassignedname.privilegemanagercloud.com/Tms/>

4. Click the **Register** button.
7. Navigate to your newly created application registration.
8. Select the **Authentication** option.
 1. Enter these additional URIs in the Redirect URI field (for Privilege Manager Cloud use `.../Tms/...`):
 - <https://myserver.example.com/TMS/Account/Signout/>
 - <https://myserver.example.com/TMS/Account/SignoutCallback/>
 2. In the Advanced Settings area, check the box labeled **ID tokens**.
9. Select the **API Permissions** option.
10. Click the **+ Add a permission** option to add the Microsoft Graph API.

Request API permissions

PREVIEW

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Office 365 Management APIs
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

Visual Studio Team Services
Integrate with Visual Studio Team

11. Select the **Application permissions** option for the type of permissions.
12. Open the **Directory category** and select the **Directory.Read.All** permission.

Request API permissions

PREVIEW

< All APIs

Microsoft Graph
<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
▶ AccessReview	
▶ Application	
▶ AuditLog	
▶ Calendars	
▶ Calls	
▶ ChannelMessage	
▶ Chat	
▶ Contacts	
▶ Device	
▼ Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All Read directory data	Yes
<input type="checkbox"/> Directory.ReadWrite.All Read and write directory data	Yes

▼ Domain

13. Click the **Add permissions** button at the bottom to finish this step.
14. Click the **+ Add a permission** option to add the **Azure Active Directory Graph API**.

Request API permissions

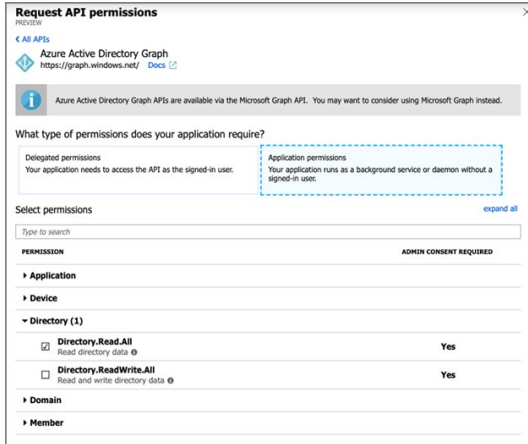
PREVIEW

Azure Batch Schedule large-scale parallel and HPC applications in the cloud	Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
Azure Data Explorer (with Multifactor Authentication) Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions	Azure Data Lake Access to storage and compute for big data analytic scenarios	Azure Import/Export Programmatic control of import/export jobs
Azure Rights Management Services Allow validated users to read and write protected content	Customer Insights Create profile and interaction models for your products	Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination
Dynamics 365 Business Central Programmatic access to data and functionality in Dynamics 365 Business Central	Dynamics CRM Access the capabilities of CRM business software and ERP systems	Dynamics ERP Programmatic access to Dynamics ERP data
Flow Service Embed flow templates and manage flows	Intune Programmatic access to Intune data	OneNote Create and manage notes, lists, pictures, files, and more in OneNote notebooks
Power BI Service Programmatic access to Dashboard resources such as Datasets, Tables, and Flows in Power BI	PowerApps Runtime Service Powerful data storage, modeling, security and integration capabilities	SharePoint Interact remotely with SharePoint data
Skype for Business Integrate real-time presence, secure messaging, calling, and conference capabilities	Speech Create powerful speech-enabled features using speech to text and text to speech conversion	Yammer Access resources in the Yammer web interface (e.g. messages, users, groups etc.)

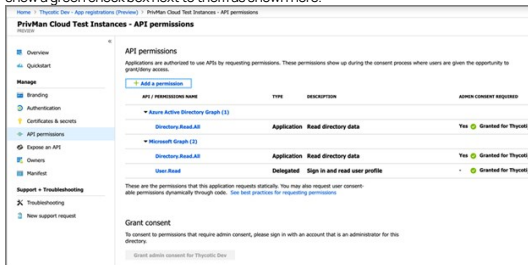
Supported legacy APIs

Azure Active Directory Graph Programmatic access to directory data and objects	Exchange A powerful, easy-to-use way to access and manipulate Exchange data
--	---

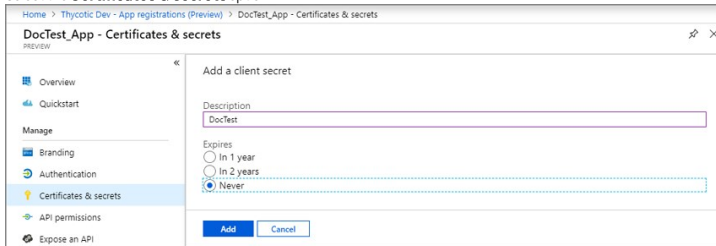
15. Select the **Application permissions** option for the type of permissions
16. Open the **Directory category** and select the **Directory.Read.All** permission.



- Click the **Add permissions** button at the bottom to finish this step.
- These permissions must be granted by the domain administrator before the application can use this registration. Click the **Grant admin consent for...** button to ensure these APIs are allowed. Once this is done, these permissions will show a green check box next to them as shown here.



- Select the **Certificates & secrets** option.



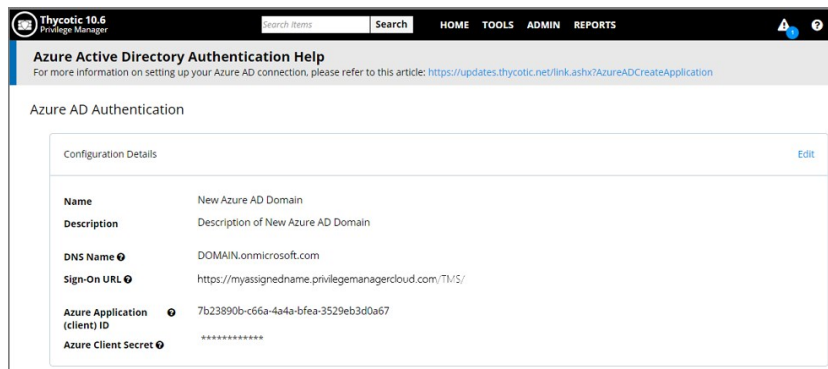
- Click **+ New client secret**.
- Add a **Description** and chose an **Expires** setting based on your business requirements.
- Click **Add** to create the secret.
- Use the **Click to copy** icon to copy the newly created secret to the clipboard.

You will need the Application Id and the Client Secret you copied to the clipboard in Privilege Manager to complete the setup.

Steps In your Privilege Manager Instance

Set-up Foreign Systems

- Select **Admin | Configuration**.
- Select the **Foreign Systems** tab.
- Select Azure Active Directory Domains.
- Select the **Add New** button at the top.
- Enter a Name and Description. Click the **Create** button.
- Select the newly created Azure AD Domain entry and click **Edit**.
- Enter the **DNS Name**. This is the DNS name of the Tenant from the Azure Portal identified at the beginning of this document.
- Verify the **Sign-on URL** is correct. This value should match what was specified in the Redirect URI option when setting up the Application Registration.
- Enter the **Azure Application (client) ID**. This is the Application ID that was created when registering your application in the Azure Portal.



10. Click **Save Changes**.

11. Continue to the Azure AD Authentication Provider section and click **Edit**.

12. Complete the three steps:

1. Import Users & Groups from Azure AD. This process may take a few minutes to complete, depending on the size of the directory. Privilege Manager offers two tasks for this import:

- **Default Import AzureAD Users/Groups**. imports ALL users and groups.
- **Import Specific Azure AD Users and Groups**. imports only the specified users and/or groups.

Refer to setup and scheduling of these tasks under the "Import Users and Groups via Privilege Manager Task" and "Create Scheduled Task for Users/Groups Synchronization" topics below.

2. Assign Azure user(s) to the Privilege Manager Administrators Role. In order for users to authenticate via Azure AD, they will need to be added as members of various roles. There must be at least one member from this Azure Directory allowed to login via Azure AD before you can continue. We recommend adding yourself to ensure that you can login after the Authentication Provider is configured.

3. Set as Authentication Provider.

13. Click **Save Changes**.

Viewing Imported Users and Groups

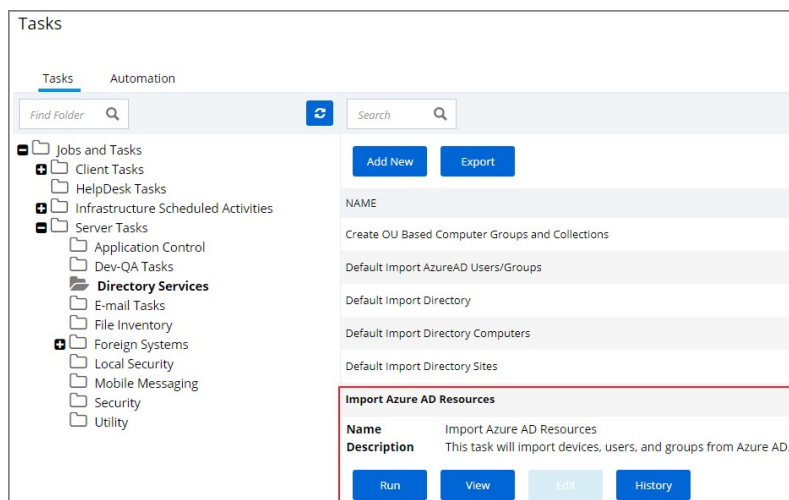
You may verify and browse the users and groups that are expected to be imported from Azure Active Directory.

1. In Privilege Manager, navigate to **Admin | Resources**.
2. Expand **Organizational Views**.
3. Expand **Default**.
4. Expand **All Resources**.
5. Expand **Security Principal**.
6. Select **Domain Users**. You should see a list that contains imported Azure AD users.
7. Select **User Group**. You should see a list that contains imported Azure AD groups (other groups may exist in the list as well).

Import Users and Groups via Privilege Manager Task

This step was performed initially as part of setting up the Azure AD directory. To re-import users and groups, you can perform that operation again to pick up changes that may have occurred in the directory, such as new users that have been added or group membership changes. To run this manually:

1. Navigate to **Privilege Manager | Admin | Tasks**
2. Expand **Jobs and Tasks**.
3. Expand **Server Tasks**.
4. Select **Directory Services**.



5. Click on **Import Azure AD Resources** to import devices, groups, and/or users based on a selected resource.
6. Click **Run**, then **Select Resource** and select from the available resources.

Task > Import Azure AD Resources

This item is read-only.

General Parameters Schedules

Directory

Import devices

Import groups

Import users

Back Edit Run Task History Create a Copy Export

7. Select the Azure Active Directory Domain you previously created.
 1. Enable **Import Devices**.
 2. Enable **Import Groups**.
 3. Enable **Import Users**.

8. Click **Run Task**

If you only want a subset of the directory to be imported, enable select and enable only the resources you wish to import at this point.

Create Scheduled Task for Users/Groups Synchronization

To schedule this operation to happen on a regular schedule:

1. Navigate to **Privilege Manager | Admin | Tasks**.
2. Expand **Jobs and Tasks**.
3. Expand **Server Tasks**.
4. Select **Directory Services**.
5. Click on **Import Azure AD Resources** to import devices, groups, and/or users based on a selected resource.
6. Click **View**.
7. In the Schedules tab, click **New Schedule** to create a new schedule.
 1. On the **Schedule** tab, define the desired schedule.
 2. On the **Parameters** tab, select the **Azure Active Directory** resource that you created earlier and make selections for importing devices, users, and groups.
8. Click **Save**.

- [Set-up an SMTP Server Connection](#)
- [Set-up a Cyance Connection](#)
- [Set-up a ServiceNow Ticketing Connection](#)
- [Set-up VirusTotal](#)
- [Set-up an SCCM Connection](#)
- [Set-up the SMP Integration](#)
- [Set-up Syslog](#)

Cylance is an Artificial Intelligence Based Advanced Threat Prevention Solution for enterprise environments. Privilege Manager (v10.5+) integrates with Cylance to help you proactively act on any unknown applications that run in your environment to prevent potential malware attacks. The steps below walk through how to setup a Cylance Integration in Privilege Manager and then create an example policy to begin using Cylance intelligence in action across your environment.

Keep in mind that while the Cylance integration provides insight into threat analysis, ultimately you can use Privilege Manager policies to act or react in whatever way makes most sense to your organization.

Cylance Connector Installation Steps (On-prem only)

1. Open a browser on your Privilege Manager Web Server, browse to [https://\[YourInstanceName\]/TMS/Setup/](https://[YourInstanceName]/TMS/Setup/)
2. On the Currently Installed Products screen, choose Install/Upgrade Products.
3. Select option Thycotic CylanceReputation Connector.
4. Click on **Install** and Accept the End User License Agreement. You will see your Installation Progress. Click on "Show install Logs" link to check for any errors
 - Note:** If the installation of Cylance initially fails, redirect to [https://\[YourInstanceName\]/TMS/Setup/](https://[YourInstanceName]/TMS/Setup/) and click the Repair button next to the Cylance Product.
5. Once the Installation is successful, click on the **Home** button.

Configuring the Cylance Connector

1. Navigate to **ADMIN | Configuration** and select the **Reputation** tab.
2. From the Select Rating Provider drop-down, select **Cylance Rating Provider**.

Configuration

General Discovery **Reputation** Credentials Foreign Systems Roles Advanced Authentication Cha

Select Rating Provider Cylance Rating Provider

Cylance administrators should add the Thycotic agent to the Cylance safe list. Review [Privilege Manager's documentation](#) on antivirus exclusions.

Credentials

Application Secret Show

Application ID Show

Settings

Tenant ID

Region North America

Edit

3. Click **Edit**.
4. Enter the required **Credentials** and **Settings** details. These details can be found in your Cylance account (login at protect.cylance.com).
 1. In our Cylance account, navigate to **Settings** and select **Integrations**. You find the **Tenant ID** on the right side of the Custom Applications area.

Settings

Application User Management Device Policy Global List Update Certificates **Integrations**

Custom Applications (4)

+ ADD APPLICATION

Tenant ID: Copy

Application	Read	Write	Modify	Delete	Actions
EdB.PrivMan.Integration	6	4	5	0	✎ 🗑️ ▼
test another one	9	6	0	0	✎ 🗑️ ▼
Demo Test	6	4	5	0	✎ 🗑️ ▼
PrivilegeManager.AppControl	6	4	5	0	✎ 🗑️ ▼

2. Select your Privilege Manager integration from the Custom Application list. You find the required **Application ID** and **Application Secret** on the left side of the page.

PrivilegeManager.AppControl Read | 6 Write | 4 Modify | 5 Delete | 0

Application ID: 314689f2-3afe-4182-bf25 [Copy](#) Application Secret: [REDACTED] [Copy](#) [Regenerate Credentials](#)

PRIVILEGE	READ	WRITE	MODIFY	DELETE
Devices	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Global Lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packages Configuration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packages Deployment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Policies	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Threats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Users	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Zones	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Focus Views	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS InstaQueries	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Rule Sets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Commands	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Exceptions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Policies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Rules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CylanceOPTICS Detections	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Once the Cylance details are entered in Privilege Manger, click **Save**.

Create a Cylance Security Rating Filter

1. Navigate to **ADMIN | More** and select **Filters**.
2. Click **Add Filter**.
3. From the **Platform** drop-down select either Windows or macOS.
4. From the **Filter Type** drop-down select **Security Rating Filter**.
5. Name the policy and add a Description.
6. Next to **Security Rating System**, click **Application Control Rating System**.

New Filter

Filter Details

Platform * Windows

Filter Type * Security Rating Filter

Name * Test Security Rating Filter

Description Filter to test security rating integration

Security rating system [View Parameters](#)
* Application Control Rating System

[Back](#) [Create](#)

7. Click the **+** next to Cylance Rating System to add the system.

New Filter

Filter Details

Platform * Windows

Filter Type * Security Rating Filter

Name * Test Security Rating Filter

Description Filter to test security rating integration

Security rating system [View Parameters](#)

*Application Control Rating System

Select	Name	Resource Type	Description
<input type="checkbox"/>	Application Control Rating System	Security Rating	Application Control Rating System
<input type="checkbox"/>	Cylance Rating System	Security Rating	Security Rating System for Application Control Cylance
<input type="checkbox"/>	VirusTotal Rating System	Security Rating	Security Rating System for Application Control VirusTotal

10 items per page

Close Clear

Back Create

8. Click **Create**

9. Click **Edit** to select the **Rating Level** you wish to apply, the options are:

- Unclassified
- Whitelist
- Greylist
- Blacklist

You can also specify a Timeout value and Error Handling conditions on timeout and/or on failure, the options are:

- Matched
- Not Matched

10. Click **Save**.

Create a Cylance Policy

After your Filter is created,

1. Navigate to **ADMIN | Policies** and click **Add New Policy**.

2. If you created a Windows filter, as we did in the example above, select Windows from the **Platform** drop-down. 1. From the **Policy Type** drop-down select a template that matches what you are trying to do, for example deny an application execution based on a bad security rating. Here we select Deny Application Execution.

New Policy

Platform * Windows

Policy Type * Show All Templates

Template Type * Blacklist: Deny Specific Applications

Name * Test Deny Application Execution Policy

Description Test security rating policy prevents processes from running.

Back Create

3. Enter a name and description.

4. Click **Create**.

5. Click **Edit**.

6. On the General tab, select the **Enabled** checkbox. And adjust any other settings like the priority. Deny policies should have low priorities.

7. Select the **Conditions** tab, then select **Add Application Target**.

8. Search for the Cylance filter created earlier. Select that filter and click **Add**.

General **Conditions** Actions Policy Enforcement Deployment Change History

Select the applications to control along with any optional criteria.

When no filters are chosen for APPLICATION TARGETS or INCLUSION FILTERS, this policy will apply to **ALL** applications except those explicitly excluded.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

ADD APPLICATION TARGET

Select an Application Target from the folders below. Use the [Application Target](#) page to define more.

View by: List

NAME	TYPE	FOLDER
<input checked="" type="checkbox"/> Test Security Rating Filter	Security Rating Filter	Windows Filters
<input type="checkbox"/> Test SMP Package Contents Filter	File Parameter Collection	Windows Filters
<input type="checkbox"/> Test Virtual Disk File Contents Filter	File Parameter Collection	Windows Filters
<input type="checkbox"/> Test Virtual Disk Package Contents Filter	File Parameter Collection	Windows Filters
<input type="checkbox"/> test.bat	Win32 Exe Filter	Windows Filters
<input type="checkbox"/> test.msi	Win32 Exe Filter	Windows Filters
<input type="checkbox"/> test.ps1	Win32 Exe Filter	Windows Filters

Add Cancel

9. On the Actions tab, add an appropriate Action to be taken.

General **Conditions** Actions Policy Enforcement Deployment Change History

Select the applications to control along with any optional criteria.

When no filters are chosen for APPLICATION TARGETS or INCLUSION FILTERS, this policy will apply to **ALL** applications except those explicitly excluded.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

ADD APPLICATION TARGET

Select an Application Target from the folders below. Use the [Application Target](#) page to define more.

View by: List

NAME	TYPE	FOLDER
<input checked="" type="checkbox"/> Test Security Rating Filter	Security Rating Filter	Windows Filters
<input type="checkbox"/> Test SMP Package Contents Filter	File Parameter Collection	Windows Filters
<input type="checkbox"/> Test Virtual Disk File Contents Filter	File Parameter Collection	Windows Filters
<input type="checkbox"/> Test Virtual Disk Package Contents Filter	File Parameter Collection	Windows Filters
<input type="checkbox"/> test.bat	Win32 Exe Filter	Windows Filters
<input type="checkbox"/> test.msi	Win32 Exe Filter	Windows Filters
<input type="checkbox"/> test.ps1	Win32 Exe Filter	Windows Filters

Add Cancel

10. Click **Save**.

Privilege Manager integrates with Microsoft System Center Configuration Manager (SCCM) to allow the

- [import of computers](#) for use in computer groups and identifying systems that exist on the network, but don't have an endpoint agent installed yet.
- [import of existing Device Collections](#) from SCCM and use them for Privilege Manager computer groups.
- [inventory of SCCM Software Packages](#) to use the package contents in Privilege Manager Application Control policies.

Create a Credential

Privilege Manager needs a username and password to access SCCM. If you have not already created an appropriate user credential:

1. Navigate to **Admin | Configuration | User Credentials**.
2. Click **Add New**, to create user credentials to access SCCM.
3. After entering the user credentials information for SCCM, click **Save Changes**.

Connecting to SCCM

Before you can import data from SCCM you need to setup a foreign systems connection in Privilege Manager for the SCCM integration.

1. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
2. Select **System Centre Configuration Manager**. If this is not listed, make sure the connector is installed by verifying via the Privilege Manager Add/Upgrade Features page.
3. Click **Add New**.

The screenshot shows the 'Configuration' page with the 'Foreign Systems' tab selected. Under the 'System Centre Configuration Manager' section, there is an 'Add New' button. Below it are two input fields: 'Name' with the value 'New SCCM Server' and 'WMI Namespace' with the value '\\[ServerName]\ROOT\SMS\site_[SiteName]'. There are 'Cancel' and 'Create' buttons below the fields. At the bottom of the form, there is a table with columns 'NAME', 'DESCRIPTION', 'LAST MODIFIED BY', and 'LAST MODIFIED'. The table contains one row with the text 'No System Centre Configuration Manager exist, please create one'. A 'Back' button is located at the bottom left of the form.

4. Enter the name of the SCCM Server and provide the **WMI Namespace of the SCCM Site**.
5. Click **Create**.
6. Select the newly created SCCM foreign system and click **Edit**.
7. Under Settings select the SCCM user credential that you created in the previous procedure.
8. Click Save.

Import Computers

Before you can import collection data from SCCM, Privilege Manager needs to know about computers in your SCCM.

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | SCCM**.
3. Click **SCCM Sync Computers**.

Tasks

The screenshot shows the 'Tasks' interface. On the left is a 'Find Folder' search bar and a tree view containing folders like 'Jobs and Tasks', 'Client Tasks', 'HelpDesk Tasks', 'Infrastructure Scheduled Activities', 'Server Tasks', 'Application Control', 'Directory Services', 'E-mail Tasks', 'File Inventory', 'Foreign Systems', 'SCCM', 'ServiceNow', 'Symantec Management Platform', 'Local Security', 'Mobile Messaging', 'Security', and 'Utility'. On the right, there is a 'Search' bar and buttons for 'Add New' and 'Export'. Below this, a task is displayed with fields for 'NAME' (SCCM Sync Collection), 'SCCM Sync Collections', and 'SCCM Sync Computers'. The 'SCCM Sync Computers' task has a 'Name' field with 'SCCM Sync Computers' and a 'Description' field with 'Imports all computers from SCCM into Privilege Manager'. At the bottom of the task details are buttons for 'Run', 'View', 'Edit', and 'History'.

4. Click **Run**.
5. Select your SCCM system via the **Select resource...** option.

Task > Synchronize Computers

The screenshot shows the 'Settings' page for the 'Synchronize Computers' task. It includes a 'Task Name' dropdown menu set to 'Interactive run on Thu Oct 24 2019', a 'Maximum concurrent branches' input field with the value '10', and an 'SCCM System ID' dropdown menu with a 'Select resource...' option. At the bottom of the settings are buttons for 'Back', 'Run Task', 'View', and 'History'.

6. Click **Run Task**

Verify the Computers have been Imported (optional)

1. Navigate to **Admin | More** and select **Resources**.
2. Open the **Resources** tab.
3. In the folder tree open **Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
4. Select a computer from that list.
5. Select the Known Data tab in the computer resource explorer view.
6. In the tree under **Foreign Systems**, you should have the Foreign System Id and SCCM Platform Id data.

Create a Collection

After computers have been imported, you can create a collection to mirror an SCCM collection.

1. Navigate to Resources, open the **Resource Filters** tab.
2. In the folder tree under **Resource Filters** open **Collections | System Center Configuration Manager**.
3. Click **Add New**
4. Enter a Name and Description, and specify the SCCM instance to connect to.

The screenshot shows the 'Resource Filters' interface. On the left is a 'Find Folder' search bar and a tree view containing folders like 'Resource Filters', 'Collections', 'MacOS', 'Symantec Management Platform', 'System Centre Configuration Manager', 'Thyrotic', 'Windows', and 'Resource Targets'. On the right, there is a 'Search' bar and an 'Add New' button. Below this, a dialog box is open for creating a new collection. It has fields for 'Name' (New SCCM Collection), 'Description' (SCCM Collection), and 'SCCM Instance' (with a 'Select resource...' option). At the bottom of the dialog are buttons for 'Cancel' and 'Create'.

5. Click **Create**.
6. Click **Edit**.
7. Select the Filter Definition tab and under **Foreign Collection** select the Collection target.

Resource Filter > New SCCM Collection

General **Filter Definition** Membership

Foreign Collection

Foreign System: PrivManGroup1

Foreign Collection: SCCM Collections Tree

- SCCM Collections Tree
 - All Systems
 - All Users
 - All User Groups
 - All Users and User Groups
 - All Custom Resources
 - All Unknown Computers
 - All Mobile Devices
 - All Desktop and Server Clients
 - PrivManGroup1

Buttons: Save, Cancel, Export

8. Click **Save**.

9. Click the **Sync Foreign Collection** to update the membership immediately. The foreign collection update can also be scheduled by following the link in the help tip.

Resource Filter > New SCCM Collection

General **Filter Definition** Membership

Foreign Collection

Sync Foreign Collection

Foreign System: PrivManGroup1

Foreign Collection: PrivManGroup1

Buttons: Back, Edit, Create a Copy, Delete, View as XML, Export

10. Select the Membership tab and then click the **Update Membership** tab to see the current membership of this collection.

Inventory Software Packages

Once the Foreign System has been created, an on-demand packages synchronization can be run and/or a regular synchronization schedule can be set-up via the following steps:

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | SCCM**.
3. Click **SCCM Sync Packages**.

Tasks

Tasks Automation

Find Folder Search

- Jobs and Tasks
 - Client Tasks
 - HelpDesk Tasks
 - Infrastructure Scheduled Activities
 - Server Tasks
 - Application Control
 - Directory Services
 - E-mail Tasks
 - File Inventory
 - Foreign Systems
 - SCCM**
 - ServiceNow
 - Symantec Management Platform
 - Local Security
 - Mobile Messaging
 - Security
 - Utility

Buttons: Add New, Export

NAME: SCCM Sync Collection, SCCM Sync Collections, SCCM Sync Computers

SCCM Sync Packages

Name: SCCM Sync Packages

Description: Imports or updates all SCCM packages into Privilege Manager

Buttons: Run, View, Edit, History

4. Click **Run**.

5. Select your SCCM system via the **Select resource...** option.

Task > SCCM Sync Packages

Settings

Task Name

SCCM System ID

[Back](#) [Run Task](#) [View](#) [History](#)

6. Click **Run Task**

Alternatively the **SCCM Sync Packages** task can be scheduled to regularly repeat. When viewing the task, navigate to the Schedules tab and create a new schedule.

Create a SCCM Package Content Filter

After the Package Synchronization completes the SCCM Packages can be used in application control policies via package content filters.

1. Navigate to **Admin | Filters**.
2. Click the **Add Filter** button.
3. From the Platform drop-down select Windows.
4. From the Filter Type drop-down scroll to Inventory Filters and select the **Package Contents Filter**.
5. Set the Name and Description of the filter.
6. Click **Create**.
7. Click **Edit**.
8. Next to Package, click **Select resource...**
9. Select the package from SCCM that will be targeted.
10. Set the Results will be to **Included**.

File Parameter Collection Filter > New Package Contents Filter

[Details](#) [Membership](#) [Related Items](#) [Change History](#)

Details

Name

Description

Platform

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source

Package

Results Will Be Included Excluded

[Save](#) [Cancel](#) [Export](#)

11. Navigate to the **Membership** tab.
12. If no items are listed in the membership table, click the **Sync Package** button.

File Parameter Collection Filter › New Package Contents Filter

Details **Membership** Related Items Change History

i This collection was last updated at Oct 25, 2019, 12:20:37 AM. To force an immediate update, click Update Membership

Update Membership Sync Package **i**

View All Files Picker Report

File Name	Product Name	Version
<input type="text"/>	<input type="text"/>	<input type="text"/>

No records available.

◀ ◁ ▷ ▶ 10 items per page

Save Cancel Export

Running the sync package task, causes the server to inventory the package referenced in the filter. If you have multiple filters and packages, Thycotic recommends to use the *Inventory Packages Referenced in Whitelists* task instead.

13. Click **Save**.

This filter can then be referenced in Application Control policies.

Privilege Manager integrates with the Symantec Management Platform (SMP) to allow the

- [import of computers](#) for use in computer groups and identifying systems that exist on the network, but don't have an endpoint agent installed yet.
- [import of existing Resource Collections](#) from SMP and use them for Privilege Manager policy targets.
- [inventory of SMP Software Packages](#) to use the package contents in Privilege Manager Application Control policies.

Create a Credential

Privilege Manager needs a username and password to access SMP. If you have not already created an appropriate user credential:

1. Navigate to **Admin | Configuration | User Credentials**.
2. Click **Add New**, to create user credentials to access SMP.
3. After entering the user credentials information for SMP, click **Save Changes**.

Connecting to SMP

Before you can import data from SMP you need to setup a foreign systems connection in Privilege Manager for the SMP integration.

1. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
2. Select **Symantec Management Platform**. If this is not listed, make sure the connector is installed by verifying via the Privilege Manager Add/Upgrade Features page.
3. Click **Add New**.

The screenshot shows the 'Configuration' page with the 'Foreign Systems' tab selected. Under the 'Symantec Management Platform' section, there is an 'Add New' button. Below it, a form is visible with the following fields:

- Name:** A dropdown menu with 'New Notification Server' selected.
- Base Uri:** A text input field with 'http://{ServerName}/Altiris/' entered.

There are 'Cancel' and 'Create' buttons below the form. Below the form is a table with columns: NAME, DESCRIPTION, LAST MODIFIED BY, and LAST MODIFIED. The table is currently empty, with a message: 'No Symantec Management Platform exist, please create one'. A 'Back' button is located at the bottom left of the table area.

4. **Name** the Symantec Management Platform and provide the **URL of the Altiris console**.
5. Click **Create**.
6. Select the newly created SMP foreign system and click **Edit**.
7. Under Settings select the SMP user credential that you created in the previous procedure.
8. Click Save.

Import Computers

Before you can import collection data from SMP, Privilege Manager needs to know about computers in your SMP.

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Symantec Management Platform**.
3. Click **SMP Sync Computers**.

Tasks

The screenshot shows the 'Tasks' page in Privilege Manager. The left sidebar contains a folder tree with the following structure:

- Jobs and Tasks
 - Client Tasks
 - HelpDesk Tasks
 - Infrastructure Scheduled Activities
 - Server Tasks
 - Application Control
 - Directory Services
 - E-mail Tasks
 - File Inventory
 - Foreign Systems
 - SCCM
 - ServiceNow
 - Symantec Management Platform**
 - Local Security
 - Mobile Messaging
 - Security
 - Utility

The main content area shows the details for the 'SMP Sync Computers' task. It includes a search bar, 'Add New' and 'Export' buttons, and a table with the following information:

NAME	DESCRIPTION
SMP Sync Collection	
SMP Sync Collections	
SMP Sync Computers	
Name	SMP Sync Computers
Description	Imports all computers from SMP into Privilege Manager

Below the table are buttons for 'Run', 'View', 'Edit', and 'History'. At the bottom, there is a section for 'SMP Sync Packages'.

4. Click **Run**.

5. Select your SMP system via the **Select resource...** option.

Task > New SMP Synchronise Computers Task

Settings

Task Name

Maximum concurrent branches

SMP Instance ID [Select resource...](#)

[Back](#) [Run Task](#) [View](#) [History](#)

6. Click **Run Task**

Verify the Computers have been Imported (optional)

1. Navigate to **Admin | More** and select **Resources**.
2. Open the **Resources** tab.
3. In the folder tree open **Organizational Views | Default | All Resources | Asset | Network Resource | Computer**.
4. Select a computer from that list.
5. Select the Known Data tab in the computer resource explorer view.
6. In the tree under **Foreign Systems**, you should have the Foreign System Id and SMP Platform Id data.

Create a Collection

After computers have been imported, you can create a collection to mirror an SMP collection.

1. Navigate to Resources, open the **Resource Filters** tab.
2. In the folder tree under **Resource Filters** open **Collections | Symantec Management Platform**.
3. Click **Add New**
4. Enter a Name and Description, and specify the SMP instance to connect to.

The screenshot shows the 'Resource Filters' dialog box with the 'Resources' tab selected. The left sidebar shows a tree view with 'Resource Filters' expanded to 'Collections' > 'Symantec Management Platform'. The main area is titled 'Add New' and contains the following fields:

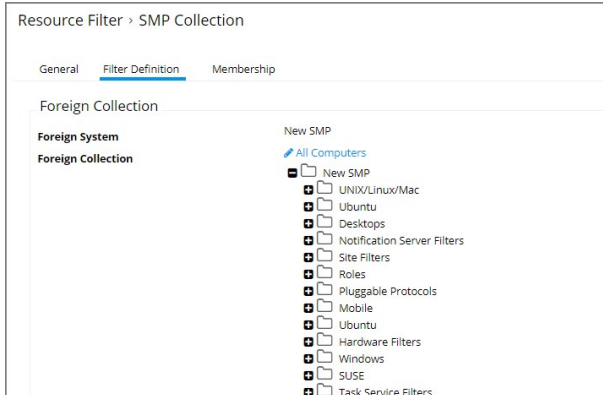
- Name:** New SMP Collection
- Description:** SMP Collection
- Symantec Management Server:** Select resource... (dropdown menu)

Below these fields is a table with the following columns: Select, Name, Resource Type, Description, and CreatedDate.

Select	Name	Resource Type	Description	CreatedDate
<input type="checkbox"/>	sm			month/day/y...
<input checked="" type="checkbox"/>	New SMP	Symantec Management Platform		10/1/19, 11:59 AM

At the bottom of the table, it shows '10 items per page' and '1 - 1 of 1 Items'. There are 'Close' and 'Clear' buttons below the table, and 'Cancel' and 'Create' buttons at the bottom of the dialog.

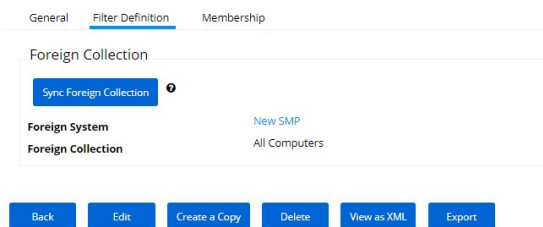
5. Click **Create**.
6. Click **Edit**.
7. Select the Filter Definition tab and under **Foreign Collection** select the Collection target.



8. Click **Save**.

9. Click the **Sync Foreign Collection** to update the membership immediately. The foreign collection update can also be scheduled by following the link in the help tip.

Resource Filter > SMP Collection



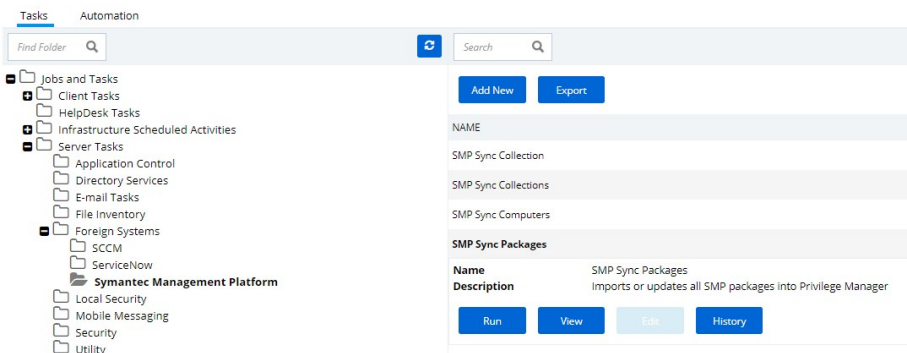
10. Select the Membership tab and then click the **Update Membership** tab to see the current membership of this collection.

Inventory Software Packages

Once the Foreign System has been created, an on-demand packages synchronization can be run and/or a regular synchronization schedule can be set-up via the following steps:

1. Navigate to **Admin | More** and select **Tasks**.
2. On the Tasks tab open the folder tree and select **Server Tasks | Foreign Systems | Symantec Management Platform**.
3. Click **SMP Sync Packages**.

Tasks



4. Click **Run**.

5. Select your SMP system via the **Select resource...** option.

Task > SMP Sync Packages

Settings

Task Name * Interactive run on Fri Oct 25 2019
[View Parameters](#)

SMP System ID * Select resource...

[Back](#) [Run Task](#) [View](#) [History](#)

6. Click **Run Task**

Alternatively the **SMP Sync Packages** task can be scheduled to regularly repeat. When viewing the task, navigate to the Schedules tab and create a new schedule.

Create a SMP Package Content Filter

After the Package Synchronization completes the SMP Packages can be used in application control policies via package content filters.

1. Navigate to **Admin | Filters**.
2. Click the **Add Filter** button.
3. From the Platform drop-down select Windows.
4. From the Filter Type drop-down scroll to Inventory Filters and select the **Package Contents Filter**.
5. Set the Name and Description of the filter.
6. Click **Create**.
7. Click **Edit**.
8. Next to Package, click **Select resource...**
9. Select the package from SMP that will be targeted.
10. Set the **Results will be to Included**.

File Parameter Collection Filter > New Package Contents Filter

Details Membership Related Items Change History

Details

Name * New Package Contents Filter

Description Filters files contained in the specified package

Platform Windows

Settings

This filter will check for the existence of a file that is a member of the following collection.

Data Source * Package Contents Query

Package [View Parameters](#)
 * Thycotic Application Control Agent

Results Will Be
 Included
 Excluded

[Save](#) [Cancel](#) [Export](#)

11. Navigate to the **Membership** tab.

12. If no items are listed in the membership table, click the **Sync Package** button.

File Parameter Collection Filter › New Package Contents Filter

Details **Membership** Related Items Change History

i This collection was last updated at Oct 25, 2019, 12:20:37 AM. To force an immediate update, click Update Membership

Update Membership **Sync Package** **i**

View All Files Picker Report ▾

File Name	Product Name	Version
<input type="text"/>	<input type="text"/>	<input type="text"/>

No records available.

◀ ◁ ▷ ▶ 10 items per page

Save **Cancel** **Export**

Running the sync package task, causes the server to inventory the package referenced in the filter. If you have multiple filters and packages, Thycotic recommends to use the *Inventory Packages Referenced in Whitelists* task instead.

13. Click **Save**.

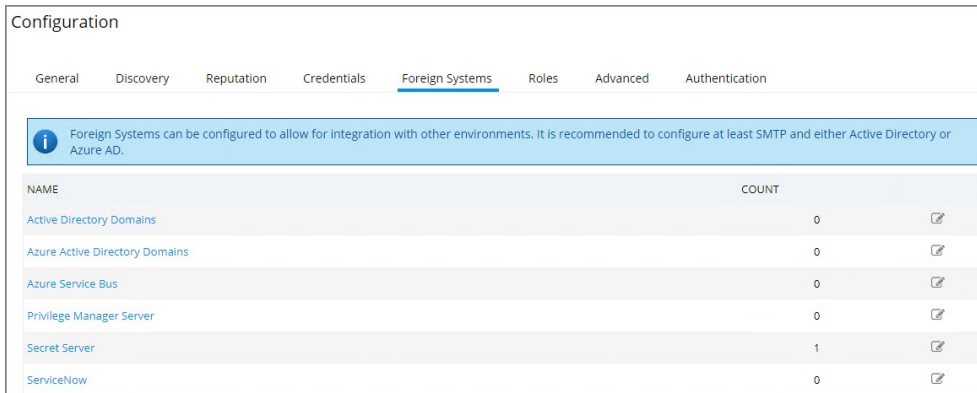
This filter can then be referenced in Application Control policies.

Here are the steps to integrate Workflow between your ServiceNow Ticketing System and Privilege Manager.

1. Verify which ServiceNow User account you will use for your integration with Privilege Manager. If you decide to create a new user account to manage your approval requests, make sure that it includes the required roles for your environment:
 - o Web Service Admin (web_service_admin) and
 - o Approval Admin (approval_admin).
 - o For ServiceNow MID Server environments, the mid_server role permission also needs to be added to the account.

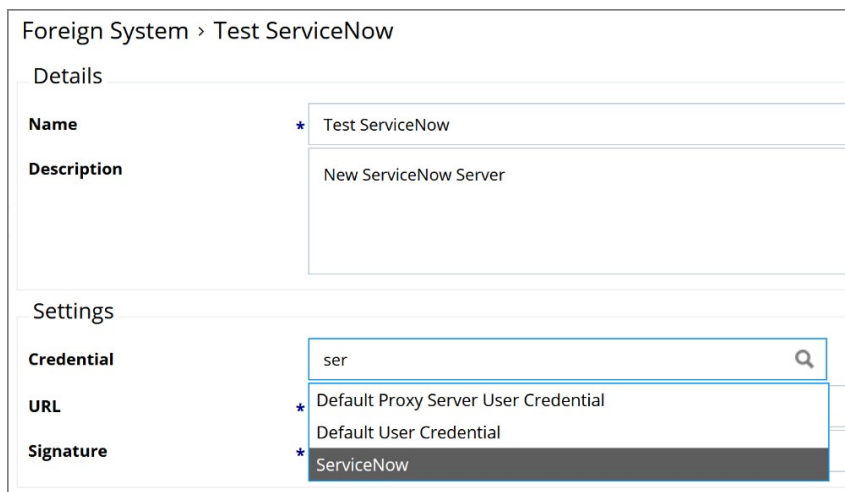
Refer to [ServiceNow product documentation](#).

2. Verify that the ServiceNow connector is installed for your Privilege Manager Cloud instance:
 1. In the Privilege Manager console navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
 2. If the connector is installed, **ServiceNow** is listed under Foreign System.



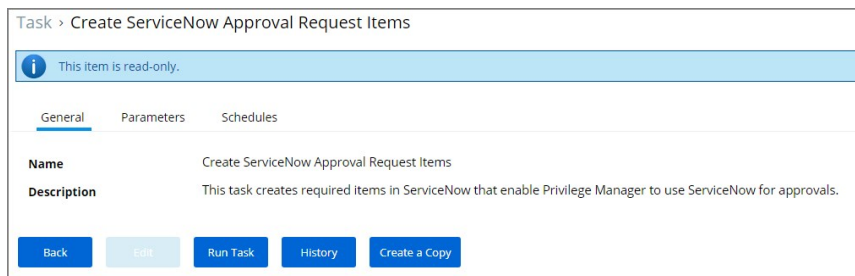
Note: If you are a 10.6 cloud customer and don't see ServiceNow in the list, contact Thycotic support to have the connector added to your cloud instance. If it is listed, continue with the next step.

3. Select the **Credentials** tab.
4. Click **Add New**.
5. Under Details, enter a Name and Description for your ServiceNow credentials.
6. Under Settings, enter the information from your ServiceNow User account that was referenced in step 1 above, click Save.
7. Select the **Foreign Systems** tab.
8. Select the **ServiceNow** link from the list of foreign systems displayed.
9. Click **Add New**.
10. Enter a Name for your Service Now Server.
11. Enter the base Uri from your ServiceNow instance
[https://\[InstanceName\].service-now.com/](https://[InstanceName].service-now.com/), click **Create**.
12. Select your ServiceNow instance, click **Edit**.
13. Assign the credentials you created to link them to your instance.



14. Next, in **Search** at the top of your Privilege Manager console, search for *Create ServiceNow Approval Request Items*.

15. In your search results, **click on this task** and then the **Run Task** button.



16. Under Task Settings, click **Select resource** and add the ServiceNow Server that you created as a Foreign System in step 10.

17. Click **Run Task**

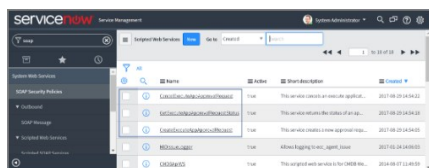
Note: Clients with robust ServiceNow installations are welcome (and in fact encouraged) to alter their ServiceNow scripted web services for use with their own ServiceNow items and workflow rather than relying on this importing task.

The task you just ran creates several new items in your ServiceNow dashboard.

ServiceNow Steps

Open ServiceNow and navigate to **Scripted Web Services | Scripted SOAP Services** to verify that these three new options are listed:

- CancelExecuteAppApprovalRequest,
- CreateExecuteAppApprovalRequest,
- GetExecuteAppApprovalRequestStatus

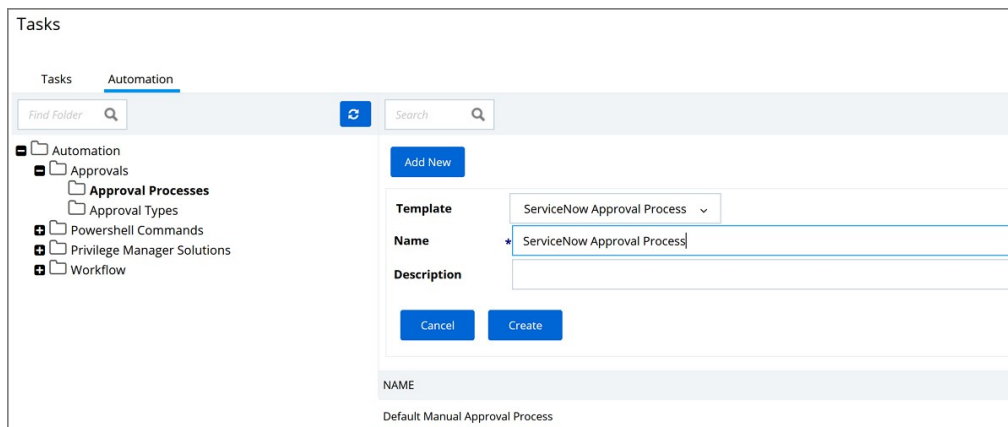


Now you've successfully defined a SOAP endpoint that Privilege Manager knows how to call to initiate a ServiceNow request for approval.

Define Action and Policy

You need to create an action and attach it to a policy to manage what events you want sent to ServiceNow for approvals. To do this,

1. In the Privilege Manager console, navigate to **Admin | More** and select **Tasks**.
2. Click the **Automation** tab.
3. In the tree navigate to **Automation | Approvals | Approval Processes**, click **Add New**.



4. Enter a name and description, click **Create**.

5. Click **Edit** on the newly created ServiceNow Approval Process.

Service Now Approval Process > ServiceNow Approval Process

Details

Name * ServiceNow Approval Process

Description

Settings

ServiceNow Server * Te

Check request status every * Test ServiceNow

Timeout after * 5 Minute(s)

Show Advanced

Save Cancel

- Under **Settings** specify your ServiceNow Server, click **Save**.
- Back in the Automation tree, select **Approval Types**, click **Edit** for the default.

Tasks

Tasks Automation

Find Folder Search

- Automation
 - Approvals
 - Approval Processes
 - Approval Types**
 - PowerShell Commands
 - Privilege Manager Solutions
 - Workflow

Add New

NAME

Default Execute Application Request Type

Name Default Execute Application Request Type

View Edit

Default Offline Execute Application Request Type

- Select your **ServiceNow Approval Process**, click **Save**.

Approval Process > Default Execute Application Request Type

Details

Name * Default Execute Application Request Type

Description

Settings

Characteristics

Policy Specific

File Specific

Options

Security Rating System(s) + Add None Selected

Process Handler Ser

ServiceNow Approval Process

Save Cancel

- Now navigate to **Admin | Actions**.
- Search and select **Approval Request (with ServiceNow Request ItemNumber) Form Action**.

Action > Approval Request (with ServiceNow Request Item Number) Form Action

i This item is read-only.

Details Related Items

Details

Name Approval Request (with ServiceNow Request Item Number) Form Action

Description This action will display a approval request form for approval before allowing application to run.

Settings

Require authentication:


By the interactive end-user

By a member of the group:

Approval type Default Execute Application Request Type

Window Design

Message prompt logo



Back Edit Create a Copy View as XML

11. Click **Create a Copy**.
12. Name your new action and click **Create**.
13. Click **Edit**.
14. Customize the Action based on your specific business requirements.
15. Click **Save**.
16. Navigate to **Admin IPolicies**, click **Create New** or find an existing policy that you want to use for ServiceNow Approvals.
17. Select the **Actions** tab.
18. Click **Edit** and **Add Action**.
19. Search for the action you created in step 5, *ServiceNow Approval Request Form Action*, click **Add**.
20. Click **Save**.
21. Select the **Deployment** tab.
22. Click **Run Policy Targeting Update** to immediately send the policy to your endpoint agents.

Policies also automatically update according to a schedule.

Integration Workflow

Now that you have a policy attached to your ServiceNow integrated Action, the requests from your policy will be sent through ServiceNow for approval.

1. On your endpoint, perform the action that your policy targets for ServiceNow Approval. You will be prompted with a justification window to explain your request. To approve these requests, open your ServiceNow Dashboard.
2. Go to **MyApprovals** in ServiceNow and you will see your new requests.
3. Click Requested for details.
4. In the Request page you will be able to view details of what action is being requested, and you can Accept the action.
5. On your endpoint, the pending justification window will update to an Approved status, and the user will be able to access their requested application.

Create Approval Request Items Task

Privilege Manager integrates with ServiceNow to manage approvals for user-requested application execution and elevation. For this integration to work there are several items that must be created in your ServiceNow instance. You can create these items manually or run the Create ServiceNow Approval Request Items task in Privilege Manager to create them automatically.

Most of the items created automatically by the Create ServiceNow Approval Request Items task are generic, and you are encouraged to replace these items with their own, and use your own workflows, forms, etc. This document describes what default items this task creates, and what is required for the integration to work so that you can adjust according to your own ServiceNow system.

How to create ServiceNow Approval Request Items Task

When you run the Create ServiceNow Approval Request Items task, Privilege Manager creates the necessary items in ServiceNow so that it can use ServiceNow to manage requests to approve execution or elevation of applications. This section describes each item and their functions:

Thycotic:

The task creates a service catalog category named "Thycotic" within your ServiceNow UI.

Execute Application Request:

The task creates a service catalog item named "Execute Application Request" and associates it with the Thycotic service catalog category.

Variables

PMApprovalId	The Privilege Manager internal identifier for the approval request
--------------	--

PMInitiatorId	The Privilege Manager internal identifier for the user that initiated the request
PMInitiatorName	The name of the user that initiated the request
PMPolicyId	The Privilege Manager internal identifier for the policy associated with the approval request
PMPolicyName	The name of the policy associated with the approval request
PMAgentId	The Privilege Manager internal identifier for the endpoint on which the request was initiated
PMAgentName	The name of the endpoint on which the request was initiated
PMProcessId	The Privilege Manager internal identifier for the process configuration item associated with the approval request
PMProcessName	The name of the process configuration item associated with the approval request
PMFilePath	The path to the application the user is attempting to run
PMUserReason	The reason given by the user requesting the approval

CreateExecuteAppApprovalRequest

The task creates a scripted SOAP service named "CreateExecuteAppApprovalRequest." When a user initiates an approval request, Privilege Manager will call this service with input data about the request. The default script will create a new Execute Application Request service catalog item, fill out the variable data from the inputs, and submit the item. The service returns the ID of the item to Privilege Manager so that it can periodically check or update the status of the item.

Script Input

The task creates inputs with the same names as the Variables in Execute Application Request listed above

Script Output

The task creates an output named "PMRequestId." Privilege Manager looks for this output by name and records it so can be used in future service calls to check or update the request status.

GetExecuteAppApprovalRequestStatus

The task creates scripted SOAP service named "GetExecuteAppApprovalRequestStatus." When an approval is in progress, Privilege Manager will periodically call this service to determine if the request has been approved or rejected.

Script Input

The task creates an input named "PMGetRequestId." Privilege Manager supplies this input using the value from PMRequestId that was output from the CreateExecuteAppApprovalRequest service.

Script Output

PMApprovalStatus	Privilege Manager expects this service to return PMApprovalStatus with one of the following values:
	approved: The request has been approved
	rejected: The request has been rejected
	pending: The request is still pending approval or rejection
	invalid: PMGetRequestId is not a valid ID, or the approval request is in an otherwise invalid state and will be rejected by Privilege Manager.
PMComment	If there is a comment by the worker that approved or rejected the request, it can optionally be returned in the output named PMComment. If this output is present Privilege Manager will record it with the status of the request in its database

CancelExecuteAppApprovalRequest

The task creates a scripted SOAP service named "CancelExecuteAppApprovalRequest." If a request is canceled or times out from within Privilege Manager, Privilege Manager will call this service to cancel the corresponding item in ServiceNow.

NOTE: Privilege Manager expects this service to be defined in ServiceNow, but the default script associated with the service does nothing.

Inputs

PMCancelRequestId	Privilege Manager call this service with PMCancelRequestId set to the value from PMRequestId returned from the CreateExecuteAppApprovalRequest service.
PMCancelComment	Privilege Manager calls this service with PMCancelComment set to a comment about why the request is being canceled.

Outputs

The task creates the output named **TmsCancelResult**. Privilege Manager expects an output with this name, but currently ignores the value.

Required Integration Points

What Can Change vs. What Must Remain

Most of the ServiceNow back end can be changed to accommodate your own items and workflows. Privilege Manager only requires the three scripted SOAP web services described above. You are welcome to change the script within the services to do whatever is necessary for your environment.

While the inputs that Privilege Manager sends to the services are fixed, once they reach ServiceNow you are free to do (or not do) what you want with the values.

Privilege Manager expects the outputs from the services as described above. PMRequestId is by default the ServiceNow sys_id of the requested service catalog item instance, but can be any string up to 256 characters used to identify the request. It's up to you to ensure that the status and cancel services can interpret that value.

You can change the names of the services if you update the names in the ServiceNow Approval Process configuration in Privilege Manager. You can also create multiple ServiceNow Approval Process items within Privilege Manager, and each can reference their own set of services.

Simple Mail Transfer Protocol (SMTP) is the Internet standard for email transmission. Often organizations use an SMTP Server – or a server that is specifically dedicated to transmitting email messages via TCP Port 25 – and in order to send email alerts with Privilege Manager policies, you must ensure that your email server is connected to Privilege Manager.

SMTP In Cloud Environments

Starting with version 10.7.1 of Privilege Manager Cloud, the SMTP foreign system is automatically configured with the email server information as provided during the cloud instance set-up. The information can be added/changed following the initial set-up.

Configuring the SMTP Connection

To set up the connection, follow these steps:

1. Navigate to **Admin | Configuration | Foreign Systems** (tab).
2. Click SMTP Server, then **Add New**.
3. Add the Name of your SMTP Server and the base Uri (ex: smtp://[hostname]:[port]), then **Create**.

Next, in order to begin email alert notifications for a policy, you will need to assign a Task for the job. The **Setting Up Email Alerts** information below is just one example of tasks that can be configured for automated email notifications.

Setting up Email Alerts

Email alerts can be created in **Admin | Tasks > Server Tasks > E-mail Tasks**, then **Add New**.

Approval Requests

1. Navigate to **Admin | Tasks | Automation** tab, then expand Approvals and select Approval Processes.
2. In the center section you will see options including Manual Approval Process with E-mail Alerts (If this option does not exist, click Add New to add it). Click this option and then **Edit**.
3. Enter the requested information. For the Start Activity, type Send E-mail for New Approval Task. For the SMTP Server, select the resource for the SMTP connection you created above, click **Save**.

Note: For cloud environments the SMTP server settings are pulled from an existing configuration and can't be edited via the parameters tab.

Privilege Manager can push out SysLog formatted messages on a set schedule. Note that this does not happen immediately upon events occurring. Listed below are steps for configuration and task creation for scheduling the action of sending Discovery Event logs to a SysLog server.

Note: The Send policy feedback option needs to be enabled on all policies that are supposed to send SysLog formatted events.

Configuring SysLog Connection

To configure SysLog messages in Privilege Manager:

1. Navigate to **Admin | Configuration** and select the Foreign Systems tab.
2. Click on SysLog and **Add New**. Set a Name and the SysLog Server Address (either tcp or udp). The default is udp on port 514.

The screenshot shows the 'Foreign Systems' configuration page. At the top, there are tabs for 'General', 'Discovery', 'Reputation', 'Users', 'Credentials', and 'Foreign Systems'. Below the tabs, the 'SysLog' section is active. It features an 'Add New' button. Below this, there are two input fields: 'Name' with the value 'New SysLog Server' and 'SysLog server' with the value 'udp://[host]:514'. There are 'Cancel' and 'Create' buttons. Below the form is a table with columns 'NAME', 'DESCRIPTION', and 'LAST MODIFIED BY'. The table is currently empty, with the text 'No SysLog exist, please create one' below it. A 'Back' button is at the bottom.

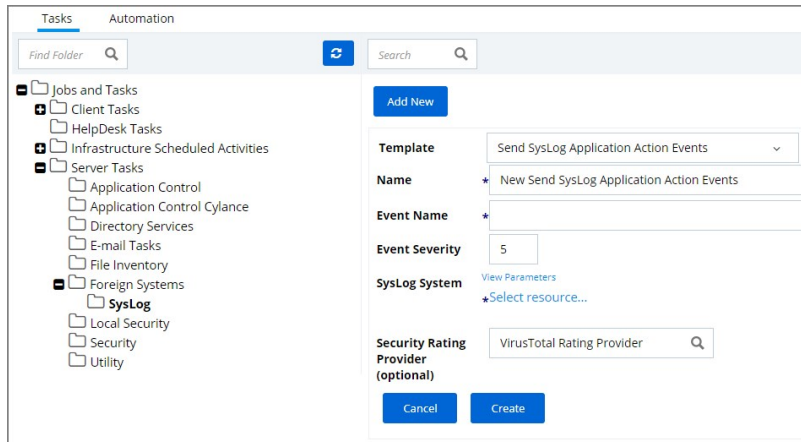
3. Once the server is created, you can use **Edit** to change any of the configuration settings.

The screenshot shows the 'New SysLog Server' configuration form. It has a 'Details' section with 'Name' and 'Description' both set to 'New SysLog Server'. Below that is a 'Settings' section with 'Protocol' set to 'UDP', 'Host' set to '[host]', and 'Port' set to '514'. At the bottom, there are four buttons: 'Back', 'Edit', 'Create a Copy', and 'Delete'.

The protocol drop-down options are UDP, TCP, and HTTPS. HTTPS supports integrations with DEVO.

Setting up SysLog Server Tasks

1. After adding a new Syslog connection, to manually send logs to your Syslog Server go to **Admin | More...** and select **Tasks**.
2. Expand the Server Tasks folder, then Foreign Systems, select SysLog and click **Add New**.
3. From the Template drop-down, for example select **Send SysLog Application Events**.
4. Add a Name for this task, an Event Name (e.g. "Privilege Manager Application Events"), and Event Severity.
5. Click **Select resource** to select your SysLog server foreign system (configured above).
6. Optionally also enter a Security Ratings Provider, depending on your other integrations.



7. Click **Create**.

Once created, you'll be taken to the new Scheduled Task's page where you can run the task on demand and/or specify how often you want events received by Privilege Manager (i.e. all events viewed in Admin I Event Discovery) to be pushed out to the SysLog server. The schedule can be hourly, every 30 minutes, daily, or whatever time period is preferred.

After this task runs and successfully completes, verify that Event Discovery events appear in your SysLog system.

Template Options

The following template options are available:



- **Send SysLog Application Action Events** - Use this template to send application action events to your SysLog system. Application Action Events contain generic information about the application that run, which policy was triggered, the date/time stamp, computer, and user for example.
- **Send SysLog Application Justification Events** - Use this template to send application justification events to your SysLog system. For example, if a user runs an application requiring a justification workflow.
- **Send SysLog Bad Rated Application Action Events** - Use this template to send an event to your SysLog system, when an application is being installed or executed, that is identified with a bad security rating.
- **Send SysLog Events** - Use this template to send all SysLog events to your SysLog system. These events are based on the different options you selected on the SysLog server during setup.
- **Send SysLog Newly Discovered File Events** - Use this template to send newly discovered file events to your SysLog system. For this to produce any events the Default File Inventory Policy needs to be enabled and resource discovery schedules need to be customized.
- **Send SysLog Password Disclosure Events** - Use this template to send all password disclosure events to your SysLog system.

Data Sources

The following five data sources can be used with the respective templates above:

- **Application Control Justification Events** (7d6bdbf0-8f2a-4e9c-9c7e-fa6b75803c45)
- **Application Control Policy Feedback** (eeb7aaf6-f675-4586-a7e3-3eb54b59ba4d)
- **Recently Discovered Applications Query** (b875d3a6-433c-42cc-8332-05350343e498)
- **Local Security Password Disclosure Events** (13d6cf4d-0132-4401-88ab-80b55301c60c)
- **Application Control Policy Feedback Restricted to Security Level** (4eb4ec69-d7a9-4797-972a-41855d3e7799)

If custom data sources are used, they need to specify the following fields:

- externalId
- Facility
- Severity
- EventTime
- Host
- DeviceVendor
- DeviceProduct
- DeviceVersion
- Name
- CEPSecurity

Troubleshooting If SysLog Option is Missing under Foreign Systems

If you are a Privilege Manager Cloud customer, contact Thycotic support to have it added to your instance.

On-premises customers, navigate to [https://\[YourOrganizationURL\]/TMS/Setup/ProductOptions/SelectProducts](https://[YourOrganizationURL]/TMS/Setup/ProductOptions/SelectProducts) and check the Thycotic SysLog Connector option. Install the SysLog Connector and accept the License Terms and Conditions.

Privilege Manager can perform real-time reputation checks for any unknown applications by integrating with analysis tools like VirusTotal. This article shows how to set up the integration between Privilege Manager and VirusTotal and then create a greylisting policy in Privilege Manager for reputation checking.

VirusTotal API Key

As a first step the VirusTotal Ratings Provider has to be configured. For this,

1. Sign up for a Free VirusTotal account at <https://www.virustotal.com/>.
2. Sign in to VirusTotal and find your API key under your **Username | Settings | API Key**.

Install VirusTotal

As a second step VirusTotal needs to be installed in Privilege Manager.

Note: You need outbound access on your server for that installation.

1. Open a browser on your Privilege Manager Web Server.
2. Browse to <https://YourInstanceName/TMS/Setup/>.
3. On the Currently Installed Products screen, choose Install/Upgrade Products.
4. Check the Thycotic VirusTotal Reputation Connector, click **Install**. Then **Accept** the End User License Agreement. You will see your Installation Progress.

Note: If the installation of VirusTotal initially fails, redirect to <https://YourInstanceName/TMS/Setup/> and click the **Repair** button next to the VirusTotal Product.

VirusTotal Reputation Connector	10.7.2055	10.7.2055	10/3/2019 12:09 PM	Repair
Install/Upgrade Products Refresh				

5. Navigate to **Thycotic Privilege Manager | Admin | Configuration | Reputation** tab.
6. Select **VirusTotal Rating Provider** from the Select Rating Provider drop down menu.

Configuration

General Discovery **Reputation** Credentials Foreign Systems Roles Advanced

Select Rating Provider

VirusTotal API Key [Update](#)

Details

Name VirusTotal Rating Provider

Description Application Control VirusTotal based provider for resource security ratings.

Classify as 'Suspect'

When or more positive indicators are found by leading scan engines

When the total number of positive indicators reaches or more across all contributors

Classify as 'Bad'

When or more positive indicators are found by leading scan engines

When the total number of positive indicators reaches or more across all contributors

[Back](#) [Edit](#) [View as XML](#)

7. Click **Edit** and enter the **VirusTotal API Key**, click Update.

Select Rating Provider: VirusTotal Rating Provider

VirusTotal API Key: Update

Details

Name	VirusTotal Rating Provider
Description	Application Control VirusTotal based provider for resource security ratings.

Classify as 'Suspect'

When or more positive indicators are found by leading scan engines

When the total number of positive indicators reaches or more across all contributors

Classify as 'Bad'

When or more positive indicators are found by leading scan engines

When the total number of positive indicators reaches or more across all contributors

Save Cancel

8. Enter information under Details and specify settings for Suspect and Bad classifications.

9. Click **Save**.

Note: VirusTotal can be used without API Key. If the free version is used, reputation checks are limited to 4 per Minute. Thycotic does not recommend this for a production environment.

For the implementation example below, we are creating two filters, using one default filter, and creating a policy. One filter is the standard Security Rating Filter the other filter controls, that we only send applications to VirusTotal for a reputation check that are in the user's Downloads and Temp directories.

Further details about creating a Security Rating Filter and other needed filters to work with reputation checking policies refer to the [Reputation Checking](#) topic.

The following topics are available in this section:

- [Remove RDP Integration](#)

The Privilege Manager feature to support RDP session monitoring is being discontinued (with version 10.6 of the product).

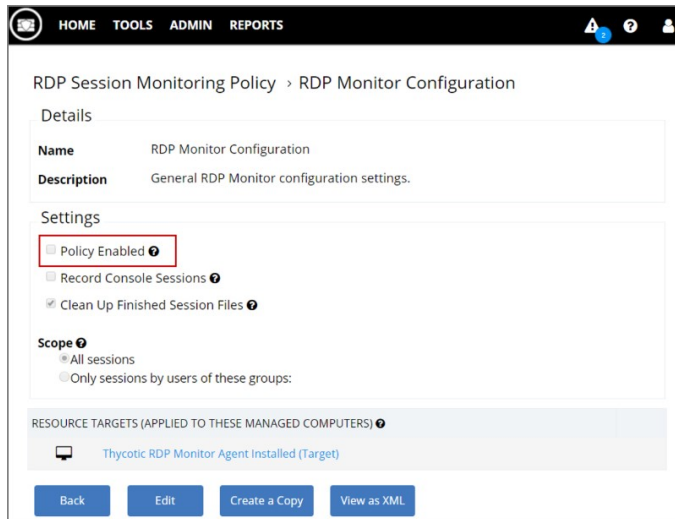
If you had previously set up RDP monitoring in Privilege Manager, perform the following steps to remove it:

1. Uninstall the RDP Monitor from all your Privilege Manager agent computers, using the following command line:

```
msiexec.exe /x {42496710-2e48-471b-ad53-19b54ca5bedd}
```

1. Disable the RDP Monitor policy by navigating to **Tools | RDP Monitor | RDP Monitor Configuration**.

2. In the Settings section, un-check the **Policy Enabled** option.



How to...

This topic is a collection of articles covering "How to..." procedures for different tasks.

- Best Practices:
 - [Disaster Recovery](#)
 - [Using a Service Account to run the IIS App pool](#)
 - [Prevent Read and Write Access to File Types or Locations](#)
- Import, Export, and Migration:
 - [Export and Import Items](#)
 - [Migrate Local Security Policies](#)
- Azure:
 - [Add Thycotic One Users Manually](#)
- Infrastructure
 - [Azure Service Bus Configuration](#)
 - [Setup High Availability/Clustering](#)
 - [Setup Reverse Proxy](#)
 - [Moving MS SQL Server Database for Privilege Manager and Secret Server Combined Installation](#)
 - [VM Deployments](#)
- macOS:
 - [Preference Pane Targeting on macOS](#)
- Maintenance:
 - [Export and Import Items](#)
 - [How to Purge Computers](#)
 - [How to Purge the Action Items Table](#)
 - [Using the Remove Programs Utility](#)

The following topics are available:

- [Disaster Recovery](#)
- [Using a Service Account to run the IIS App pool](#)
- [Prevent Read and Write Access to File Types or Locations](#)

Privilege Manager Disaster Recovery

Any disaster recovery plan needs to include contingency plans for the event when a company's data center goes down, as such, it should always include storing backups of the latest web application and database offsite, potentially at multiple locations.

For Privilege Manager web application backups, Thycotic recommends creating a copy following any install/upgrade. For the database backups, SQL database backup recommendations should be followed.

Maintaining Privilege Manager in a Disaster

With Privilege Manager environments three types of Disaster recovery strategies can be implemented. The framework of a solid Privilege Manager Disaster Recovery Plan should follow these methods of maintaining operations:

- manual backups to restore (restoring/rebuilding from backup)
- passive failover (built and ready, but with a few manual switches)
- active fail-over via High Availability setup. Privilege Managers licensing allows for full clustering.

As a best practice for Privilege Manager databases, we recommend asynchronous replication. There are a lot of transactions - too many transactions for synchronous replication in most enterprise environments. Asynchronous replication works with a manual failover.

Simple Installation and Architecture

Privilege Manager operates on typical modern servers On-Premises, in the Cloud, and in virtual environments.

By design, Privilege Manager's installation is a quick and easy process. Keeping this process as quick and easy to install was a goal from the outset. This serves as a viable fallback option should redundancy plans fail. In a worst-case scenario where the host server fails, a cluster/mirror fails, and the other backup plans fail, Privilege Manager can be installed from scratch quickly and data imported from various methods.

Administrators familiar with Microsoft SQL and IIS can typically install Privilege Manager in about 30 minutes on a prepared server.

Refer to the following installation topics:

- [Privilege Manager Product Installation - Basic](#)
- [Privilege Manager Manual Installation](#)

Restoring from Backup

Thycotic recommends to make a back-up copy of your Privilege Manager web application folder after installation or following an upgrade. This back-up copy is used during disaster recover to restore the instance. Microsoft SQL database restores are simple as well, but require several steps, depending on the backup scenario. Refer to vendor details, such as [Back Up and Restore of SQL Server Databases](#).

Start by preparing servers for installation. When the servers are prepared, restore the Privilege Manager application on one and the database on the other. Some specific web configurations may be needed to match the previous IIS settings.

Restoring Privilege Manager from a Backup

When restoring from backup in the single-server configurations, be certain to make copies of the backup files on a different device or media.

Follow instructions as detailed under [Installing as a Virtual Directory](#).

High Availability

A Privilege Manager implementation based on a high availability setup plays well with any disaster recovery plan.

With HA clustering, there are more than one front-end web servers, and more than one active node. Allowing users to use Privilege Manager through more than one active node simultaneously requires enabling clustering within the application. Only one server handles background processes, meaning that one of the active nodes will be designated as the Primary Node at any given time (this can be changed manually, if necessary, in the application). In the event that the Primary Node becomes unavailable, the "Primary" status will be transferred to one of the other active nodes and users can continue using the application without interruption. There can be more than one active and passive server nodes (no limit), depending on the needs of the organization.

A Disaster Recovery Plan for High Availability consists of failover for Web Server or Microsoft SQL Server issues. If the failover members were to themselves fail, then Web Application Backups and Automated Application Database Backups can be used to restore functionality. If these Servers are virtualized, leveraging strategies such as making scheduled Snapshots or having a hot/cold Site may add additional layers of redundancy.

Refer to [Privilege Manager High Availability Setup](#).

Summary & Additional Support Resources

The integration of Privilege Manager into Business Continuity Planning should not present any unique challenges beyond normal server and database recovery. If your organization already has disaster recovery plans for servers and databases, Privilege Manager and its Microsoft SQL database should fit within your organization's current framework. Using server virtualization to assist with Business Continuity and Disaster Recovery in terms of snapshots, replication, and other 3rd party features are recommended where applicable.

Thycotic recommends setting up a domain service account that can both:

- access the Thycotic product's SQL database
- run the IIS Application Pool(s) dedicated to your Thycotic product

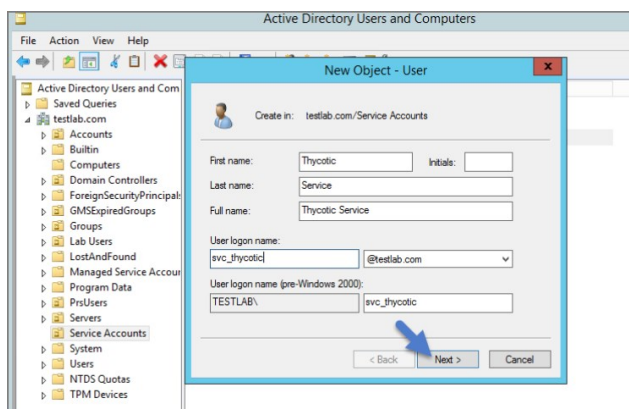
Note: The service account created in this KB should NOT be the same account that is created during the installation of SQL and used to manage SQL as a whole.

To set up this service account correctly you will need to:

1. Create a service account in Active Directory that will be dedicated to your Thycotic product (Domain).
2. Grant the service account access to the SQL Server database (Database).
3. Assign the service account as Identity of the Application Pool(s) in IIS (Web).
4. Grant folder permissions for the service account on two folders (Web).
5. Configure User Rights Assignment to the service account (Domain AND/OR Web).

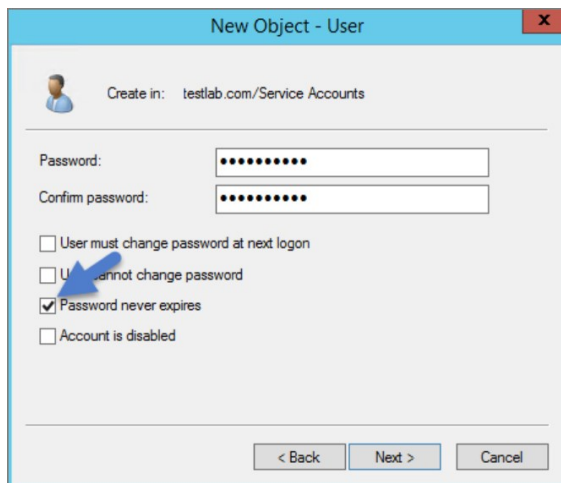
Creating a Domain Service Account

1. Open the **Active Directory Users and Computers** link from Administrative Tools.
2. Right-click the directory where you want to assign this account (i.e. testlab.com > Service Accounts).
3. Click **New and User**.
4. Add a name and logon name for the service account.
5. Click **Next**.



6. Enter a password.

Note: Uncheck "User must change password at next login if checked." Check Password never expires or the account could lock you out of Secret Server.



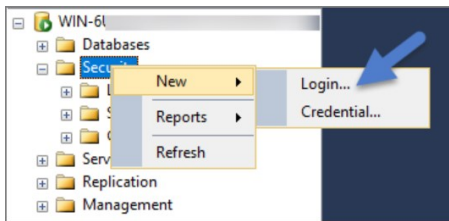
7. Click **Next**.
8. Click **Finish**. This account can now be given access to the database server and the application server.

Granting Access to SQL Database

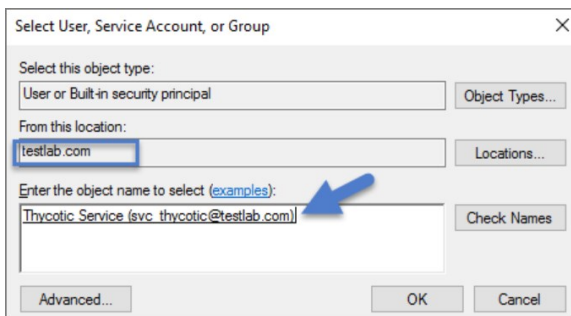
You must have SQL installed on your database server before completing these steps:

1. Using SQL Management Studio (on your database server), connect to your Thycotic product's SQL Database using an Administrator account.
2. Right-click on the Security node (Ensure this is the top most Security node under the instance and not under the database name itself).

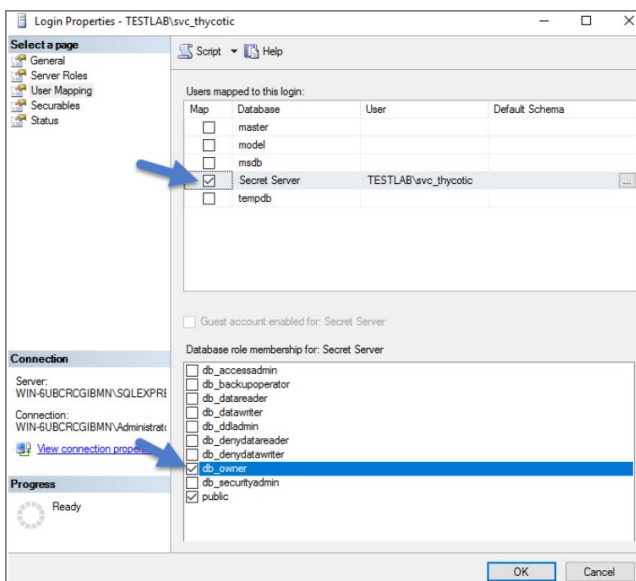
3. Click **New** and **Login**.



4. Ensure Windows Authentication radio button is selected.
5. On the New Login page click Search... Ensure that your domain/AD server is selected as the location.
6. In the "Enter the object name to select" box enter the Login name created for your Thycotic service account (e.g., "svc_thycotic"). Click Check Names and select the correct account.
7. Click **OK**

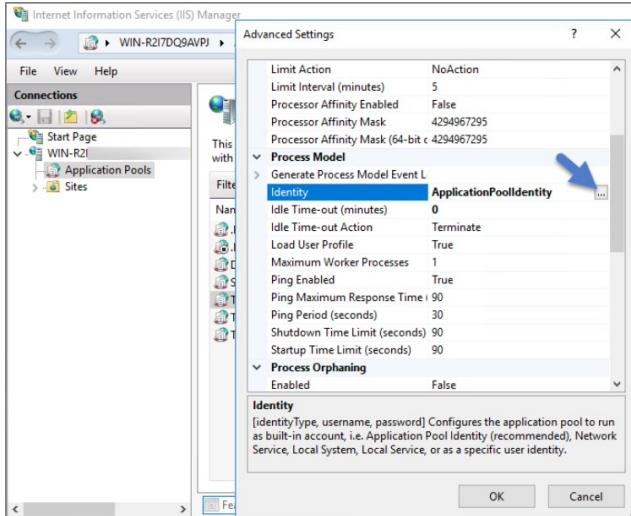


8. If you have already created the database for your Thycotic product, under User Mappings select the database and check the box to grant the db_owner permission (example pictured below). OR - If you have not yet created the Database, Under Server Roles select db_creator
9. Click **OK**



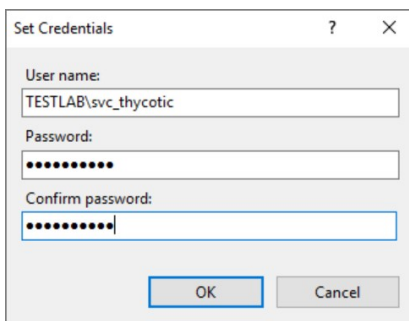
Assigning Identity of Application Pool(s) in IIS

1. Open IIS on your web server **Search I Inetmgr**.
2. Locate the application pool(s) that your Thycotic product is using, right-click Advanced Settings.
3. The Identity box in the **Process Model** section, click the three dots on the right of the box.



4. Select the Custom Account radio button.
5. Click **Set** and enter your service account's name and password.
6. Click **OK**.

Note: You will need to perform this step for multiple application pools for Privilege Manager.



Granting Folder Permissions

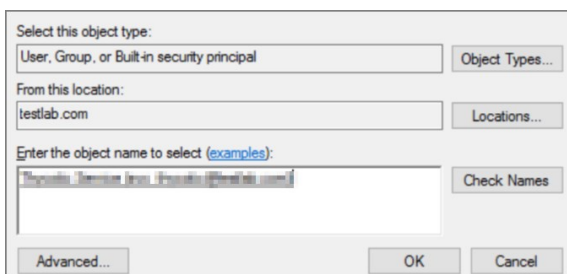
You must have the Thycotic product application files installed (on your web server) before completing this section.

Following the steps below you will need to give the service account **Modify** access to two folders:

- **C:\Windows\TEMP**
- The folder where your Thycotic product's application files are located (i.e.: **C:\inetpub\wwwroot\SecretServer**)

You must have the Thycotic Product Application Files installed on your web server before completing these steps.

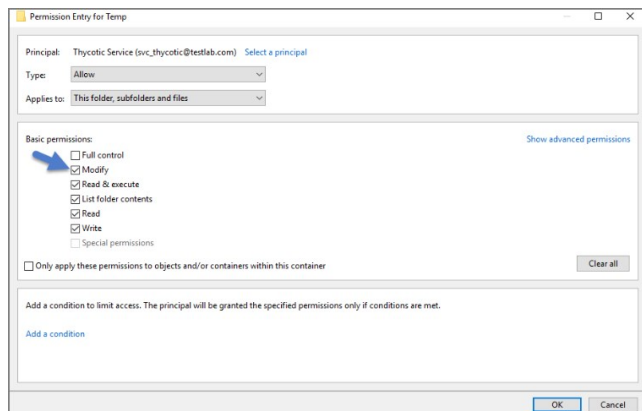
1. Open **C:\inetpub\wwwroot\TMS** and right-click the folder you are modifying.
2. Click **Properties** | **Security** | **Advanced**.
3. Click **Add** and then select a principal.
4. Ensure the domain machine is listed as the Location and type the service account under the "Enter the object name to select" box, click Check Names and Enter network credentials for accessing your domain machine.
5. Click **OK**.



6. Click the **Modify** checkbox.

Your service account should now have Modify, Read & execute, List folder contents, Read, and Write permissions for this folder.

7. Click **OK**, then **Apply**.



Note: If a Windows Security pop-up appears, click Yes. The service account will now be able to access this folder.

Note: The application folder only needs Write and Modify permissions during the installation or during an upgrade. You can remove these once the installation process is complete.

Configuring User Rights Assignment

The following settings are required for Thycotic Secret Server to function:

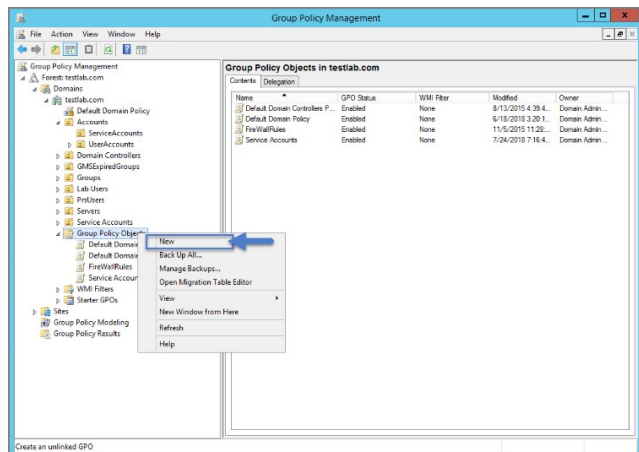
- Log on as a batch job
- Impersonate a client after authentication

You can adjust these settings either

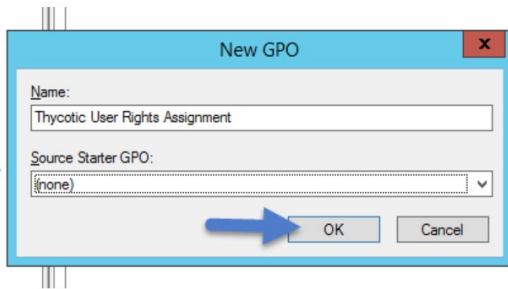
- At the Domain level using Group Policy
- Locally on your IIS Web Server using the Local Security Policy Console

Setting User Rights Assignment on the Domain

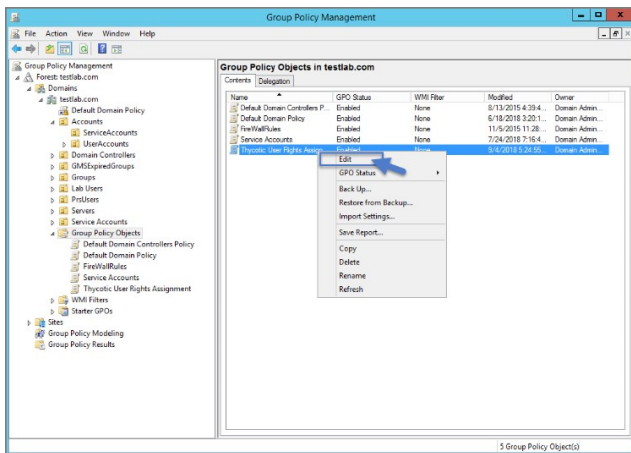
1. Open Group Policy Management Console and right-click your preferred GPO container (i.e. Group Policy Objects).
2. Click **New**.



3. Name the new GPO (i.e. Thycotic User Rights Assignment).
4. Click **OK**.
5. Right-click **new GPO**.
6. Click **Edit**.
7. Expand **Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies**.
8. Click **User Rights Assignment**.
9. Right-click **Log on as a batch job** and click **Properties**.



10. Ensure that the **Define these policy settings** box is checked
11. Click **Add User or Group**
12. Add your Thycotic Service Account.
13. Click **OK** then **Apply**.



14. Grant **Impersonate a client after authentication** permission to the service account under "User Rights Assignment" the same way "Log on as a batch job" was assigned above.
15. Link your new GPO to the OU where your Thycotic product machine accounts exist (web + database servers).

Note: This will overwrite any configuration in the local security policy. Utilizing the local security policy is a safer option if you are not sure about your usage across your domain.

Setting User Rights Assignment Locally

1. On the web server hosting IIS and your Thycotic Application files.
2. Open **Local Security Policy Console** (Run as administrator).
3. Expand **Local Policies | User Rights Assignment**.
4. Right-click **Log on as a batch job | Properties | Add User or Group**.
5. Select your Thycotic Service Account and then click **OK**.
6. Do the same to set Impersonate a client after authentication.

Note: If you get a **Service Unavailable** after applying "Log on as a batch job" permissions, try updating your group policy settings:

1. Open the Command Console.
2. Type in **gpupdate /force**.
3. Restart the Windows Process Activation Service.

You can restrict access to specific file types or locations using Privilege Manager. To prevent read / write access to file types or locations, do the following steps:

- Create a Deny File Access Action
- Create an Application Control Policy to which you will add the Deny File Access Action
- Test the privilege reduction you've just created

In the following scenario you will create a Microsoft Word document and save it on your machine to:

c:\company invoices\invoice 101.doc

Create a Deny File Access Action

1. Navigate to **ADMIN | Actions**.
2. Under Filter Type enter **Deny File Access Action**.
3. Click on the Deny File Access Action.

NAME ^	DESCRIPTION	TYPE	MACOS	WINDOWS
Filter	Filter	deny file access action	Any	Any
Deny Read/Write Access to Microsoft Office Document Files	This action can be used to deny read and write access to Microsoft Office documents.	Deny File Access Action	Not Supported	Supported
Deny Write Access to Executable Files	This action can be used to deny write access to common executable files.	Deny File Access Action	Not Supported	Supported
New Deny Write Access to Executable Files	This action can be used to deny write access to common executable files.	Deny File Access Action	Not Supported	Supported

4. Click on **Create a Copy**.
5. Name the new copy of the action.
6. Click **Edit**.
7. Select the **Read** and **Write** check boxes.
8. Enter in the path of the file (e.g., c:\company invoices).
9. Select **Add** to the right of MIME types and enter in **Word document** for the example.

Details

Name New Deny Write Access to Executable Files

Description This action can be used to deny write access to common executable files.

Deny File Access Settings

Deny Access Deny Read Deny Write

Deny File Access Settings

Path c:\company invoices Include subdirectories

File Extensions + Add None Selected

MIME Types + Add None Selected

Save Cancel Export

10. Click **Save**.

Create an Application Control Policy

1. Navigate to **ADMIN | Policies**.
2. Click **New Policy**.
3. From the Platform drop down Select **Windows**.
4. From the Policy Type drop down Select **Show All Templates**.
5. From the Template Type drop down Select **Other: Empty Policy**.
6. Add Name and Description, click **Create**.

New Policy

Platform: Windows

Policy Type: Show All Templates

Template Type: Other: Empty Policy

Name: Write-protect Word documents in the Company Invoices directory

Description: Prevent Microsoft Word from having write access to, or creating new Word documents in the company invoices directory

Back Create

1. Click **Edit**.
2. Select the **Enabled** Check box.
3. Navigate to the **Conditions** tab.
4. Click on **Application Target**.
5. In the search box enter **word** and select the **MS Word** filter.
6. Click **Add**.

Policy > Write-protect Word documents in the Company Invoices directory

General **Conditions** Actions Policy Enforcement Deployment Change History

Select the applications to control along with any optional criteria.

When no filters are chosen, this policy will apply to **ALL** applications.

APPLICATION TARGETS (WILL APPLY TO ANY OF THE FOLLOWING)

ADD APPLICATION TARGET

Select an Application Target from the folders below. Use the [Application Target](#) page to define more.

View by: List word 1 to 1 of 1

NAME	TYPE	FOLDER
<input type="checkbox"/> MS Word	Win32 Exe Filter	MS Office Suite

Add Cancel

7. Navigate to the **Actions** tab.
8. Click **Add Action**.
9. In the search box enter **Deny File Access Action** and select the new deny file access filter you created.
10. Click **Add**.

Policy > Write-protect Word documents in the Company Invoices directory

General Conditions **Actions** Policy Enforcement Deployment Change History

Send policy feedback

Actions to apply to the application

TYPE ACTION NAME

View by 1 to 7 of 7

<input type="checkbox"/>	NAME	TYPE	FOLDER
<input type="checkbox"/>	Deny Execute	Deny Execute Action	Actions
<input type="checkbox"/>	Deny Execute Message	Display User Message Action	Basic
<input type="checkbox"/>	Deny Files Read and Write Access Message	Display User Message Action	Basic
<input type="checkbox"/>	Deny Read/Write Access to Microsoft Office Document Files	Deny File Access Action	Deny File Access
<input type="checkbox"/>	Deny Windows Hooking	Deny Windows Hooking Action	Actions
<input type="checkbox"/>	Deny Write Access to Executable Files	Deny File Access Action	Deny File Access
<input checked="" type="checkbox"/>	New Deny Write Access to Executable Files	Deny File Access Action	Deny File Access

11. Click **Save**.

12. After you run the Policy Targeting Update under the **Deployment** tab, the appropriate endpoints will receive the new policy.

Test Access

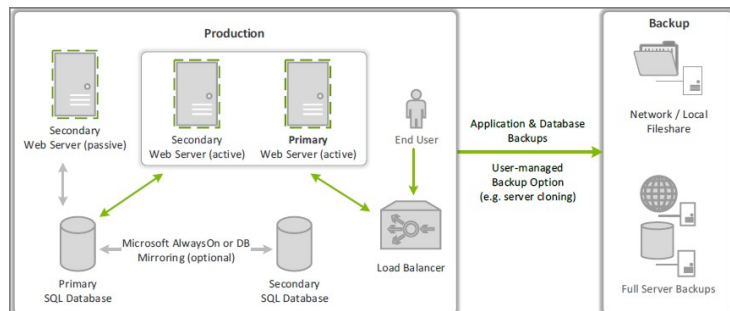
Verify that the restricted access you set up was successful by applying the following tests:

- In Microsoft Word, open c:\company invoices\invoice 101.doc. The file is read only and can't be modified.
- Create a new document and attempt to save it to c:\company invoices\. You will be unable to open it and will receive a File Permission error.
- Verify that you can create or modify a Word document in a different directory.
- In Microsoft Excel, save a spreadsheet to c:\company invoices\invoice 101.doc. The permissions are limited to Microsoft Word.

This sections contains topics around infrastructure set-up and/or changes:

- [Setting up Internet Connected Clients](#)
- [Setup High Availability/Clustering](#)
- [Setup Reverse Proxy](#)
- [VM Deployments](#)
- [Moving SQL DB](#)

This topic explains the steps involved to set up Thycotic Privilege Manager High Availability, also known as clustering.



Pre-Requisites

Make sure that Privilege Manager is installed and working on a primary node with an existing database.

To cluster Privilege Manager a secondary server must be prepared with the proper Privilege Manager pre-requisites. The pre-requisites check can be performed via standard Privilege Manager setup.exe. However, exit that automated installer once all pre-requisites clear.

Except for the Operating System, the following pre-requisites will be installed automatically by our installer. If you already have some of them installed or wish to install them yourself then the installer will skip over them.

System Requirements Overview

1. **Windows 2012 R2 or newer** operating system (2012 or newer is recommended)
2. Microsoft **SQL Server 2012 or newer** (Standard edition or higher is recommended)
3. Microsoft **Internet Information Services (IIS) 7 or newer**
4. Microsoft **.NET Framework 4.6.1 or newer**

Note: Windows Server 2016 comes with the .NET Framework already installed.

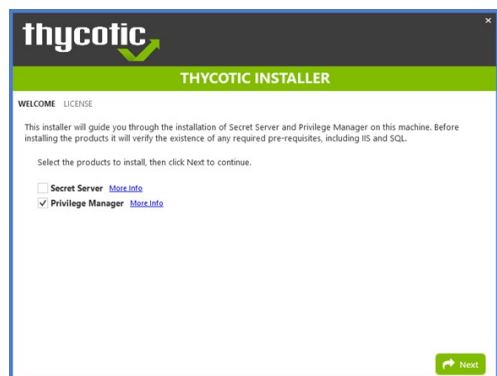
Using the Installer to Install/Confirm Pre-Requisites

The latest version of Privilege Manager is available for [download](#). By clicking the Installer (.exe) link, a setup.exe file will be downloaded to your machine. It is recommended to run the setup.exe file as an administrator.

Note: The setup executable will ONLY be used to install/confirm all pre-requisites are installed on the web server. After confirming the pre-requisites, the installer will be closed and a manual installer will be completed. The manual installation will allow for separate databases and custom file locations. Do NOT complete the installation with the setup executable.

Running the setup.exe will begin an installation wizard. This wizard will ONLY be used to install any remaining pre-requisites required on the web server. The wizard will walk through the initial installation steps, beginning with a Welcome page.

1. On the Welcome dialog, verify that Privilege Manager is selected and select the checkbox if not already checked.



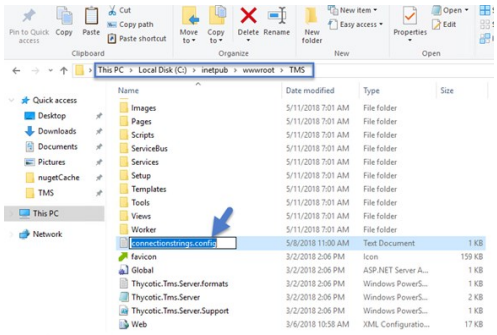
2. Click **Next**.
3. On the License dialog review the End User License Agreement (EULA) and click **Accept License**.
4. On the Database dialog select **Connect to an existing SQL Server**, click **Next**.
5. The Pre-Requisites dialog helps you to ensure everything that is required gets installed for Privilege Manager. Click **Fix Issues** to automatically install the necessary pre-requisites.
6. Close the installer once all pre-requisites are successfully installed.

Note: Do NOT continue installing the products with this installer.

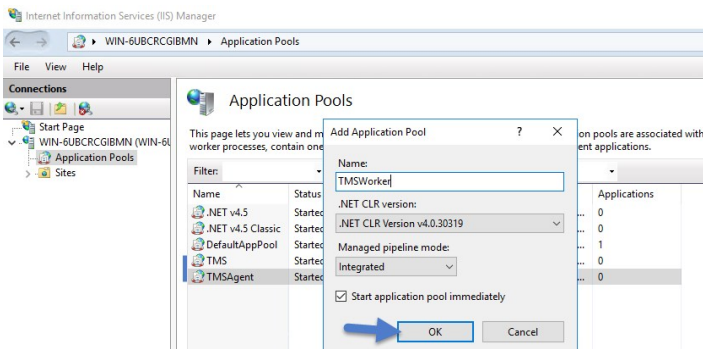
Manual Set-up of Secondary Node

In this procedure you will first copy the web application files from the primary server to the secondary server and then use those copied files to setup and configure the secondary Privilege Manager server.

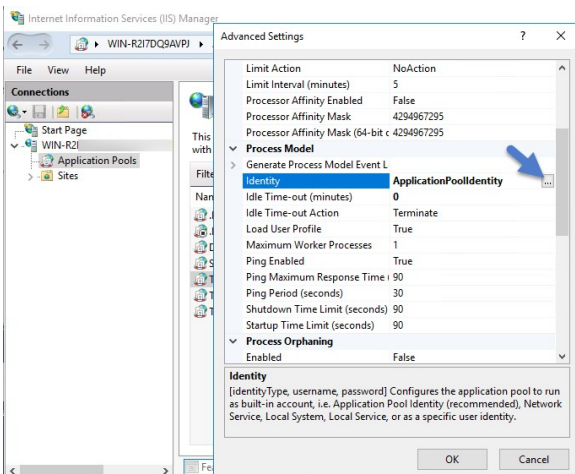
1. On the primary server, decrypt the **connectionStrings.config** by running the following command:
`C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -pd "connectionStrings" -app "/Tms"`
2. Select and copy all contents of the Privilege Manager web application folder at
`C:\inetpub\wwwroot\TMS\`
 Including the unencrypted connectionStrings.config file.
3. On the secondary server, create the same folder path.
4. Paste the entire contents of the Privilege Manager web application folder from the primary web server to the similar location on the secondary web server.



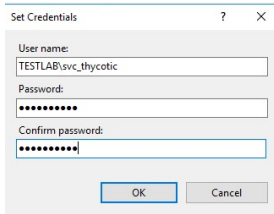
5. Open **Internet Information Services Manager** (inetmgr).
6. Under your local server, right-click **Application Pools** and select **Add Application Pool...**
7. **Add** three new application pools.
 1. **TMS**
 2. **TMSAgent**
 3. **TMSWorker**.



8. For each of the 3 app pools (TMS, TMSAgent, and TMSWorker),
 1. right-click on each app pool,
 2. select **Advanced Settings...**
 3. then the **Identity** box in the "Process Model" section,
 4. click the three dots on the right of the box.

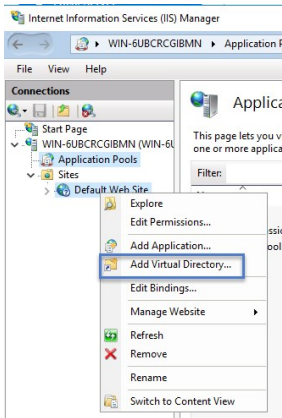


5. Select the **Custom Account** radio button.
6. Click **Set**, enter your service account's name and password.



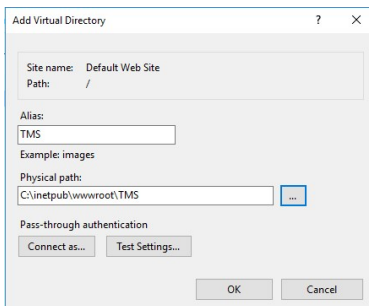
7. Click **OK**.

9. Right-click **Default Web Site** in IIS and select **Add Virtual Directory...**



10. Select an alias for your Privilege Manager. The alias is what will be appended to the website. For instance, "TMS" in <http://myserver/TMS>.

11. Next, enter the physical directory where you unzipped Privilege Manager (i.e., C:\inetpub\wwwroot\TMS).

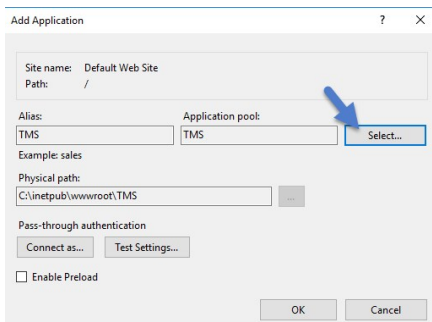


12. Click **OK**.

13. In the tree, right-click the new virtual directory and select **Convert to Application**.

1. Set the **Application Pool** to the one called **TMS**.

2. Click **OK**.



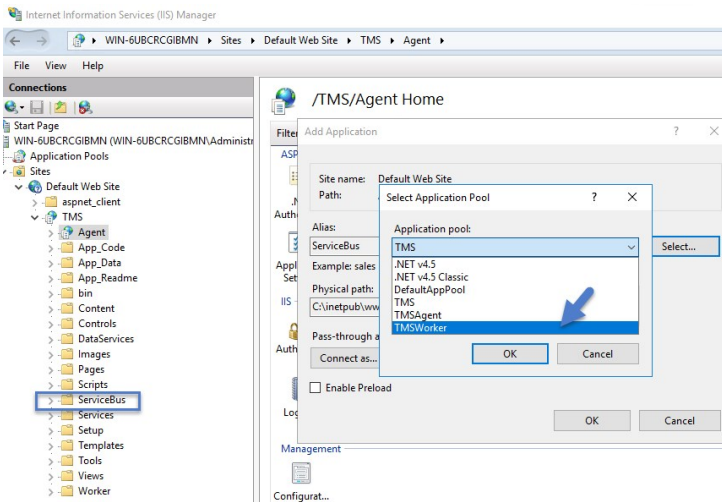
14. In the virtual directory expand the new **TMS** site,

1. right click the **Agent** Subfolder and select **Convert to Application**.

2. Set the **Application Pool** to the one called **TMSAgent**, click **OK**

15. In the virtual directory navigate to the **ServiceBus** Subfolder.

1. Right-click and select **Convert to Application**.
2. Set the **Application Pool** to the one called **TMSWorker** you created earlier, click **OK**



16. In the virtual directory select the **Services** Subfolder.

1. Right-click the new virtual directory and select **Convert to Application**
2. Ensure that the **Application Pool** is set to the one called **TMS**, click **OK**

17. In the virtual directory select the **Setup** Subfolder.

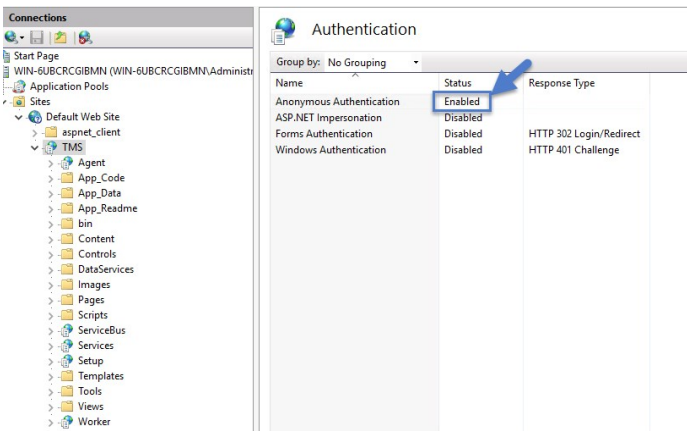
1. Right-click the new virtual directory and select **Convert to Application**.
2. Ensure that the **Application Pool** is set to the one called **TMS**, click **OK**

18. In the virtual directory select the **Worker** Subfolder.

1. Right-click the new virtual directory and select **Convert to Application**.
2. Set the **Application Pool** to the one called **TMSWorker**, click **OK**

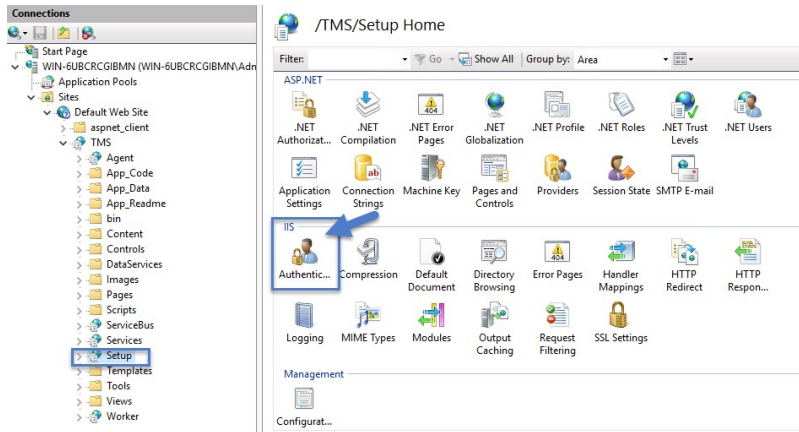
19. Select your **TMS** virtual directory.

1. Double-click **Authentication** in the features pane.
2. Make sure that only **Anonymous Authentication** is set to **Enabled**. Everything else should be set to disabled.



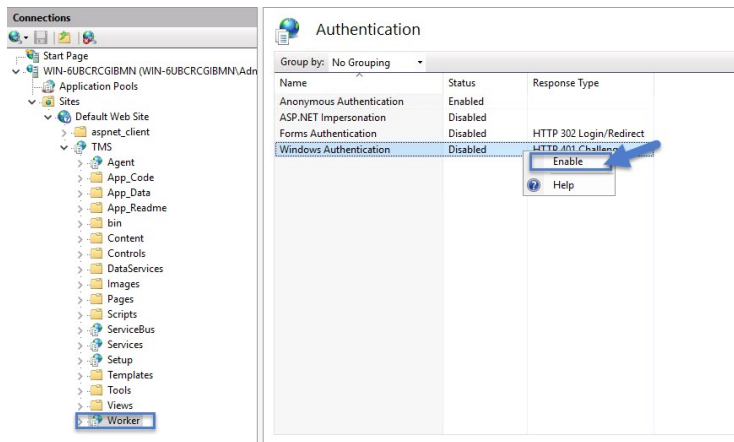
20. Select the **Setup** directory.

1. Double click **Authentication** in the features pane.
2. Make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled** and everything else is disabled.



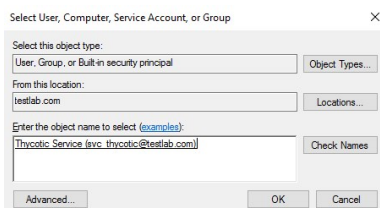
21. Select the **Worker**.

1. Double-click **Authentication** in the features pane and make sure that **Anonymous Authentication** and **Windows Authentication** are both set to **Enabled** and everything else is disabled.

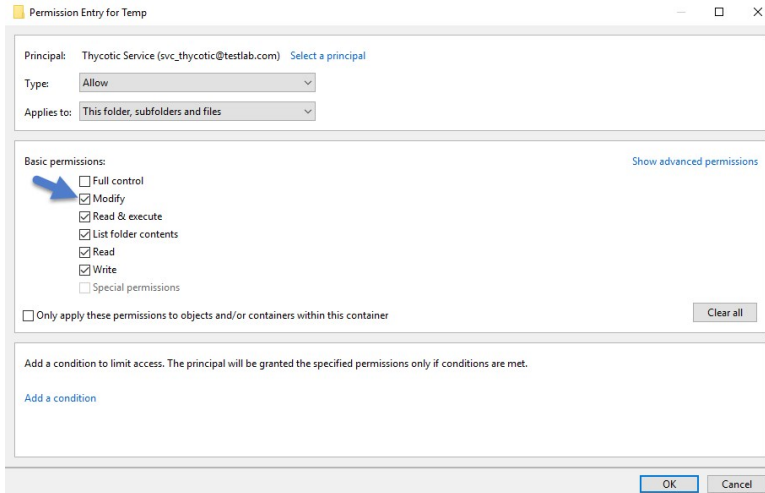


Folder Permissions to C:\Windows\Temp

1. Navigate to the **C:\Windows\TEMP** folder.
2. Right-click the folder and select Properties | Security | Advanced.
3. Click **Add** and **Select a principal**.
4. Ensure the domain machine is listed as the **Location** and type the service account into the **Enter the object name to select** field.
5. Click **Check Names** and **Enter network credentials** for accessing your domain machine.



6. Click **OK**.
7. Under Basic permissions, select the **Modify** checkbox**.**

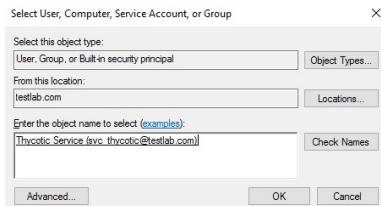


8. Verify your service account has **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** permissions for the **C:\Windows\TEMP** folder.

9. Click **OK** then **Apply**.

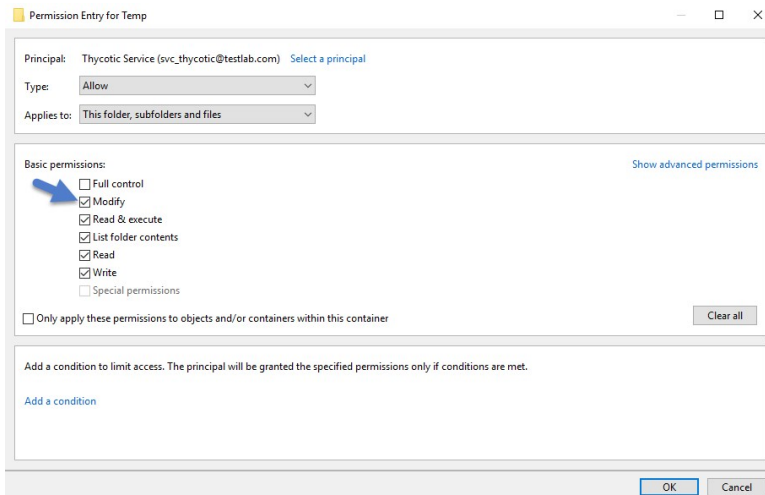
Folder Permissions to the Privilege Manager Application Folder

1. Navigate to the Privilege Manager application folder at **C:\inetpub\wwwroot\TMS**.
2. Right-click the folder and select Properties | Security | Advanced.
3. Select **principal**.
4. Ensure the domain machine is listed as the **Location** and type the service account into the **Enter the object name to select** field.
5. Click **Check Names** and **Enter network credentials** for accessing your domain machine.



6. Click **OK**.

7. Under Basic permissions, select the **Modify** checkbox.



8. Verify your service account has **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** permissions for the **C:\Windows\TEMP** folder.

9. Click **OK** then **Apply**.

Note: The application folder only needs **Write** and **Modify** permissions during the installation or during an upgrade. You can remove these once the installation process is complete.

Permission to Certificate Private Key (prior to 10.6 only)

Note: This is only required for Privilege Manager prior to release 10.6.

TMS requires **Read** access to the private key of the certificate being used for the HTTPS binding. To set this:

1. Open **mmc.exe** as an administrator.
2. Add the certificate manager snap-in choosing to manage certificates for the computer account (**File | Add/Remove Snap-In...**)
3. Click **Certificates**.
4. then **Add | Computer account | Next | Local computer | Finish | OK**
5. Find the certificate that the HTTPS binding for your site is using.
6. Right-click on the certificate and select **All Tasks | Manage Private Keys**.
7. Grant **Read** access to the identity account for your application pools.

If the "Manage Private Keys" option is not available, you can set this permission in PowerShell.

Verify Login on Secondary Node

1. Navigate to Privilege Manager, ex: **http://localhost/TMS**. You should be able to authenticate to Privilege Manager.
2. After logging in, all policies and all data accessible on the primary node should be accessible on the secondary node.

Re-encrypt ConnectionStrings.config

1. On the **primary node**, run the following command to re-encrypt the connectionStrings.config file:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regis.exe -pe "connectionStrings" -app "/Tms"
```

2. On the **secondary node**, run the same command to re-encrypt the connectionStrings.config file:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_regis.exe -pe "connectionStrings" -app "/Tms"
```

Privilege Manager has now successfully been clustered. A load balancer, GTM, VIP, etc. can be used to manage the traffic. The settings to configure this will be handled on the side of this infrastructure piece and is beyond the scope of this document. Contact Thycotic's Professional Services team if additional consultation is required.

Thycotic requires that **sticky sessions** are enabled on the load balancer to prevent a user from bouncing between servers on each request of a single session.

On-premises Privilege Manager instances need to use an Azure Service Bus for internet connected clients. The Azure Service Bus is a subscription service that external agents can connect to and use to communicate with an internal Privilege Manager Server (TMS) instance.

Note: Cloud customers don't need to use the Internet Connected Clients set-up, because their clients can already connect to the internet-based cloud instance.

With Privilege Manager 10.7 and up TLS 1.2 is supported.

This page is broken up into three sections:

- Azure Service Bus Queue Configuration
- Setting up the Service Bus as a Foreign System in Privilege Manager
- Configuring the Agents to use the Service Bus (if this is a new agent installation, the Agents can be pointed directly at the Service Bus namespace URL)

Azure Service Bus Queue Configuration

Thycotic requires a Service Bus relay for remote communication. For this a Service Bus Queue needs to be created, follow the procedure as outlined by Microsoft [here in Quickstart: Use Azure portal to create a Service Bus queue.](#)

1. In the Azure Service Bus portal go to the **Shared access policies** page.
2. Find the policy called **RootManageSharedAccessKey**. If you don't have one yet, create one by that name and select the **Manage** option and save it.
3. On the **RootManageSharedAccessKey** policy you can see the **Primary Key** field. Make note of where this is. We have use it in a step down below.
4. Next, navigate to the **Queues** page and create a new queue.
5. Do not check any of the options, using the defaults is fine. Take note of the queue name you gave it.

Next you will need to follow the instructions below to create a credential for the Service Bus and add the Service Bus as a foreign system in Privilege Manager.

Setting up the Service Bus Foreign System

The Azure Service Bus requires a Foreign Systems configuration in Privilege Manager. To configure a Service Bus instance with a custom URL and credentials follow these steps:

1. In the Thycotic Privilege Manager Console, click **Admin | Configuration**.
2. Click the **User Credentials** tab.
3. Click **Add New**.

1. Enter a **Name**, for example *Azure Service Bus Credential*.

2. Set the Account name to **RootManageSharedAccessKey**.
3. Set the Password to the value of the **Primary Key** obtained during the Azure Service Bus configuration procedure **step 3** under "Azure Service Bus Queue Configuration" above.
4. Click **Save**.
4. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
5. Click the **Azure Service Bus** option.
6. Click **Add New**.
 1. Enter a **Name**, for example *Privilege Manager Azure Service Bus*.
 2. Set the **ServiceBus Name** to the namespace of the Service Bus from the Azure Portal. To find this value, open the Azure Portal, locate the Service Bus that is being used for this integration (refer to the intro above). Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance you just located in the list of Service Bus instances).
 3. Deselect the **Enabled** box for now.
 4. Click **Create**.
7. Click **Edit** to provide more Settings details.
 1. Set the credential to the credential created in step 3 of this procedure (*Azure Service Bus Credential*).
 2. Enable the Service Bus.
 3. Leave the URL field as is (and ignore the fact that it's called URL – it's just the Service Bus name).
 4. Make sure the URI matches the first part of the namespace created in Azure.
 5. Set the QueueName to the same queue name created above in **step 4** under "Azure Service Bus Queue Configuration".
 6. Set the Queue Policy Name to **RootManageSharedAccessKey**.
 7. Set the Queue Policy Secret to the **Primary Key** as obtained in **step 3** under "Azure Service Bus Queue Configuration" above.
 8. Click **Save**.

8. Recycle the App Pools on the Privilege Manager Instance following any changes for this integration. Without the recycle, the new settings won't be applied.

9. To verify everything is working correctly, open your browser and point it to the ServiceBus worker service:

- **On-Premises:** <https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc>

Wait for the page to respond.

Configuring Agents to Use the Service Bus

When setting the URL for Agent communication, Internet connected clients need to use the Service Bus URL created above.

Note: For new installations, the agents can be set up to communicate with the service bus during the initial installation process when the **TMSURL** and installation codes are provided, refer to [Bundled Install](#).

Using regedit

1. Open the Registry Editor (**regedit**).
2. Navigate to **HKEY_LOCAL_MACHINE | SOFTWARE | Policies | Arellia | AMS**.
3. Right click **BaseUrl** and select **Modify**.
4. In the **Edit String** dialog box, change the **BaseURL** to your Privilege Manager (TMS) Address based on the **Azure Service Bus Queue** configuration, for example [https://\[your company\].servicebus.windows.net/](https://[your company].servicebus.windows.net/), which in our example is <https://testing.servicebus.windows.net/>
5. Close the Registry Editor.
6. Restart the Agent service.

Using PowerShell

To modify the TMS address via PowerShell, run this command as Administrator:

```
C:\Program Files\Thycotic\Powershell\Arellia.Agent\SetAmsServer.ps1
```

The script will then ask you to type in the fully qualified domain name of the server, enter the **Azure Service Bus Queue URL**, for example [https://\[your company\].servicebus.windows.net/](https://[your company].servicebus.windows.net/), which in our example is <https://testing.servicebus.windows.net/>.

If you have a combined installation of Privilege Manager and Secret Server and wish to move/migrate the MS SQL Server databases, follow the steps below for the case that applies to you:

- **Case I:** Keeping all data in the current database: Backup the existing databases and restore them to the new SQL Server using the instructions below:
 - For Privilege Manager: see Moving the Privilege Manager DB topic below.
 - For Secret Server: <https://thycotic.force.com/support/s/article/Moving-Microsoft-SQL-Server-Database-to-another-machine>

If you have successfully performed the backup and restore (per the applicable instructions above), your site will be connected to the new database.

- **Case II:** Abandoning all data and starting fresh:
 1. In Privilege Manager, go to [https:// <SERVERNAME>/Tms/Setup/Database/ConnectDatabase](https://<SERVERNAME>/Tms/Setup/Database/ConnectDatabase)
 2. Provide the new database connection and click **OK**
 3. Install desired Thycotic products like Privilege Manager and/or Secret Server.

Moving the Privilege Manager DB

Step 1: Backup and Restore the Database

1. Stop the TMS site (Ams site for Arellia) in Internet Information Server (IIS) to prevent any changes to the database
2. Stop the TMS, TMSAgent, and TMSWorker application pools (Ams and AmsWorker application pools for Arellia).
3. Back up the database by accessing SQL Management Studio and right-clicking on the database to select Tasks > Back Up.
4. Select a file location for the .bak file. Transfer this file to the new server.
5. On the new database server, through SQL Management Studio, restore the database backup (the .bak file).
6. Create and/or grant access to the account that will be accessing the database (see TMS Installation Guide for account creation instructions)

We recommend taking the old database offline.

Step 2: Connect to the new database (configure the database connection details)

1. Restart TMS website.
2. Check that the TMS, TMSAgent, and TMSWorker application pools are running.
3. Browse to your TMS URL database connection page e.g. [https:// <YOUR_URL_INSTANCE>/Tms/setup/database/connectdatabase](https://<YOUR_URL_INSTANCE>/Tms/setup/database/connectdatabase) (for Arellia this URL would be slightly different e.g. [https:// <YOUR_URL_INSTANCE>/ams/setup/database/connectdatabase](https://<YOUR_URL_INSTANCE>/ams/setup/database/connectdatabase)) and you will see a page to enter your new database connection details.
4. Enter your new SQL Server and the account information.
5. Click Next and the site will connect to the new database.

Your site is now pointing to the new database.

If also migrating to new web servers or doing a reinstallation, copy the tmsEncryption.config file(s) to the new web servers(s). The file is located on the web server at the root of the TMS web site and should be copied to the same place on the destination server(s): \\inetpub\wwwroot\TMS This file is only applicable if current servers are on version 10.5 or higher. (refer to [Item Encryption](#))

To roll back changes and restore the original database, simply start back at Step 1 and move the database back to the original database server.

Note: Thycotic Management Server, or "TMS", is an umbrella term for our base application layer that Privilege Manager runs on top of. For this guide you only need to recognize that "Tms" is programmed into your Privilege Manager URL string for configuration purposes.

Many organizations as a best practice restrict their privilege manager web server from inbound and outbound internet traffic. However this can cause a functional issue as agents not connected to the corporate network would not be able to reach the server to receive policy updates or submit event feedback.

To resolve this functional issue while maintaining security Thycotic supports agent connections through a Reverse Proxy which can live in the DMZ. The proxy will filter connection requests and only forward those from the agents allowing communication while significantly reducing the potential attack surface. Proxies can be configured using many different networking tools and in this document we will show how to do so with Windows Application Request Routing in IIS.

In this setup, only the endpoint agent needs to be accessible via HTTPS. It is important to note that the certificate being used for HTTPS communication should be the same certificate that is installed on your Privilege Manager web server.

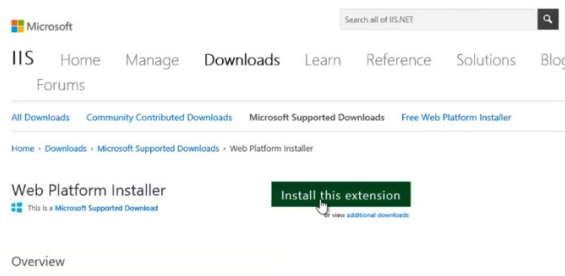
System Specifications

These are the minimum system specifications for a server that is used as a reverse proxy:

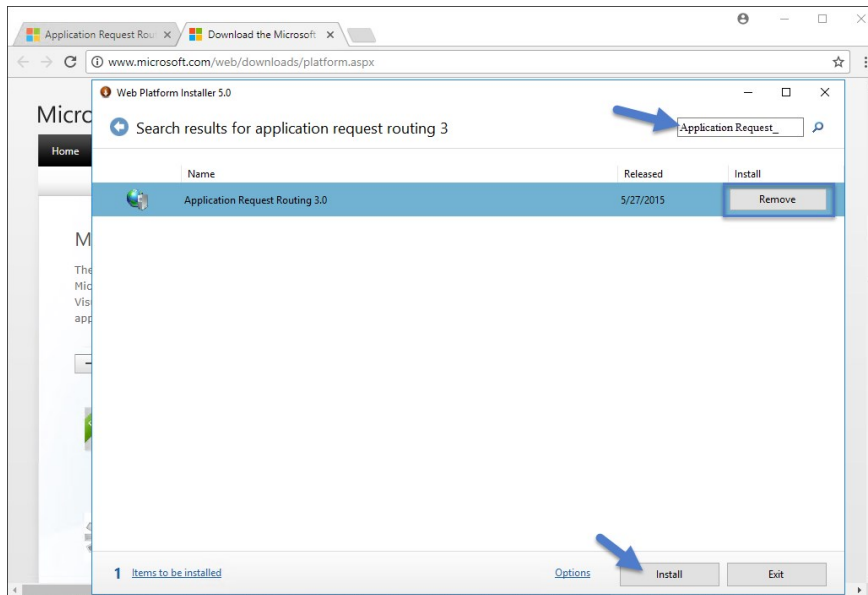
- 2 Cores
- 4 GB RAM
- 40 GB hard drive

Server Configuration

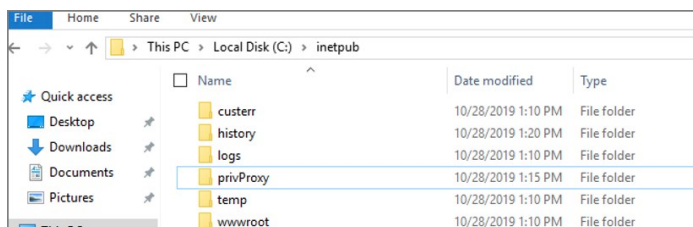
1. Setup a new server or modify an existing server to be in the DMZ.
2. Download [Web Platform Installer](#) on your new Reverse Proxy server. This allows you to add updated IIS extensions from Microsoft.



3. In the search bar of the Web Platform Installer, enter **Application Request Routing #3.0**. Click **Add** and then **Install**. You will need to accept the license terms.



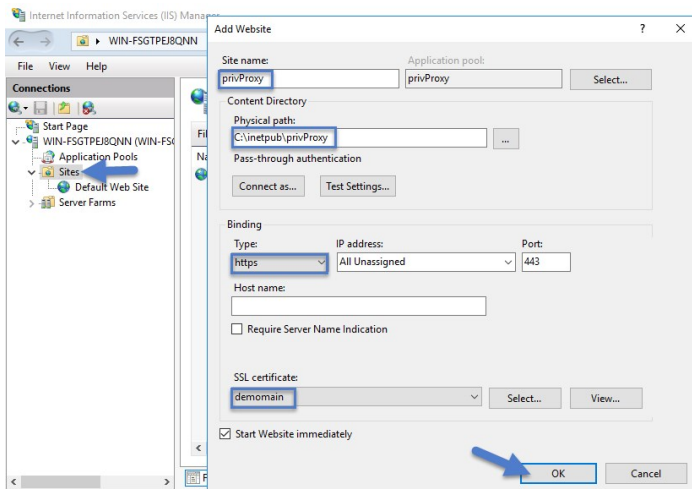
4. Create an empty folder under C:\inetpub\ named **privProxy**.



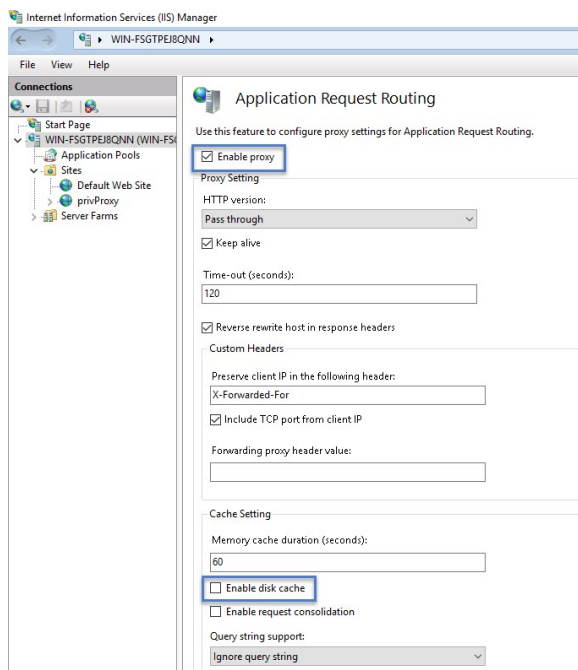
- Open IIS Manager and right-click **Sites** and select **Add Web Site**.
- Name the site **privProxy** and set the **Physical Path** to the folder under C:\inetpub named **privProxy**.
- Change the binding to **HTTPS**.
- Use the default port of 443.

Note: If there are other applications using port 443 on this server, such as Symantec CEM, then set the privProxy to use a different port, such as **4593**. If you use a port other than 443, make sure to add the appropriate firewall rule.
- Select a certificate for the binding to use and Click **OK**. The certificate being used for HTTPS communication should be the same certificate that is installed on your Privilege Manager web server. Follow [these instructions](#) to install a certificate on your Reverse Proxy server.

Note: The certificate used for HTTPS binding on the Web App Server needs to be exported then imported into the Root and Intermediate certificate stores on the Proxy Server.



- In the IIS Manager's left hand navigation pane select the server node.
- Open **Application Request Routing** from the middle pane.
- Select **Server Proxy Settings** in the right hand actions pane
- In the **Application Request Routing** pane, select **Enable Proxy** and deselect **Enable disk cache**.



- Select **Apply** under the actions pane and then select **URL Rewrite**.
- Select **Add Rule(s)** on the actions pane and then under **Inbound rules** select **Blank rule**.

16. Name the rule **privProxy**.

17. In the Edit Inbound Rule window, do the following steps:

1. Under **Match URL** from the **Requested URL** menu, choose **Matches the Pattern**.
2. From the **Using** menu, choose **Wildcards**.
3. From the **Pattern** menu, choose **Tms/Agent/***.
4. Select **Ignore case**.

Edit Inbound Rule

Name:

Match URL

Requested URL: Using:

Pattern:

Ignore case

18. Under **Conditions**, from the **Logical Grouping** menu, choose **Match All**.

19. Add a condition for : **Matches the pattern: on**

20. (optional) You can also add a condition and set it to the port number configured above.

Conditions

Logical grouping:

Input	Type	Pattern
j(HTTPS)	Matches the Pattern	on
{SERVER_PORT}	Matches the Pattern	45593

Track capture groups across conditions

21. Under **Action**, from the **Action Type** menu, choose **Rewrite**.

22. Under **Action Properties**, in the **Rewrite URL** field, type the URL `https://server.example.com/Tms/Agent/{R:1}`

23. Select **Append query string**

24. Select **Stop processing of subsequent rules**

Action

Action type:

Action Properties

Rewrite URL:

Append query string

Stop processing of subsequent rules

25. In the **Actions** pane, click **Apply**.



Now your internet-connected agents will be able to communicate with the Privilege Manager server through <https://external-name.domain.com:45593/Tms/> or <https://external-name.server.com/Tms/>, depending on the port you chose.

Testing Agent URLs

To test registered agent URLs use the following, based on Privilege Manager version:

- /agent/agentregistration4.svc
- /agent/agentregistration3.svc
- /agent/agentregistration2.svc

For example using `https://PrivilegeManagerAppServerName.DomainName/TMS/Agent/agentregistration4.svc` at the agent agent point, should successfully return XML like the following:

```

<?xml:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:xs="http://schemas.xmlsoap.org/2004/09/xsd" xmlns:i0="http://tempuri.org/"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/wss-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsa10="http://www.w3.org/2005/08/addressing"
xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wspap="http://schemas.xmlsoap.org/ws/2004/08/addressing/policy"
xmlns:mcc="http://schemas.microsoft.com/ws/2005/12/wsdl/contract" xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:wsm="http://www.w3.org/2007/05/addressing/metadata" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tms="http://arellia.com/services/Agent/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:wsm="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/" name="Thycotic.Tms.Services.Agent.AgentRegistration4" targetNamespace="http://arellia.com/services/Agent/"
<wsdl:import namespace="http://tempuri.org/" location="https://localhost/TMS/Agent/AgentRegistration4.svc?wsdl-wsdl1"/>
<wsdl:types/>
<wsdl:service name="Thycotic.Tms.Services.Agent.AgentRegistration4">
  <wsdl:port name="CustomBinding_IAgentRegistration2" binding="i0:CustomBinding_IAgentRegistration2">
    <soap12:address location="https://localhost/TMS/Agent/AgentRegistration4.svc"/>
    <wsa10:EndpointReference>
      <wsa10:Address>https://localhost/TMS/Agent/AgentRegistration4.svc</wsa10:Address>
    </wsa10:EndpointReference>
  </wsdl:port>
  <wsdl:port name="CustomBinding_IAgentRegistration21" binding="i0:CustomBinding_IAgentRegistration21">
    <soap12:address location="http://win-e6gkpm7j7tf/TMS/Agent/AgentRegistration4.svc"/>
    <wsa10:EndpointReference>
      <wsa10:Address>
        http://test-system/TMS/Agent/AgentRegistration4.svc
      </wsa10:Address>
    </wsa10:EndpointReference>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

Note: Make sure that the server acting as the reverse proxy trusts and matches the certificate that the Privilege Manager web server is using for its HTTPS binding. If the certificate is not trusted, the proxy will return a 500.21 Gateway error.

Agent Configuration

When you set up the Agent, make sure that the BaseURL has been set to the DMZ Server Address by following the steps in [Setting the Privilege Manager Server Address](#).

Important: The Privilege Manager server is **not** able to push tasks to agents when the agents are not connected to the same network. However, the internet connected clients will automatically pull tasks from the server on a scheduled interval.

Privilege Manager agents are installed on endpoint machines to implement policies which are defined by the user (the Privilege Manager administrator) in the Privilege Manager console (the user interface of the Privilege Manager Server).

This article is about agent deployment to endpoints in Virtual Desktop Infrastructure (VDI) or other similar environments. It describes the different cases and options for deploying Privilege Manager agents to VDIs and discusses the pros and cons where relevant. It is expected to be read by a user who is the Privilege Manager administrator for the customer.

Installing the Privilege Manager agent is supported as part of a VDI image build. There are a few different ways to accomplish this, based on the (Privilege Manager) customer's environment and preferences. Discussion of the relevant issues and options is grouped in this article as follows:

Identifying Agents to The Console

The pertinent question here is: Do you (the user) plan to use (or are using) persistent virtual machines (VMs) or dynamic VMs? There are different implications for each of these, discussed below.

Persistent VMs

In a persistent VM, machines images are created, spun up, and then persist indefinitely. This case is fairly simple. We can treat these machines the same as we would physical machines except for concerns around the universally unique identifier (UUID), which will be discussed further on (in the section, "Multiple VMs Collapsed to a Single Resource").

Dynamic VMs

In a dynamic VM, a golden image is spun up each time a user requests it with their profile and it is then applied on top. This case is more complicated.

The major concern is agent spamming, which would happen as follows: the Privilege Manager console sees each new image as a new computer and rapidly runs through the customer's licenses, leaving a large number of orphan machines. There are a few different ways to deal with this situation, discussed in the sub-sections below.

Multiple VMs Collapsed to a Single Resource

The easiest way to support dynamic VMs is for you to collapse all of your VMs to a single computer resource on the console. This can be accomplished as follows:

1. Add a registry entry in HKLM\Software\Arellia\Agent called "AgentIdOverride."
2. Install the agent on a physical computer and allow it to register.
3. Next, in the Privilege Manager console:
 1. Navigate to Admin > Agents.
 2. Click on one of the charts to view a list of registered computers.
 3. Find the computer in the report and click on it. This will take you to the Resource View of that computer. The ID for this computer is the UUID displayed as the last part of the URL (after "/item/view/") in the browser address bar.
 4. Copy this ID value (the last part of the browser URL).
4. Place the copied ID value in the AgentIdOverride registry entry.

Alternatively, if you want multiple VDI images to which differing policy sets are applied, you could have different values. The rollout computers in the console could then be assigned to the appropriate resource targets.

The benefits of this approach are:

- It is by far the simplest to implement.
- It results in the fewest licensing issues.
- Moreover, because the resources are created ahead of time they can be inventoried and assigned to the appropriate resource targets. Consequently, a machine would get the appropriate policies as soon as it spins up with no need to wait for processes to run either on the desktop or server.

The downside of this approach is:

- There would be some loss of fidelity in data on the console, specifically around which machine an event happened on. However, since virtual desktops are by nature transitory that may be less of a concern. Privilege Manager will still attach usernames to the event data so you will know "who" (the end user) if not necessarily "where" (the specific endpoint).

Pool of Values to Support Multiple VMs

If you wish to be more specific, the following technique could be used: create a pool of UUID values to be assigned to the AgentIdOverride and assign one from this pool when the machine spins up.

With this technique, as part of the VDI provisioning, Privilege Manager would trigger the basic inventory task to make sure that the server gets correct information on the machine name and details. You would want a pool of values rather than a random one to prevent spamming new agents. Reusing the values would keep that under control.

Managing Agent Trust and Certificates

This section discusses certificate management.

As of version 10.5, Privilege Manager validates agent certificates against the specific agent that was initially registered. There are two cases:

- All desktops using a single agentID: This case is fairly straightforward. A single certificate would be included as part of the desktop image which would match what was stored in the database for that ID and all of the communication would be accepted.
- A pool of IDs: In this case, there are two potential ways to do certificate management:
 - Method 1: Navigate to Admin > Configuration > Advanced; select the "Allow Agent Certificate Mismatch" option; turn on the option. (It is off by default.)
 - Method 2: Deploy the install code on machine imaging, as follows:
 - Add a registry entry in HKLM\Software\Arellia\Agent of type String and call it "InstallCode."
 - In the Privilege Manager console:
 - Navigate to Admin > Agents > "Installation Codes" tab.
 - Click "Copy" to copy the value displayed under Code.
 - Paste the copied value into the InstallCode registry entry.
 - Once this entry is set, then during the agent registration process, the agent sends this InstallCode up to the server along with whatever certificate it has. This overrides the database entry and allows that agent to communicate as long as it is up and running.

Minimizing Time Between VDI Deployment and Policy Enforcement

This section is about policy deployment.

In a non-VDI environment, when Privilege Manager deploys agents to desktops, there can be a significant delay between deployment and policy enforcement and it is not a concern because it is a one-time issue.

However, in the case of VDI, machines are created and recreated daily and this delay becomes a larger issue. In this case, you must make sure that the Client Items database, with the appropriate policies, is part of the initial desktop image. This file can be created in C:\ProgramData\Arellia\ClientItems and can be simply copied from a machine that has the agent deployed and all policies downloaded.

However, if any policy changes are made after image creation you would need to either update that file in the golden image or add a post-deployment step to run the Powershell script "C:\Program Files\Thycotic\Powershell\Arellia.Agent\UpdateClientItems.ps1" and trigger the virtual desktop to download the latest policy items.

Licensing Concerns with Windows 10 Amazon Workspaces

This section discusses licensing concerns, specifically with Windows 10 Amazon Workspaces.

Although Amazon claims to offer a Windows 10 VDI environment, what they offer is not technically speaking Windows 10. Rather, what they provide is a Windows Server 2016 environment running what they call Windows 10 Experience.

This means that when Privilege Manager inventories it, the Privilege Manger agent believes that it is running on a server class OS. Therefore, from a licensing perspective, Amazon Workspaces need to be licensed as servers, rather than as clients.

This topic is a collection of articles covering maintenance procedures for different areas of the Privilege Manager product.

The following topics are available:

- [How to Purge Computers](#)
- [How to Purge the Action Items Table](#)
- [Using the Remove Programs Utility](#)
- [Export and Import Items](#)
- [Migrate Local Security Policies](#)

After using Privilege Manager for a certain amount of time, you may have computers that haven't communicated with the Privilege Manager server for an extended period of time. This can be done via the Purge Computers task, which can be found under Configuration on the General tab.

1. Navigate to **Admin | Configuration** and select the **General** tab.
2. Under the Maintenance Settings section click **Purge Old Computers**.

Configuration

General | Discovery | Reputation | Credentials | Foreign Systems | Roles | Advanced | Authentication | Change History

Policy Targeting ⓘ

Run Policy Targeting Update

Approval Types

Approval Types
Default Execute Application Request Type
Default Offline Execute Application Request Type

Approval Processes

Approval Processes
Default Manual Approval Process

Maintenance Settings

Assign Orphaned Agent Uploads
Copy of Purge Maintenance - Agent Logs
Delete Old Performance Counter Events
Initialize Item Change History
LSS Migration Task (1/2): Migrate all Items.
LSS Migration Task (2/2): Enable migrated items.
Maintenance Tasks
Purge Maintenance - Agent Logs
Purge Maintenance - Application Control Events
Purge Maintenance - Audit Events
Purge Maintenance - Completed File Upload Sessions
Purge Maintenance - Files Undiscovered
Purge Maintenance - Incomplete File Upload Sessions
Purge Maintenance - Message History
Purge Maintenance - Orphaned Local Users and Groups
Purge Old Computers

3. On the **Maintenance Task > Purge Old Computers** page select the **General SQL Executions** tab.
4. Verify that **Query 1** is set to **Purge Agent Gauge Data for Deleted Computers Query**.

Maintenance Task > Purge Old Computers

General | Schedule | **General SQL Executions** | Resource Purge SQL Executions

Query 1 Purge Agent and Gauge Data for Deleted Computers Query
Show Parameters

Back Edit Run Task History Create a Copy Delete View as XML Export

If that specific query is not listed,

1. Click **Edit** to either replace the query currently listed or add this query.
 2. Start typing the query name *Purge Agent Gauge Data for Deleted Computers Query* and select the query from the results list.
5. Select the Resource Purge SQL Executions tab.
6. Verify that **Query 1** is set to **Managed Computers to Delete**.

Maintenance Task > Purge Old Computers

General | Schedule | General SQL Executions | **Resource Purge SQL Executions**

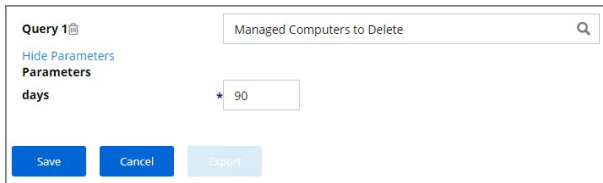
Query 1 Managed Computers to Delete
Show Parameters


Back Edit Run Task History Create a Copy Delete View as XML Export

If that specific query is not listed,

1. Click **Edit** to either replace the query currently listed or add this query.
 2. Start typing the query name *Managed Computers to Delete* and select the query from the results list.
7. Click **Show Parameters**. The Days field indicates after how many days a system is considered to be an old computer and thus should be purged. The default value is 90 days. If you want a different value,

1. Click **Edit** and change the number of days.



Query 1 

Managed Computers to Delete

Hide Parameters

Parameters

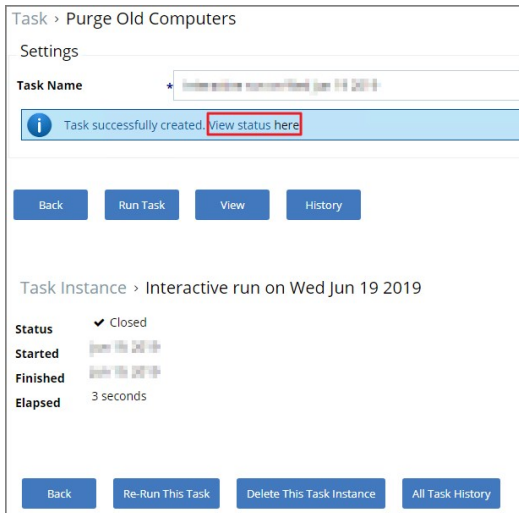
days 90

Save Cancel Export

1. Click **Save**.

8. Click **Run Task**


9. You can view the status of the running task by clicking the View Status here link.



Task > Purge Old Computers

Settings

Task Name * Interactive run on Wed Jun 19 2019

 Task successfully created. [View status here](#)

Back Run Task View History

Task Instance > Interactive run on Wed Jun 19 2019

Status Closed

Started Jun 19 2019

Finished Jun 19 2019

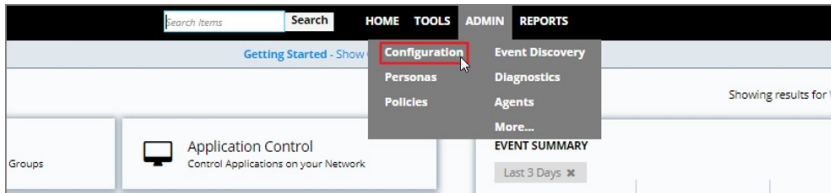
Elapsed 3 seconds

Back Re-Run This Task Delete This Task Instance All Task History

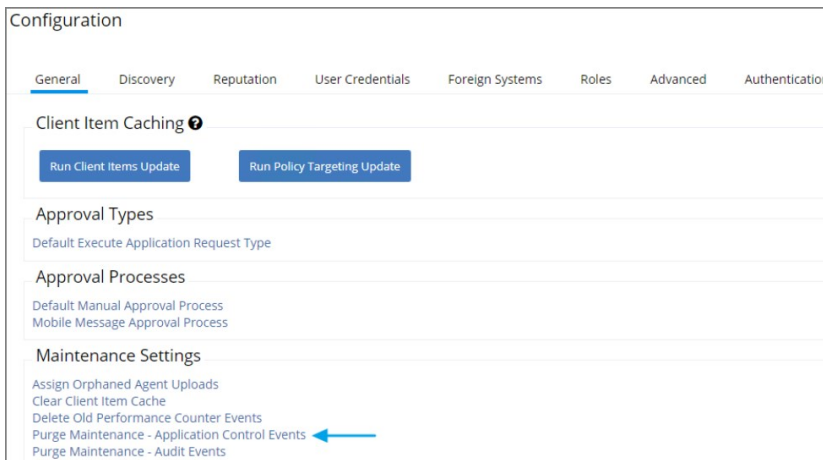
If the application action table frequently grows too large, you can use the steps below to create a scheduled event to purge old application action events.

Creating a Scheduled Event for Purging

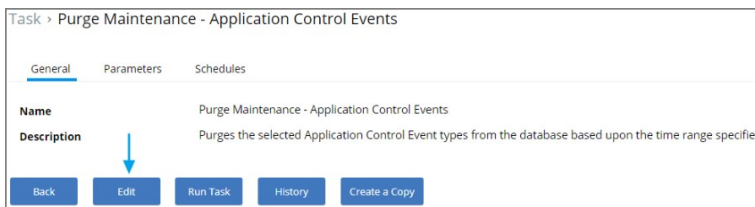
1. Launch **Privilege Manager**.
2. Click **ADMIN | Configuration**.



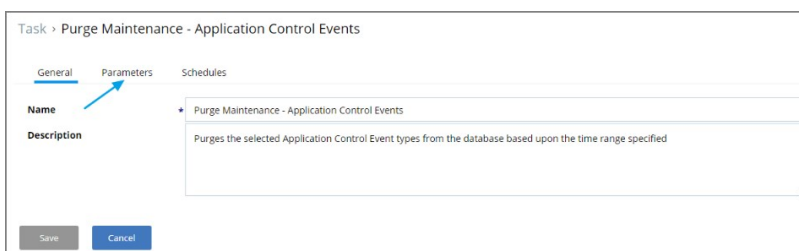
3. Click **Purge Maintenance – Application Control Events**.



4. Click **Edit**.



5. Click **Parameters**.



6. Select **Purge Application Action events** and the number of days.

Note: You can also select the other events to purge as well.

Task > Purge Maintenance - Application Control Events

General Parameters Schedules

Enter default parameter values for this task.

Purge Application Action events

Purge Application Justification events

Purge Application Metering events

Purge Application Verifier events

Max rows per chunk * 10000

Purge events older than * 30 Day(s) v

Only purge events from these policies + Add None Selected

Save Cancel

7. Click **Save**

Task > Purge Maintenance - Application Control Events

General Parameters Schedules

Enter default parameter values for this task.

Purge Application Action events

Purge Application Justification events

Purge Application Metering events

Purge Application Verifier events

Max rows per chunk * 10000

Purge events older than * 30 Day(s) v

Only purge events from these policies + Add None Selected

Save Cancel

8. Click **Schedules**

Task > Purge Maintenance - Application Control Events

General Parameters Schedules

Enter default parameter values for this task.

Purge Application Action events

Purge Application Justification events

Purge Application Metering events

Purge Application Verifier events

Max rows per chunk * 10000

Purge events older than * 30 Day(s) v

Only purge events from these policies + Add None Selected

Save Cancel

9. Click **New Schedule**

Task > Purge Maintenance - Application Control Events

General Parameters Schedules

NAME	SUMMARY
------	---------

New Schedule

Save Cancel

10. Enter in a **Schedule name** and the frequency you want the task to run.

Task Schedule > New Task Schedule

Task to run Purge Maintenance - Application Control Events

Schedule name * **New Task Schedule**

Schedule Parameters

At predefined schedule

At date/time

Once

Daily

Weekly

Monthly

Starting * 11/2/2019 8:00 AM UTC

Recur every * 1 day(s)

Show Advanced

Save Cancel

11. Click **Save**.

The Remove Programs Utility provides a solution to the following problem that Windows standard users are not able to remove applications from the control panel because of Windows checking for admin rights. This utility is available for deployment via Privilege Manager.

Customers can use this utility in any of the following ways:

- Allow users to uninstall any and all applications by using the utility.
- Make the utility show an approval request for each uninstaller that is launched.
- Make the utility show an approval prompt when it launches.

The utility will list all the same applications as the Remove Programs in the Control Panel, but it can also hide software that end users should not be able to uninstall (such as the Thycotic agents).

With Privilege Manager version 10.7 Thycotic is introducing support for Windows 10 **Apps & Features** and the management of Windows Store apps via the **Remove Programs Helper**. Certain apps designed as a Windows 10 package are registered in **Apps & Features** but do not appear in the operating systems Add Remove Programs options. Privilege Manager locates those applications and provides management via the enhanced **Remove Programs Utility**.

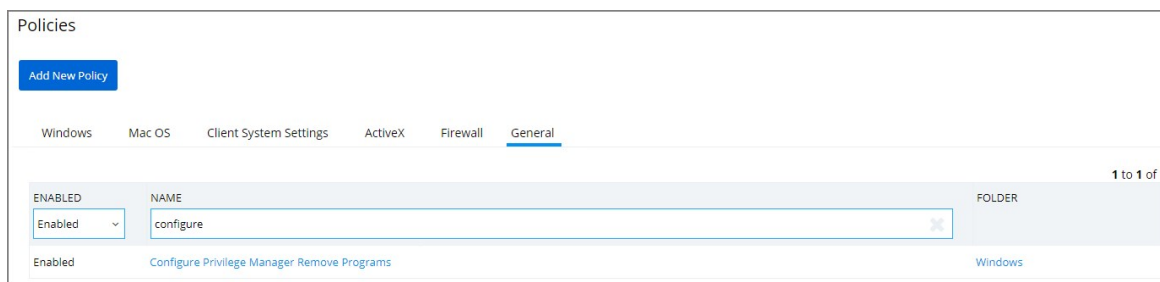
Using the Configure Privilege Manager Remove Programs Policy

With the Privilege Manager 10.7 release the Remove Programs Utility has moved from being delivered via configuration feed to being fully integrated and delivered via the Server and Agent installation packages.

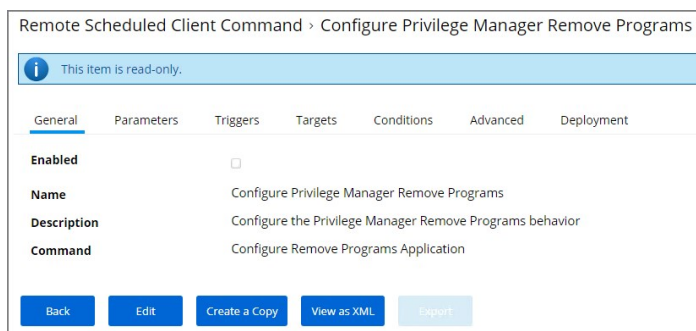
To allow standard users to use the utility refer to the [Elevating the Privilege Manager Remove Programs Utility Policy](#) set-up instructions.

Configuring the Remove Programs Utility

1. Navigate to **Admin | Policies** and select to the **General** tab.
2. Search for **Configure Privilege Manager Remove Programs**.

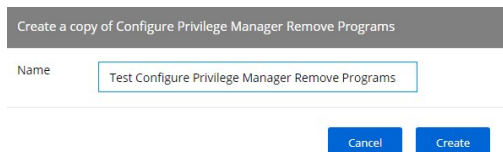


3. Click on the policy link **Configure Privilege Manager Remove Programs**.



If you need to customize the default policy, Thycotic recommends to create a copy.

4. Click **Create a Copy** and name your policy.



5. Click **Edit** to customize any of the defaults for the policy. Several parameters and attributes are available for customization in the various tabs on the page. On the
 - o **General** tab, enable your policy and verify the command is set to **Configure Remove Programs Application**.

Remote Scheduled Client Command > Test Configure Privilege Manager Remove Programs

General Parameters Triggers Targets Conditions Advanced Deployment

Enabled

Name * Test Configure Privilege Manager Remove Programs

Description Configure the Privilege Manager Remove Programs behavior

Command * Configure Remove Programs Application

Save Cancel Export

Set the policy to enabled by checking **Enabled**.

- Parameters tab, customize the access and functions of the utility. For example, choose whether a shortcut on the start menu or on the control panel should be created.

General Parameters Triggers Targets Conditions Advanced Deployment

Enter default parameter values for this task.

Create Start Menu Shortcut

Add to Control Panel

Hide Repair for All Installers

Hide Modify for All Installers

Hide Windows 10 Apps in List

Show Blocked Installers in List

Ignore NoRemove Flag in Registry

Products that can't be Uninstalled

Vendor software that can't be Uninstalled

Save Cancel Export

List products that you want to prevent being uninstalled. There are two options for this:

- If the "Show Blocked Installers in List" option is unchecked, the products will be hidden.
- If the "Show Blocked Installers in List" option is checked, the products will just be disabled from being uninstalled.

If you selected "Create Start Menu Shortcut", the users will see Privilege Manager Remove Programs on the Start Menu. If you selected "Add to Control Panel", the users will see Privilege Manager Remove Programs in the Control Panel.

- Triggers tab, customize when to run the utility for inventory purposes. This determines how often you want the policy from the Task Scheduler on the endpoint to check to ensure the settings match.

General Parameters Triggers Targets Conditions Advanced Deployment

TRIGGERS (WHEN TO RUN)

Daily at 10:00:00 PM starting Tue Jul 31 2018 (repeating every 2 hours for a duration of 24 hours)

Upon task creation/modification

Save Cancel Export

- Advanced tab, customize additional conditions that impact running the task, e.g. allowing the utility to be used on demand.

General Parameters Triggers Targets Conditions **Advanced** Deployment

Specify additional settings that affect the behavior of the task.

Allow task to be run on demand

Run task as soon as possible after a scheduled start is missed

If the task fails, attempt to restart every 0 minute(s)

Attempt to restart up to 0 time(s)

Stop the task if it runs for longer than 0 minute(s)

If the running task does not end when requested, force it to stop

If the task is not scheduled to run again, delete it after 0 minute(s)

If the task is already running, then the following rule applies

Default (Do not start a new instance) v

Save Cancel Export

- **Deployment** tab, users can see information about the policy status, when modified and total resources targeted. The tab also offers a Refresh Status option.

General Parameters Triggers Targets Conditions Advanced **Deployment**

Policy Deployment

Policies are automatically deployed to targeted managed computers on a schedule. Use the Policy Deployment tab to understand the status of a particular Policy in relation to the end points.

Refresh Status Run Policy Targeting Update

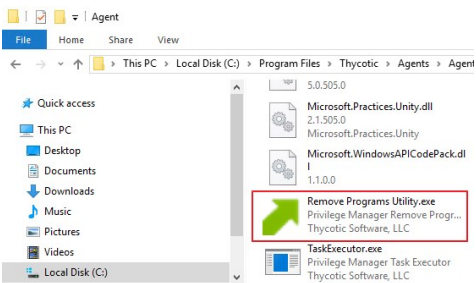
Policy Modified Nov 8, 2019, 6:32:01 AM

Total Resources Targeted 0

Resources with Latest Version

Save Cancel Export

1. Click **Save** to save all changes you made.



Use the Utility

The utility is straightforward to use. It's installed on endpoints as part of the Agents installation. Users can select the row containing the program that they want to uninstall and then select the uninstall button.

Name	Publisher	Installed On	Size	Version
3D Viewer	Microsoft Corporation			7.1908.9012.0
Alarms & Clock	Microsoft Corporation			10.1906.1972.0
Calculator	Microsoft Corporation			10.1908.0.0
Calendar	Microsoft Corporation			16005.12026.20218.0
Camera	Microsoft Corporation			2019.821.30.0
Feedback Hub	Microsoft Corporation			1.1903.2331.0
Get Help	Microsoft Corporation			10.1706.22112.0
Groove Music	Microsoft Corporation			10.19072.14111.0
MS 10.0 Express	Microsoft Corporation	9/16/2019 12:00:00 AM	53 MB	10.0.03203
Mail	Microsoft Corporation			16005.12026.20218.0
Maps	Microsoft Corporation			5.1906.1972.0
Messaging	Microsoft Corporation			4.1901.10241.1000
Microsoft .NET Core SDK 2.1.802 (x64)	Microsoft Corporation		491 MB	2.1.802
Microsoft Azure Authoring Tools - v2.9.6	Microsoft Corporation	9/16/2019 12:00:00 AM	12 MB	2.9.8899.26
Microsoft Azure Compute Emulator - v2.9.6	Microsoft Corporation	9/17/2019 1:18:36 AM		2.9.8899.26
Microsoft Azure Libraries for .NET - v2.9	Microsoft Corporation	9/16/2019 12:00:00 AM	67 MB	3.0.0127.060

In Privilege Manager Administrators need the ability to export complete policies, including dependent filters, actions, resource targets and any related items. They also need the ability to then import those policies into another instance.

The export and import feature can be used for production environments with multiple instances and for troubleshooting purposes when assistance is needed.

The feature provides the ability

- to export single policies for specific troubleshooting purposes.
- to bulk export via policies folders at any given folder level, except on root folders, depending on specific needs.
- to choose to overwrite or leave in place what's already there.
- to select specific objects or bulk select

This feature supports the bulk migration and creation of policies, including all of their dependencies.

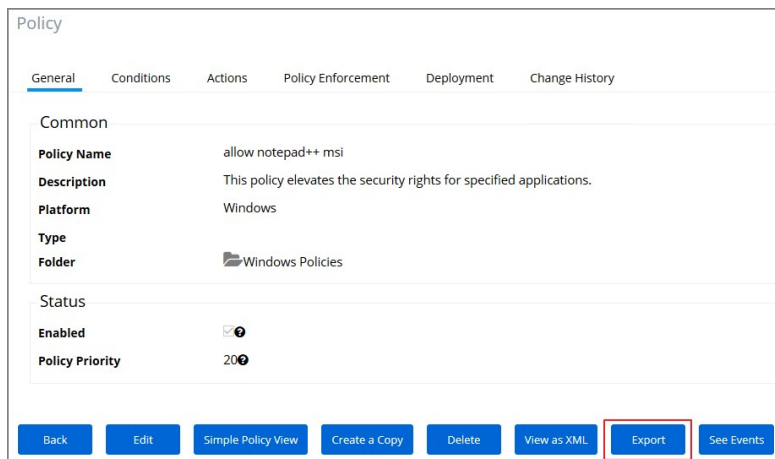
Exporting Items

Items at various levels of complexity can be exported. The UI offers several access points for an export operation.

Specific Policy Export

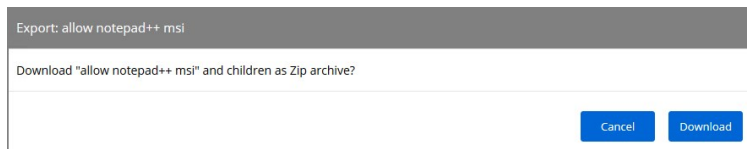
To export a specific policy with dependent filters and actions:

1. Navigate to the specific Policy and select it.



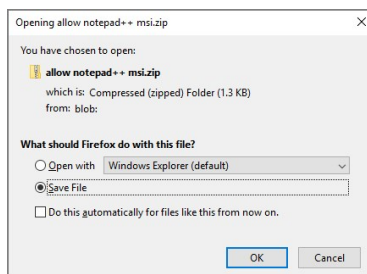
2. On the **General** tab in the bottom row of buttons, the second from the right is Export. Click that **Export** button.

3. A modal opens asking the user to confirm the download of the specific policy.



Click **Download**.

4. A file opening or save dialog opens, select **Save** file (and optionally check "Do this automatically for files like this from now on.").



5. Click **OK**

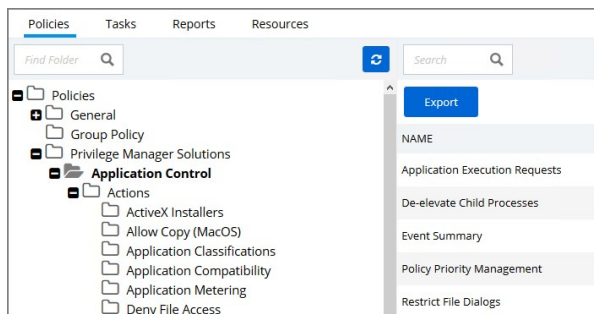
The policy details are downloaded in a zip file named after the policy name that was selected for export. The zip file contains one items.xml file with all the exported data. Extract the zip file and open/edit the exported xml.

The export of filters, tasks, or reports is done in a similar way, by navigating to the specific item, locating the Export button and proceeding through the export process steps.

Folder Exports

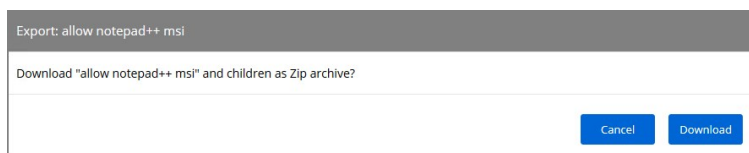
Bulk export of items is possible via the Folders page.

1. Navigate to **Admin | More** and select **Folders**. The export of folders is available on the Policies, Tasks, Reports, and Resources tabs. On the Resources tab, the export is only possible for Resource Filters.
2. From the folders tree select any of the available folders.



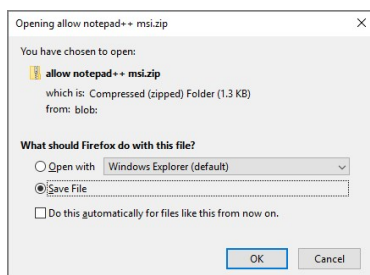
Click **Export**.

3. A modal opens asking the user to confirm the download of the specific policy.



Click **Download**.

4. A file opening or save dialog opens, select **Save** file (and optionally check "Do this automatically for files like this from now on.").



5. Click **OK**.

The items are downloaded in a zip file named after the folder that was selected for export. The zip file contains one items.xml file with all the exported data. Extract the zip file and open/edit the exported xml.

Importing Items

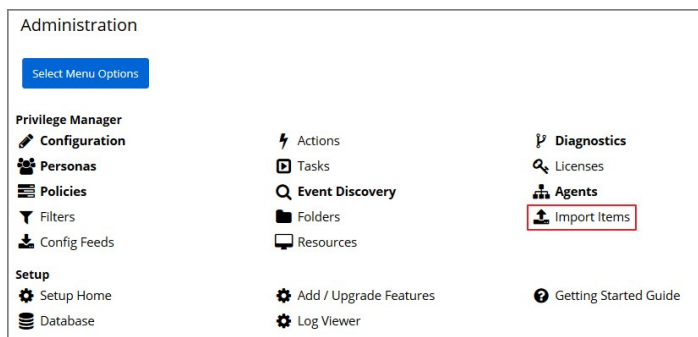
Note: Prior to importing any data into your environment, Thycotic recommends to create a backup of the current Privilege Manager Database.

Items can be imported in different ways, which are further detailed below.

Using Import Items

To import items via the Import Items link follow these steps:

1. Navigate to **Admin | More** and select the **Import Items** link.



2. The xml viewer opens and you may copy xml item data here to import.

Import Items

New Item(s)

i You can import a single item or multiple items (<items>...</items>)

1

Back Import Cancel

[Upload Items File](#)

Or use the **Upload Items File** option as described under [Using Diagnostics Upload Items File](#) step 2.

Using Diagnostics Upload Items File

To import items via file upload follow these steps:

1. Navigate to **Admin | Diagnostics** and select the **Import Items** button.

Diagnostics

i This page shows you general diagnostics about your environment that can be used to troubleshoot issues or submit to Technical Support.

Back Clear Descriptive Item Cache Clear Local Storage Cache Import Items Console Logs

2. Scroll to the bottom of the page and select the **Upload Items File** link.

Back Import Cancel

[Upload Items File](#)

3. The **Import Items** dialog opens, browse to your file location and select the file containing the data to import.

Import Items

File

Choose File No file chosen

Overwrite Existing Items

Cancel Upload

Supported file types for the import are .xslt, .xbl, .xsl, .xml, and .zip.

By default the **Overwrite Existing Items** checkbox is selected. If you want to skip items that already exist, un-check the box.

4. Click the **Upload** button.

You can verify the uploaded data by navigating to **Admin | More** and selecting **Folders**. Depending on your import, the data is listed under Policies, Tasks, or Resource Filters.

Troubleshooting

This section contains a collection of troubleshooting articles to help with problems that might occur in your Privilege Manager integration/instance.

The following troubleshooting topics are available:

- [Troubleshooting Installation Issues](#)
- [10.5 Folder Permission for MachineKeys](#)
- [Retrieving the COM class factory error](#)

- [Agent Registration Error Following an OS Upgrade](#)
- [Running updateclientitems.ps1 on an Agent triggers an error](#)
- [Client Item List Downloads](#)
- [Advanced Messages not working for child processes of Microsoft Edge](#)

- [Where are My Server Logs?](#)
- [Where are My Agent Logs?](#)
- [SQL Server Transaction Log](#)
- [User Interface and Ports](#)

- [Improve Boot-up Performance](#)
- [Unable to access Privilege Manager](#)

- [Common Errors](#)
- [Error: Could not allocate space for object](#)
- [UI Storage Error Message](#)
- [Notify User Justification failed](#)
- [Invalid Product Identifier](#)
- [Installation Hangs with Error: Worker Role Monitor received exception during ping](#)

- [Endpoint Troubleshooting](#)
- [How to Recover an Unresponsive macOS Endpoint](#)
- [Catalina FileSystemWatcher Issue](#)

- [How to use the Thycotic Monitor for Troubleshooting](#)
- [Using Process Hacker for Troubleshooting](#)
- [Troubleshooting a Policy with Process Explorer](#)

The following topics for agents troubleshooting are available in this section:

- [Advanced Messages not working for child processes of Microsoft Edge](#)
- [Agent Registration Error Following an OS Upgrade](#)
- [Running updateclientitems.ps1 on an Agent triggers an error](#)
- [Client Item List Downloads](#)

While running the updateclientitems.ps1 powershell script on a machine, you receive the following error:

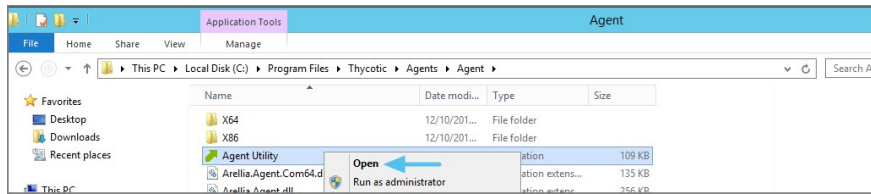
"KeySet does not exist"

```
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\UpdateClientItems.ps1
-----
Client Items
-----
[FAILED] Downloading Windows Group Policies client item list
Keyset does not exist
```

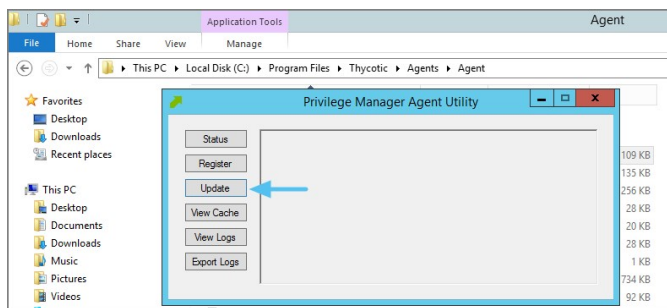
Note: The best practice to updating policies on machines would be to run the Agent Utility versus the PowerShell script. If you are still receiving the same error when using the Update button on the Agent Utility, open up a support case and include a screenshot of the error in the Agent Utility along with the agent logs.

1. Navigate to the Machine(s) where you want to update the policy and open the Agent Utility.

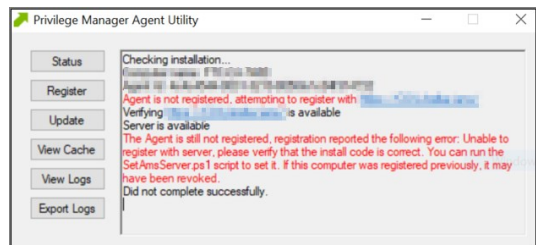
C:\Program Files\Thycotic\Agents\Agent



2. Select **Update**.



After upgrading, you encounter the following issue with the Agent utility after selecting "Register".



This can be caused by a Windows OS upgrade due to either a new version or build. The certificate changes and the agent will need to be re-configured for the new certificate.

Detailed Information

A. Uninstall and reinstall the agent on the machine.

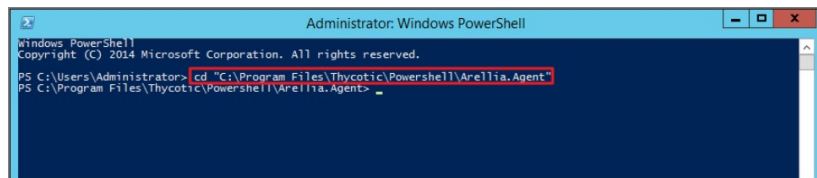
Or

B. Run the following PowerShell scripts to re-configure the agent.

Using a PowerShell Script

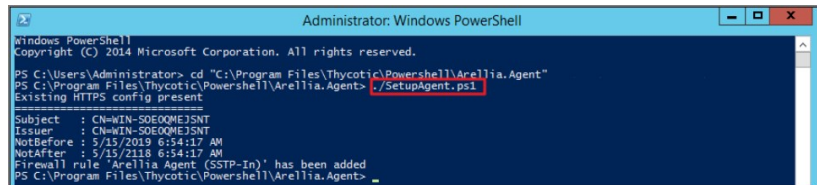
1. Right-click on **Windows PowerShell** and **Run as Administrator**.
2. Enter in the following command:

```
cd "C:\Program Files\Thycotic\PowerShell\Arellia.Agent"
```



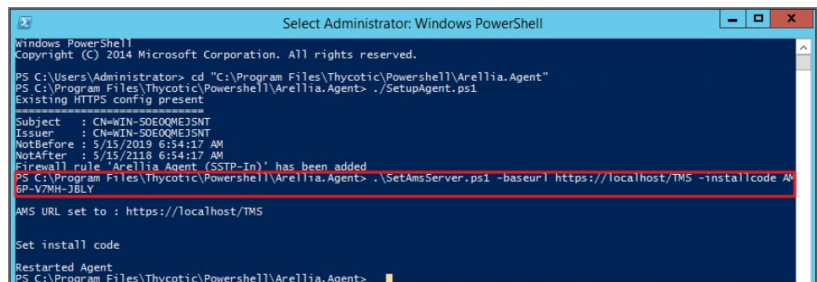
3. Enter in the following command:

```
.\SetupAgent.ps1
```



4. Enter in the following command:

```
.\SetAmsServer.ps1 -baseurl https://servername/TMS -installcode ???-???-???
```



5. Enter in the following command:

```
.\UpdateClientItems.ps1
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd "C:\Program Files\Thycotic\Powershell\Arellia.Agent"
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\SetupAgent.ps1
Existing HTTPS config present
=====
Subject       : CN=WIN-S0E0QMEJ5NT
Issuer        : CN=WIN-S0E0QMEJ5NT
NotBefore     : 5/15/2019 6:54:17 AM
NotAfter      : 5/15/2118 6:54:17 AM
Firewall rule 'Arellia Agent (SSTP-In)' has been added
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\SetAmsServer.ps1 -baseurl https://localhost/TMS -installcode AM
6P-V7MH-JBLY
AMS URL set to : https://localhost/TMS

Set install code

Restarted Agent
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\UpdateClientItems.ps1
=====
Client Items
=====
Refreshing Agent Commands: 7/31 client items
Refreshing Agent Gauges: 0 client items
Refreshing Agent Policies: 17/61 client items
Refreshing Application Actions: 2/41 client items
Refreshing File Filters: 2/292 client items
Refreshing Provisioned Resources: 0/1 client items
Refreshing Scap Entities: 0 client items
Refreshing Windows Group Policies: 0/1 client items
Refreshing Windows Group Policy Settings: 0 client items

No client item updates required

Last client item update: Force Client Item Update Command - 2 minutes ago

=====
Policies
=====
Last added policy: Global Process Monitor - 3 hours ago
Last updated policy: Global Process Monitor - 2 hours ago
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent>
```


When you run the UpdateClientItems.ps1 PowerShell script to update policies on a machine you see errors below:

```
PS C:\Program Files\Thycotic\Powershell\Arellia.Agent> .\UpdateClientItems.ps1
*****
Client Items
*****

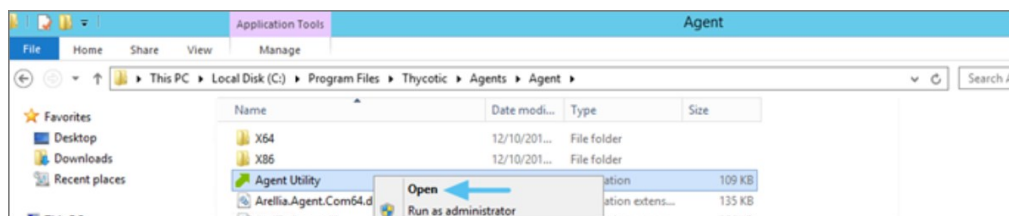
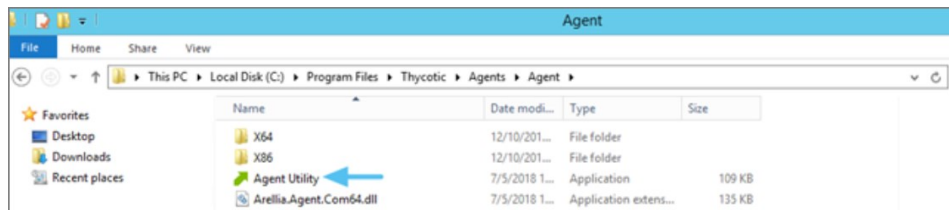
[FAILED] Downloading Windows Group Policies client item list
Keyset does not exist
```

Error: [FAILED] Downloading Windows Group Policies client item list - Keyset does not exist

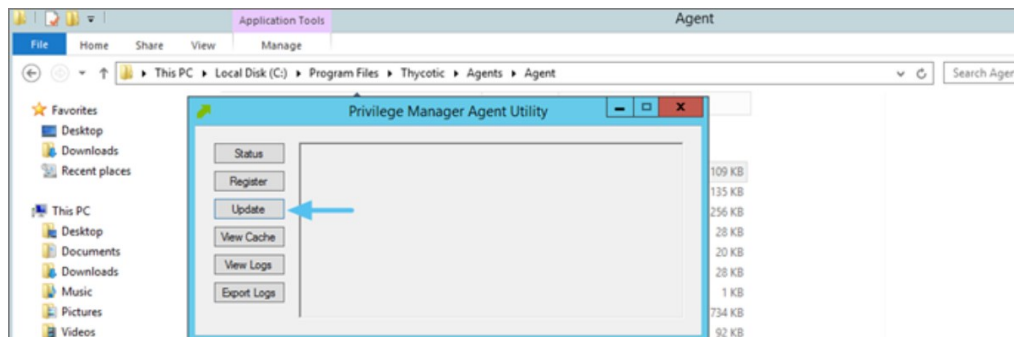
Note: This will only affect systems prior to Privilege Manager 10.7.

Resolve

1. Navigate to the Machine(s) where you want to update the policy.
2. Open the Agent Utility by going to C:\Program Files\Thycotic\Agents\Agent



3. Click **Update**.



When opting to Run an application from Microsoft Edge on Windows 10 version 1803, Advanced Messages for application justification or approval are not honored.

Detailed Information

If an application control policy targets an application such as the Google Chrome installer, the approval or justification messages will prevent the process from continuing until the message prompt is completed. However, when choosing the "Run" option when downloading an application in Microsoft Edge, the process will be created under the browser_broker.exe service and in Windows 10 version 1803 the process continues and does not wait for the Privilege Manager message to be completed.

Other versions of Windows 10 and Microsoft Edge do not appear to have this issue.

Workaround

An application control policy can be created to block browser_broker.exe and prevent users from using the "Run" option in Microsoft Edge.

Alternatively, upgrading Windows 10 will also fix the issue.

The following topics about Endpoint Troubleshooting are available:

- [Endpoint Troubleshooting](#)
- [How to Recover an Unresponsive macOS Endpoint](#)
- [Catalina FileSystemWatcher Issue](#)

This topic is intended to assist users in troubleshooting issues (such as policies not yielding expected results) from an endpoint machine that has the Thycotic agent installed on it.

Agent Install Codes

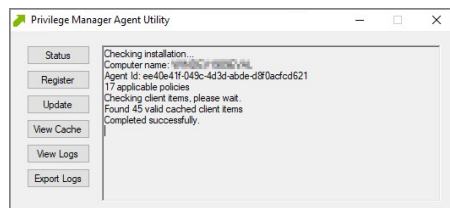
Privilege Manager version 10.5 and above will require an installation code when installing the latest agent on an endpoint. This is a code for only one-time use and is removed from the endpoint after the agent is installed. Refer to the [Agent Install Codes](#) topic for further details.

If it becomes necessary to set the install code after the agent is installed, an install code can be set using a PowerShell script that must be run as an Administrator. This script, along with other useful agent scripts, will be located in the C:\Program Files\Thycotic\PowerShell\Arelia.Agent folder on any machine with the Thycotic agent installed and is called **SetAMSServer.ps1**. The script will request parameters, as follows:

- The first parameter the script will request is the URL of the server you wish to connect to; its value should be `https://PrivilegeManagerURL/TMS/`.
- The second parameter it will ask for is the install code.

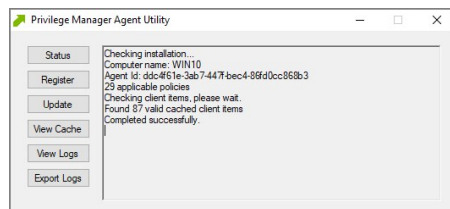
Agent Utility

Most endpoint troubleshooting will begin with the agent. There is an Agent Utility that is installed with the agent, used to troubleshoot issues from the endpoint. To open the utility, navigate to the `C:\Program Files\Thycotic\Agents\Agent` folder on the endpoint, and run the **Agent Utility.exe** application. That will launch the utility, and it will look like the screenshot below.



Status Button

The Status button will check that the endpoint can communicate with the server and will show you helpful information (such as the Agent ID and how many policies the machine has) and will validate the client items cache. It is also helpful in determining if there are any communication issues between the endpoint and the web server. Below is a screenshot of the information shown after clicking on the Status button.



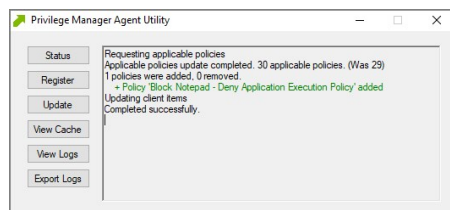
Register Button

The Register button will attempt to register the agent machine with the web console. It will show you the URL that the machine is using to communicate with the console. It will also give errors if there are issues with that communication. If you have just installed an agent on the machine, then it will also give information about the install code if there are any errors with that.



Update Button

The Update button will communicate back to the web server and update any new applicable policies or changes to current policies, filters, actions, etc. the endpoint already has on it.



View Cache Button

The View Cache button will open the Agent Cache Viewer in a separate window. It displays the Policies, Filters, and Actions the endpoint has cached currently.

Type	Name	Last Updated
Agent Policies	Retry errored TMS Events (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Local User Inventory Policy	10/18/2019 12:34:06 PM
Agent Policies	Cleanup Agent Inventory Transfers (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Scheduled Check Pending Client Tasks - Cloud (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Update Applicable Policies (Windows)	10/18/2019 12:34:06 PM
Agent Policies	Perform Resource Discovery (Windows)	10/18/2019 12:34:06 PM

Starting with Privilege Manager version 10.7 the Client Item Cache is list also searchable. Enter a search term into the search bar and just review items that contain that term.

Type	Name	Last Updated
Agent Commands	Force Client Item Update Command	10/21/2019 5:56:17 AM

View Logs

Clicking on the View Logs button will open the Agent Log Viewer in a separate window. The screenshot below shows what the log viewer looks like.

TimeGenerated	Message	Source	Module
2018-09-14 09:44:26	No policies applies to process 5152 (C:\Windows\System32\audiodg.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control
2018-09-14 09:44:26	DoProcessWork Ignoring Process 6176 (C:\Windows\System32\svchost.exe) as it is a protected process. Source: C:\font	C:\font\Process	Application Control
2018-09-14 09:44:25	No policies applies to process 5560 (C:\Windows\System32\backgroundtaskhost.exe) Source: CASMonitor Module: Avel	CASMonitor	Application Control
2018-09-14 09:44:24	No policies applies to process 4184 (C:\Program Files\Thyrotic\Agents\Agent\Thyrotic.Agent\User.exe) Source: CASMo	CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Program Files\Thyrotic\Agents\Agent\Thyrotic.Agent\User.exe last updated 2018-09-04	CFEScanEngine	Application Control
2018-09-14 09:44:24	Policy Block Notepad - Deny Application Execution Policy (8-3x25ee-1b6e-43b1-9605f08b-9f08ca) priority 31 applied	CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Windows\System32\notepad.exe last updated 2018-09-06 12:07:54. Source: CFEScanE	CFEScanEngine	Application Control
2018-09-14 09:44:24	No policies applies to process 6202 (C:\Windows\System32\smartscreen.exe) Source: CASMonitor Module: AvebaACSvc	CASMonitor	Application Control
2018-09-14 09:44:18	No policies applies to process 6036 (C:\Windows\System32\dfhost.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control
2018-09-14 09:44:18	No policies applies to process 4332 (C:\Windows\System32\dfhost.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control

Export Logs Button

Clicking on the Export Logs button will allow you to save the agent logs so that you can send them to someone if needed. They will be saved in the .evtx format so they can be opened with Event Viewer in Windows. Anytime there are issues with policies on endpoints and you need additional assistance, you will need to collect the agent logs first to help with determining what is causing the issue.

Policy Troubleshooting

If there is an issue with policies not getting updated on the endpoint, or specific files or applications not being elevated or blocked, please use the information below to help determine what is causing the issue.

Policies Not Getting Updated

If policies are not getting updated on the endpoint, there could be a communication issue between the machine that has the agent installed on it and the web server. The best way to determine if there is a communication issue would be to open the Agent Utility on the endpoint as described in the previous section, and then do the following:

1. Click on the Status button and see if there are any errors shown.
2. Click on the Register button and check for errors shown there.
3. Click on the Update button and check for errors there as well.

If there is an issue with the endpoint communicating with the web server, there will be errors displayed in red after clicking on those buttons.

Specific Files or Applications Not Being Elevated or Blocked

If specific files or applications are not being elevated or blocked properly, then you will need to look in the Agent Logs on the endpoint. You can open the logs by first opening the Agent Utility on the machine. Once that is open, click on the View Logs button to bring up the Agent Log Viewer.

The Agent Log Viewer is very helpful for troubleshooting issues with policies not applying correctly. In the log, you can see if a policy applied to a certain process, and if so, what policy applied to that process. You can also see if there was no policy that applied to that specific process.

For example, in the screenshot below of the Agent Log Viewer, you will see a policy called "Block Notepad - Deny Application Execution Policy" that has been applied to the endpoint.

TimeGenerated	Message	Source	Module
2018-09-14 09:44:26	No policies applies to process 5152 (C:\Windows\System32\audiodg.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control
2018-09-14 09:44:26	DoProcessWork Ignoring Process 6176 (C:\Windows\System32\svchost.exe) as it is a protected process. Source: C:\font	C:\font\Process	Application Control
2018-09-14 09:44:25	No policies applies to process 5560 (C:\Windows\System32\backgroundtaskhost.exe) Source: CASMonitor Module: Avel	CASMonitor	Application Control
2018-09-14 09:44:24	No policies applies to process 4184 (C:\Program Files\Thyrotic\Agents\Agent\Thyrotic.Agent\User.exe) Source: CASMo	CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Program Files\Thyrotic\Agents\Agent\Thyrotic.Agent\User.exe last updated 2018-09-04	CFEScanEngine	Application Control
2018-09-14 09:44:24	Policy Block Notepad - Deny Application Execution Policy (8-3x25ee-1b6e-43b1-9605f08b-9f08ca) priority 31 applied	CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Windows\System32\notepad.exe last updated 2018-09-06 12:07:54. Source: CFEScanE	CFEScanEngine	Application Control
2018-09-14 09:44:24	No policies applies to process 6202 (C:\Windows\System32\smartscreen.exe) Source: CASMonitor Module: AvebaACSvc	CASMonitor	Application Control
2018-09-14 09:44:18	No policies applies to process 6036 (C:\Windows\System32\dfhost.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control
2018-09-14 09:44:18	No policies applies to process 4332 (C:\Windows\System32\dfhost.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control

The highlighted entry on the screenshot above shows that the "Block Notepad - Deny Application Execution Policy" was triggered when notepad was opened. Double-click on the log entry to see further details as shown below. This shows the exact process that met the criteria of the policy and shows the priority number of that policy. The policy priority is useful information if the application continues processing through multiple policies.

TimeGenerated	Message	Source	Module
2018-09-14 09:44:26	No policies applies to process 5152 (C:\Windows\System32\audiodg.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control
2018-09-14 09:44:26	DoProcessWork Ignoring Process 6176 (C:\Windows\System32\svchost.exe) as it is a protected process. Source: C:\font	C:\font\Process	Application Control
2018-09-14 09:44:25	No policies applies to process 5560 (C:\Windows\System32\backgroundtaskhost.exe) Source: CASMonitor Module: Avel	CASMonitor	Application Control
2018-09-14 09:44:24	No policies applies to process 4184 (C:\Program Files\Thyrotic\Agents\Agent\Thyrotic.Agent\User.exe) Source: CASMo	CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Program Files\Thyrotic\Agents\Agent\Thyrotic.Agent\User.exe last updated 2018-09-04	CFEScanEngine	Application Control
2018-09-14 09:44:24	Policy Block Notepad - Deny Application Execution Policy (8-3x25ee-1b6e-43b1-9605f08b-9f08ca) priority 31 applied	CASMonitor	Application Control
2018-09-14 09:44:24	Hash being recalculated for C:\Windows\System32\notepad.exe last updated 2018-09-06 12:07:54. Source: CFEScanE	CFEScanEngine	Application Control
2018-09-14 09:44:24	No policies applies to process 6202 (C:\Windows\System32\smartscreen.exe) Source: CASMonitor Module: AvebaACSvc	CASMonitor	Application Control
2018-09-14 09:44:18	No policies applies to process 6036 (C:\Windows\System32\dfhost.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control
2018-09-14 09:44:18	No policies applies to process 4332 (C:\Windows\System32\dfhost.exe) Source: CASMonitor Module: AvebaACSvc.exe	CASMonitor	Application Control

With this information, you know that the policy applied to the Notepad process correctly. If there were other policies that applied to that same process, you would see them in the log viewer as well. There are certain situations in which clients will apply multiple policies to the same process. When troubleshooting issues with certain files or applications, the log viewer is a valuable tool to use.

If there is no policy that applies to a certain process, the Agent Log Viewer shows you that as well. In the screenshot of the log viewer, presented above in this section, you can notice entries showing that there are some processes to which no policies apply. Entries that begin with "No policies applies to process..." indicate that no policy was triggered when the application executed on the endpoint. If a client says that a specific file or application is not being blocked or elevated, then in the log viewer you can see what process is running when they launch the application and whether a policy is applying to that process.

If there are any Errors in the log viewer, they are shown in **Red**. Warnings are shown in **Blue**, and Informational messages are shown in Black.

On macOS Catalina there is a known issue, preventing the the agent from receiving notification of events that need to be sent to the server. To workaround this, the **Retry errored TMS Events - Catalina (macOS)** policy can be enabled to ensure all events get sent to the server.

The defaults for this new Remote Scheduled Client Command are as follows:

- On the General tab:

General	Triggers	Targets	Conditions	Advanced	Deployment
Enabled	<input checked="" type="checkbox"/>				
Name	Retry errored TMS Events - Catalina (macOS)				
Description	Scan Agent queue for any events that require retransmission.				
Command	Retry errored TMS Client Events (MacOS)				

- On the Triggers tab:

Customize the schedule if necessary to best suit your particular implementation.

General	Triggers	Targets	Conditions	Advanced	Deployment
TRIGGERS (WHEN TO RUN)					
<input type="radio"/> Daily at 2:00:02 AM starting Mon Oct 01 2018 (repeating every 5 minutes for a duration of 24 hours)					
Begin On a schedule					
<input type="radio"/> Once <input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly					
Starting 10/1/2018 02:00:02 <input type="checkbox"/> UTC					
Recur every 1 day(s)					
<input type="checkbox"/> Delay task for up to (random delay) 0 minute(s)					
<input checked="" type="checkbox"/> Repeat every 5 minute(s) for a duration of 1 day(s)					
<input type="checkbox"/> Stop all running tasks at end of repetition duration					
<input type="checkbox"/> Expire month/day/year hour:minute:seco... <input type="checkbox"/> UTC					

- On the Targets tab:

The default resource targets required are specified by default as **All macOS Catalina Computers with Application Control Agent Installed (Target)**. The results of the computer group include any macOS Catalina computers that have the agent installed and are properly configured for Application Control.

Computer Group Name	All macOS Catalina Computers with Application Control Agent Installed (Target)		
Description	All macOS Catalina Computers with Application Control Agent Installed (Target)		
Folder	MacOS		
Show in Left Menu	No		
Filter Rules	Results	Related Policies	
Filter Rules			
RULE #	OPERATION	LIST TYPE	SELECTED ITEMS
Start with all computers			
1) THEN	Include Computers in	Filter	Application Control Agent Installed
2) THEN	Only Keep Computers in	Filter	All macOS Catalina Computers

- On the Conditions tab:

General	Triggers	Targets	Conditions	Advanced
Specify the conditions that, along with the trigger, determine whether the task is to be performed.				
Idle				
<input type="checkbox"/> Start the task if the computer is idle for 0 minute(s)				
<input type="checkbox"/> Wait for idle for 0 minute(s)				
<input type="checkbox"/> Stop if the computer ceases to be idle				
<input type="checkbox"/> Restart if the idle state resumes				
Power				
<input checked="" type="checkbox"/> Start the task only if the computer is on AC power				
<input checked="" type="checkbox"/> Stop if the computer switches to battery power				

- On the Advanced Tab:

General Triggers Targets Conditions **Advanced**

Specify additional settings that affect the behavior of the task.

- Allow task to be run on demand
- Run task as soon as possible after a scheduled start is missed
- If the task fails, attempt to restart every
Attempt to restart up to
- Stop the task if it runs for longer than
- If the running task does not end when requested, force it to stop
- If the task is not scheduled to run again, delete it after

If the task is already running, then the following rule applies

Default (Do not start a new instance) ▾

Once the policy is enabled on an endpoint, the agent will perform the **Retry errored TMS Client Events (MacOS)** command and send any events that have not been sent.

In case a macOS endpoint ever becomes unresponsive due to conflicting policy configurations, the following steps allow user to recover the endpoint without having to restore or rebuild the system.

1. Turn off the macOS system.
2. Hold down the `⌘+s` keys and power the system back on. Keep holding those keys down until it shows that it is booting in single-user mode.
3. Follow the prompts to mount the root device as read-write. It will instruct you to enter the following:

```
/sbin/fsck -fy  
/sbin/mount -uw /
```

4. Rename the kernel extension so that you can get back to a functioning macOS:

```
cd /Library/Extensions  
mv ThycoticACS.kext ThycoticACS.kext.org  
exit
```

5. The system will restart.
6. Disable and/or delete policies that are causing the issue.
7. Update client items before renaming the kernel extension and having it start automatically. You can force client item updates by performing the following in Terminal.app:

```
sudo /usr/local/thycotic/agent/updateClientItems.sh
```

8. Restore the kernel extension in Terminal.app:

```
cd /Library/Extensions  
sudo mv ThycoticACS.kext.org ThycoticACS.kext  
exit
```

The following topics about error messages in Privilege Manager are available:

- [Common Errors](#)
- [Error: Could not allocate space for object](#)
- [UI Storage Error Message](#)
- [Notify User Justification failed](#)
- [Invalid Product Identifier](#)
- [Installation Hangs with Error: Worker Role Monitor received exception during ping](#)

Access Denied

Error: "Access Denied. You do not have permission to view this directory or page using the credentials that you supplied."

To Resolve:

After logging in to Privilege Manager 10.3 with a user account that has Privilege Manager Administrator Role rights, if you experience this error, verify if SSL 3.0 and/or TLS 1.0 have been disabled. If those protocols have been disabled on the server, you'll need to replace C:\inetpub\wwwroot\Tms\bin\Thycotic.Owin.Security.dll With http://tmsnet.thycotic.com/scripts/Thycotic.Owin.Security.dll

Recycle the TMS Application Pools in IIS and attempt to access Privilege Manager again.

Server Error in...

Error: "Server Error in '/' Application. Runtime Error"

Your Secret Server instance doesn't have the correct URL pointing at Privilege Manager.

To Resolve:

Go to your Secret Server instance (Tools | Secret Server). Then Admin | Configuration. Verify that your TMS Installation URL is set to ~/../TMS.

SSL Connectivity or Certificate Issues

Error: SSL Connectivity or Certificate Issues?

Trusting an SSL Certificate on a Client Machine (KB)

When a self-signed certificate is installed on a server for the Secret Server website, client computer browsers will generally give security warnings for that web site. This is because for public websites, only certificates issued by trusted authorities can be trusted as valid certificates. For certificates that will only be used within a company or domain, self-signed certificates the security warnings can generally be ignored.

However, the security warnings can also interfere with the use of the Secret Server Launcher and Web Password Filler. To resolve, the certificate can be installed on the client machine either through Internet Explorer or Certificates snap-in.

The following steps can be used to trust the certificate:

1. Make sure that the host to which the certificate is issued is the same as the host name for your Secret Server website.
 - o Open Internet Explorer and navigate to Secret Server
 - o Click Continue to this website if you are prompted
 - o Click the Certificate Error icon next to the navigation bar and then click View certificate. The value next to Issued to should match the host name for your website. For example, if your website is https://www.mydomain.local/SecretServer, it should say "Issued to: www.mydomain.local". If these fields do not match, the client will not be able to fully trust the certificate.
2. Obtain a copy of the certificate file and transfer it to the client computer.
 - o On the server that Secret Server is installed on, find Run from the start menu or screen and type in mmc, then hit Enter.
 - o From the File menu, select Add/Remove Snap-in.
 - o Select the Certificates snap-in, then click the right arrow button to add it.
 - o In the window that appears, select Computer Account, then Local Computer, and then click Finish.
 - o You should now see the Certificates (Local Computer) node. Expand the Personal folder and then the Certificates folder under it.
 - o Right-click the certificate that Secret Server uses, then click All tasks and select Export.
 - o Keep clicking Next to accept defaults in the wizard. Enter a filename, and then click Finish. The certificate has now been exported.
 - o Copy the certificate from your server and transfer it to your client computer. **Note:** If you have Firefox, the certificate can be saved to your client computer by viewing and exporting it after navigating to the website.
3. Install the certificate on the client computer.
 - o On the client computer, find Run from the start menu or screen and type in mmc, then hit Enter.
 - o From the File menu, select Add/Remove Snap-in.
 - o Select the Certificates snap-in, then click the right arrow button to add it.
 - o In the window that appears, select My user account, and then click Finish.
 - o Expand the Trusted Root Certification Authorities folder, then right-click the Certificates folder, and select All Tasks | Import.
 - o Click Next and Yes to accept default settings for all steps of the wizard.
 - o When prompted for the certificate file, select the file you saved in the previous step (2).

Note: You may need to reopen Internet Explorer and browse to Secret Server once more to see the change reflected on the client machine.

Granting Permissions on New SSL Certificate for Privilege Manager (KB)

If you change your certificate or if it is automatically renewed, you may need to grant permissions on your new SSL certificate to the service account that the TMS app pools run under. TMS accesses the SSL certificate to sign all of the policies that Privilege Manager sends out to agents, adding an extra security layer to your environment.

Messages you may see include:

- https: does not render
- Navigating to https://[ServerName]/TMS/PrivilegeManager loads a blank screen
- Agents stop receiving configuration information from the Privilege Manager Web Server.
- Http: TMS requires an https (SSL) / secure connection

For the fastest resolution to Permissions issues, you can run a Powershell script:

- Navigate to your TMS Website on your Privilege Manager web server (Usually located in c:\inetpub\wwwroot\), then navigate to Tms\App_Data\Tools\SSLHelper.ps1 on your Privilege Manager web server, right-click this and select Run with Powershell to execute.

To grant permissions manually, follow these steps

1. Using MMC on your Privilege Manager web server, open the certificates snap-in (File | Add/Remove Snap-in... | Certificates I click Add), then select Computer account to manage the local computer. Click Next, then Finish and OK.
2. Double click Certificates (Local Computer) and locate the certificate that your TMS site is using (it will most likely be under Personal\Certificates unless you specified a different location*)
3. Right click on the certificate and select All Tasks | Manage Private Keys

Grant Read Access to the account(s) that TMS is running under

If this is a user account then you may adjust permissions to the user account. To check, go to your app pool in IIS, right-click the IIS app pool | Advanced Settings... | "Identity" row: if your app pool "identity" is listed as something OTHER THAN "ApplicationPoolIdentity" in IIS, i.e. "THYCOTIC IServiceAccount", then your app pool is using a user account.

If this IS the Application Pool Identity (i.e. not a user account) you will need to adjust permissions to three app pools: "IIS AppPool\TMS", "IIS AppPool\TMSWorker" and "IIS AppPool\TMSAgent." Note that names of app pools may vary depending

on your environment.

Recycle your TMS, TMSAgent, and TMSWorker app pools in IIS.

Note: If you are unsure which certificate matches the one you are using in IIS, follow these steps to ensure your certificate thumbprints match:

In IIS on your Privilege Manager web server, navigate to the site you are using to run Privilege Manager Right-click on this site, click Bindings. Choose the https port you need to update and select Edit. View the SSL Certificate this is attached to.

Next, choose the Details tab and scroll down to find the certificate's Thumbprint. copy the list of numbers and letters that make up your certificate's thumbprint (an sha1 hash)

Return to your certificates in MMC (step 2 above). Right-click Certificates (Local Computer) and select Find Certificates...

In the Contains box, paste your Thumbprint sha1 hash and select sha1 from the Look in Field drop down. Click Find Now. This will return the certificate name that your Privilege Manager Binding is currently linked to.

Tasks Stuck at Ready

Error: Are your tasks sitting at "Ready" for extended periods of time?

To Resolve:

1. Navigate to Admin | Configuration | Advanced and make sure the URL for the "Monitor Worker Role" are accurate for the bindings (Check the hostname in the Base local address and the Port).
2. Open IIS Manager, check to make sure the app pools have Read Access to the certificate that you've assigned to that binding via MMC Certificates plug-in. More instructions on how to do this in our Granting Permissions on New SSL Certificate for Privilege Manager KB, posted here.
3. Manually recycle the TMS and TMS Worker app pools.

CPU Issue

Error: CPU overworked in your Agent or 'Unexpected failure in ACS Agent background'

Your agent may be configured incorrectly.

To Resolve:

1. In Privilege Manager navigate to Admin | Agents.
2. Under the Windows tab, verify that your "Send Application events every" and "Refresh Client item cache every" settings are both set to 0.
3. Save changes, refresh your client item cache, enforce the update on your endpoint machine (Follow the update Powershell script instructions listed under "How do I Update Specific Agents Immediately?" above).

System Critical Error

Error: 'System Critical Error - execute/PolicyDetailComponent' in Firefox

To Resolve:

Open Privilege Manager in a different browser, such as Chrome or Internet Explorer 11. If you prefer Firefox as your web browser, download this zip file: <http://tmsnugget.thycotic.com/scripts/firefox.fix.zip> Unzip these files, then copy and paste into C:\inetpub\wwwroot\Tms\Spa\PrivilegeManager\ on your Privilege Manager Server.

Refresh your Firefox browser.

This topic describes the following error while working with Privilege Manager:

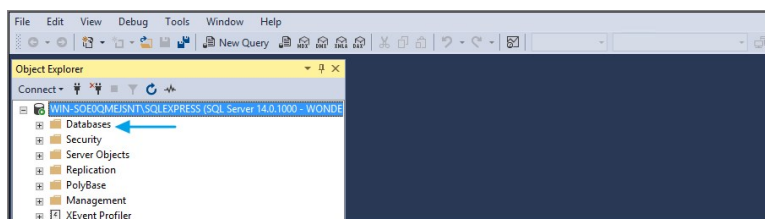
Could not allocate space for object 'Ams.ItemState'. 'UX_ItemState' in database 'ThycPrivMgr' because the 'PRIMARY' filegroup is full.



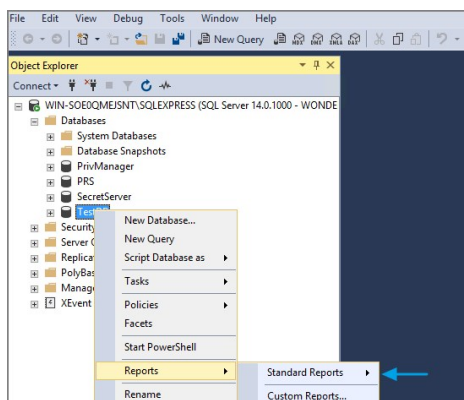
The error indicates that either the Privilege Manager database is full and out of space or the database server running is out of space.

Resolving the Error

1. Navigate to SQL Server Management Studio.
2. Click Connect.
3. Expand Databases.



4. Right-click on the Privilege Manager Database, select **Reports**.
5. Select **Standard Reports**.



6. Select Disk Usage by Top Tables report.

Table Name	# Records	Reserved (KB)	Data (KB)	Indexes (KB)	Unused (KB)
Ams.Activities.ActivityEvent	9,442	46,096	45,816	224	56
Ams.ItemState	6,005	35,352	34,640	408	304
Ams.ItemRole	39,435	8,728	2,280	6,376	72
Ams.Activities.TaskInstance	3,474	8,088	7,616	336	136

7. The report shows the top tables by data usage.
8. If the top table does contain a lot of data, locate the table which contains the highest number of files and open a support case. Provide the information collected with a screenshot of the report to determine the best way to reduce the size of the table.

If the top tables do not contain a lot of data, the issue could possibly be:

- o The database server is running out of disk space. You can check to see what drive the database is stored on to see how much space is left. This will be specific to your environment regarding disk space.
- o Check if there are other databases on the same server and investigate if a different database is taking up space.

During the installation of Privilege Manager the install hangs and is unable to proceed to the next step of the installation.

After checking the Thycotic Monitor, you see the below error in the log viewer:

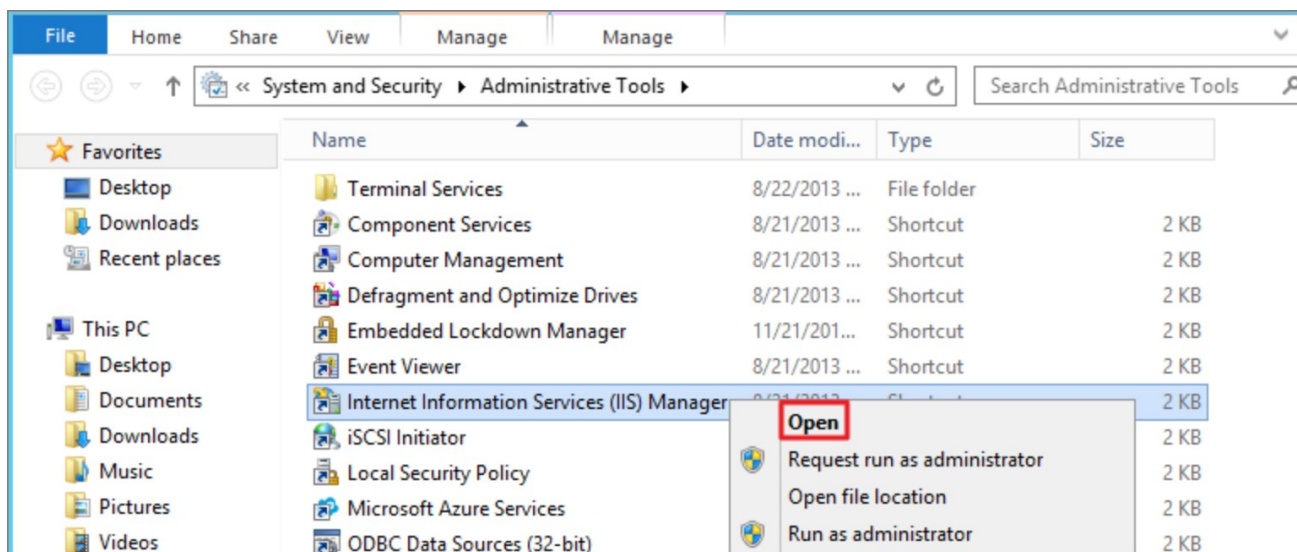
Worker Role Monitor received exception during ping: The HTTP request is unauthorized with client authentication scheme 'Negotiate'. The authentication header received from the server was 'Negotiate,NTLM'



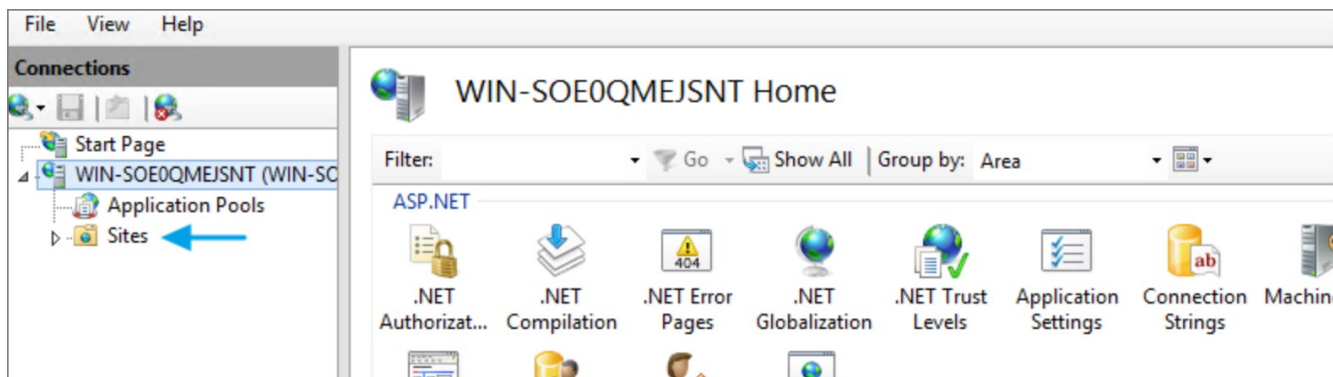
Note: This error is due to a host name in the binding within IIS.

Resolve

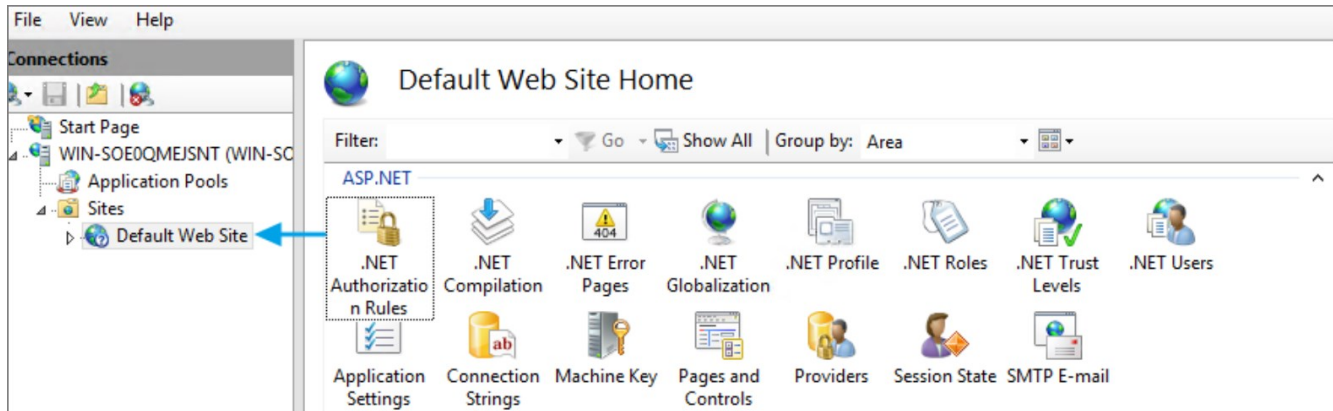
1. Open **Internet Information Services (IIS) Manager**.



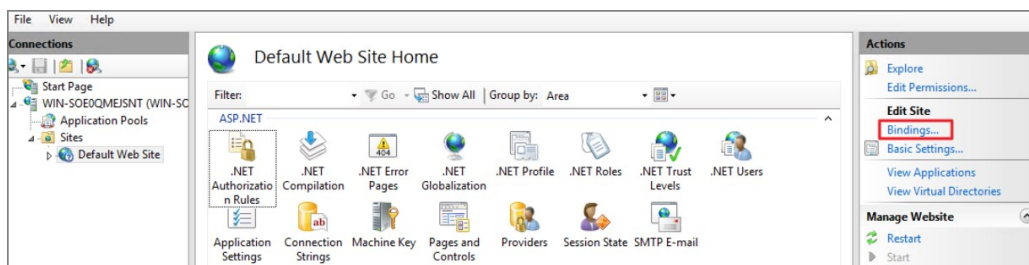
2. Expand down to **Sites**.



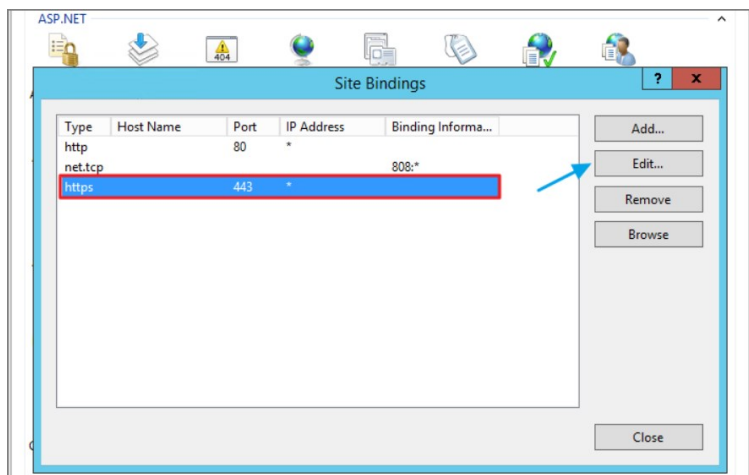
3. Click **Default Web Site** or the **top node site**.



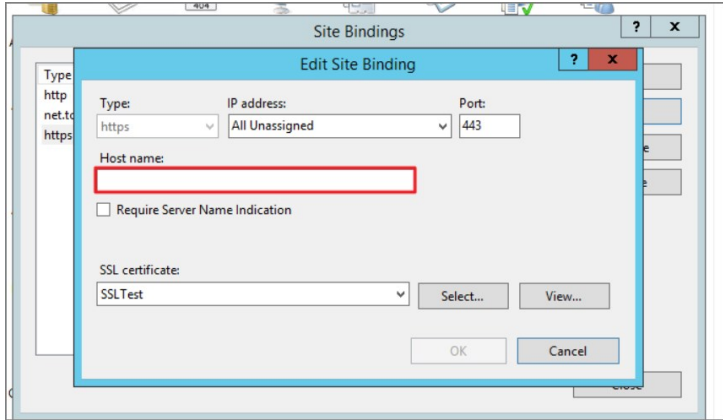
4. Click **Bindings**.



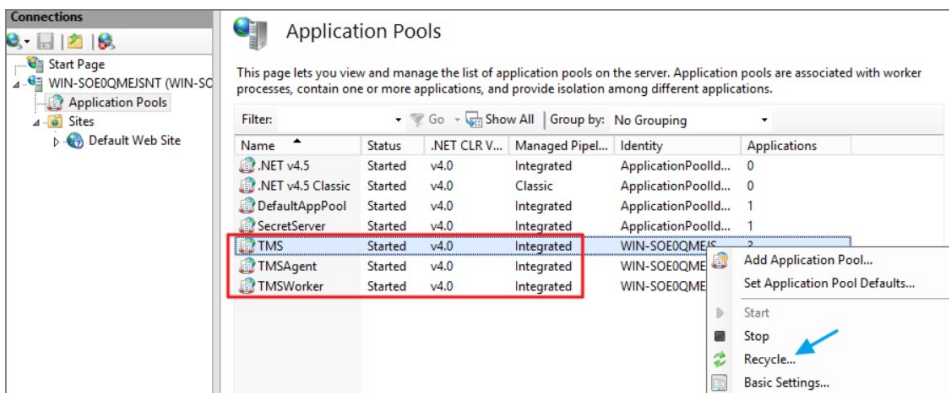
5. Select the **HTTPS binding** | click **Edit**.



6. Confirm that there is no Hostname included for the HTTPS binding for the TMS site. If so, please delete it.



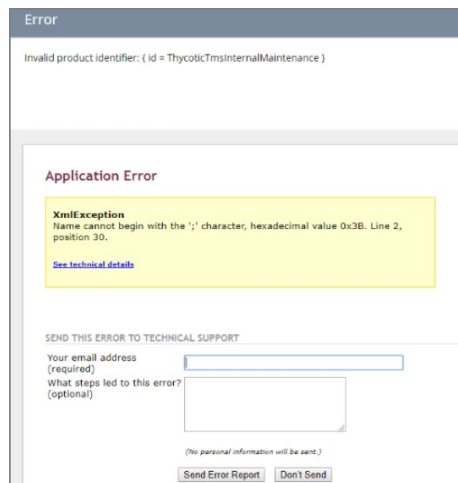
7. **Recycle** all the TMS application pools in IIS.



8. Try the install again by going to <https://localhost/TMS/Setup>

When attempting to upgrade Privilege Manager, you receive the following error:

Error: Invalid product identifier:



Error

Invalid product identifier: { id = ThycoticTmsinternalMaintenance }

Application Error

XmlException
Name cannot begin with the ';' character, hexadecimal value 0x3B. Line 2, position 30.
[See technical details](#)

SEND THIS ERROR TO TECHNICAL SUPPORT

Your email address (required)

What steps led to this error? (optional)

(No personal information will be sent.)

Send Error Report Don't Send

Resolve

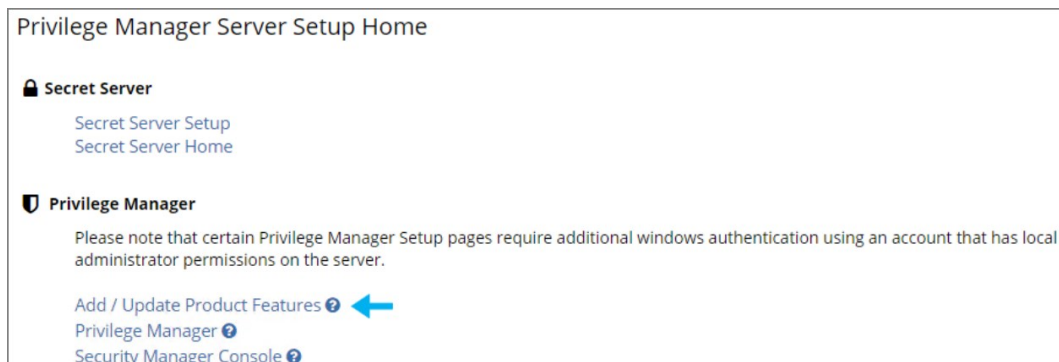
1. Navigate to [https://\[YourInstanceName\]/TMS/Setup](https://[YourInstanceName]/TMS/Setup).
2. Click the **Upgrade Banner** at the top of the Privilege Manager home page.



Search Items Search HOME TOOLS ADMIN REPORTS

Upgrade Available - There are 3 updates for Privilege Manager available.

3. Click **Add / Update Product Features**.



Privilege Manager Server Setup Home

Secret Server

- Secret Server Setup
- Secret Server Home

Privilege Manager

Please note that certain Privilege Manager Setup pages require additional windows authentication using an account that has local administrator permissions on the server.

- Add / Update Product Features
- Privilege Manager
- Security Manager Console

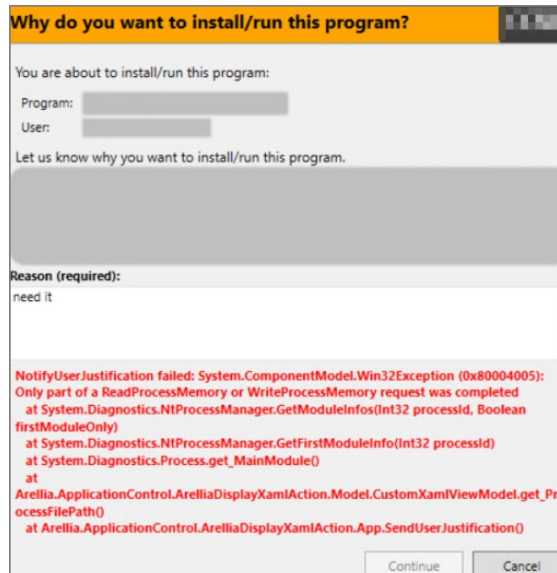
4. Click **Install/Upgrade Products**.

Product Name	Installed	Available	Published
Application Control Solution	10.5.1050	10.5.2007 Install	12/11/2018 7:05 AM
Directory Services Connector	10.5.1024	10.5.2004 Install	12/13/2018 9:50 AM
File Inventory Solution	10.5.1020	10.5.2004 Install	12/11/2018 7:05 AM
Local Security Solution	10.5.1014	10.5.2018 Install	12/11/2018 7:05 AM
Privilege Manager	10.5.1240	10.5.2002 Install	12/11/2018 7:05 AM
Privilege Manager Server Core Solution	10.5.1254	10.5.2008 Install	2/15/2019 12:40 PM
RDP Monitor Solution	10.5.1014	10.5.1014	8/15/2018 5:04 AM

[Install/Upgrade Products](#) [Refresh](#)

5. Select **ALL** of the required solutions.
6. Click **Install** and the upgrade process will begin.

You receive the following error when users attempt to run a program with a policy that uses the action for Notify User justification.



Resolve

1. Either disable the Anti-Virus Real time scan.
2. Or, set Anti-Virus Real-time scanning exclusions.

You might have to clear your browser cache if you get the following error in the Privilege Manager console:

Not Enough Storage is available to complete this operation

Privilege Manager Error

Not enough storage is available to complete this operation.

[Hide Exception](#)

```
"Error: Not enough storage is available to complete this operation.\n\n\n at s\n (https://thycotic/TMS/PrivilegeManager/main.js?10.6.0.586df7d:1:802266)\n at t.prototype.invokeTask (https://thycotic/TMS/PrivilegeManager/polyfills.js?\n 10.6.0.586df7d:1:35372)\n at onInvokeTask\n (https://thycotic/TMS/PrivilegeManager/main.js?10.6.0.586df7d:1:488983)\n at t.prototype.invokeTask (https://thycotic/TMS/PrivilegeManager/polyfills.js?\n 10.6.0.586df7d:1:35372)\n at e.prototype.runTask\n (https://thycotic/TMS/PrivilegeManager/polyfills.js?10.6.0.586df7d:1:30648)\n at e.invokeTask (https://thycotic/TMS/PrivilegeManager/polyfills.js?\n 10.6.0.586df7d:1:36576)\n at y (https://thycotic/TMS/PrivilegeManager/polyfills.js?\n 10.6.0.586df7d:1:50109)\n at b (https://thycotic/TMS/PrivilegeManager/polyfills.js?\n 10.6.0.586df7d:1:50426)"
```

[Reload Privilege Manager](#) [Close](#)

Resolution

1. Open your browser window and clear the cache.
2. Close and re-open the browser
3. Launch Privilege Manager and re-try the action.
Note: If the error continues, open a different browser and try to replicate the error. Save any screenshots and open a support case.
4. If this occurs while on the server, please ensure that there is enough disk space to complete the action.

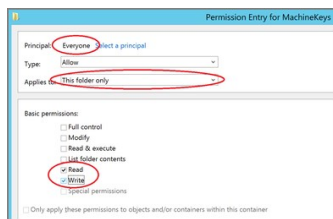
The following topics are available:

- [Troubleshooting Installation Issues](#)
- [10.5 Folder Permission for MachineKeys](#)
- [Retrieving the COM class factory error](#)

During installation of Privilege Manager 10.5 (or an upgrade from prior versions) Privilege Manager attempts to create a new self-signed certificate for internal use. If permissions on the folder %ProgramData%\Microsoft\Crypto\RSA\MachineKeys are incorrect, the install fails with a cryptographic exception and the text **Access Denied**.

Follow the steps below to add Everyone (Read, Write, This Folder Only) permissions to %ProgramData%\Microsoft\Crypto\RSA\MachineKeys.

1. Browse to %ProgramData%\Microsoft\Crypto\RSA\MachineKeys.
2. Right-click on the folder and select **Properties**.
3. Select the **Security** tab and click the **Advanced** button.
4. On the **Permissions** Tab, click the **Change permissions** button. (If you are already running as an administrator, you may not need this step.)
5. On the **Permissions** Tab, click **Add**.
6. On the next dialog, click the **Select a principal** link.
7. In the **Enter the object name to select** field, type **Everyone** and click **OK**.
8. You will see the dialog shown below, select **This folder only** and **Read and Write**.

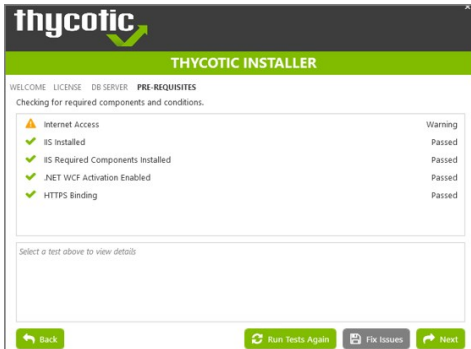


9. Click **OK** to add the entry.
10. Click **Apply** to apply the changes.
11. Navigate back to the Privilege Manager Setup page and select the repair option for the Privilege Manager Server Core Solution.

This article provided troubleshooting tips to help anyone who hits a snag during an install for Privilege Manager.

Internet Connection

If your server is not connected to the internet, you see the following:

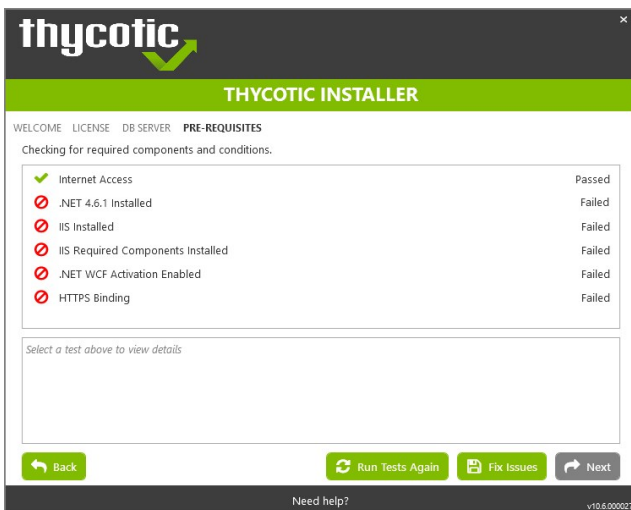


To Resolve:

Click **Next** to proceed through your installation offline.

.NET Dependency

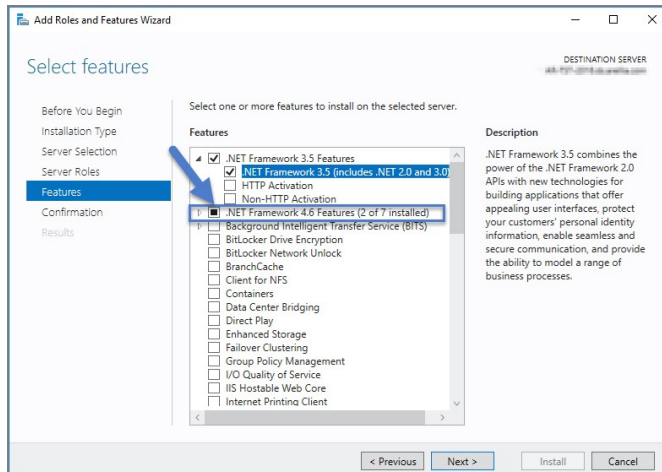
Don't have the required .NET version Dependency installed to accompany your SQL DB? This is what you will see:



To Resolve: Click the Fix Issues button on the Thycotic Installer, then run the pre-requisites check again.

If the error persists, manually install the recommended .NET version.

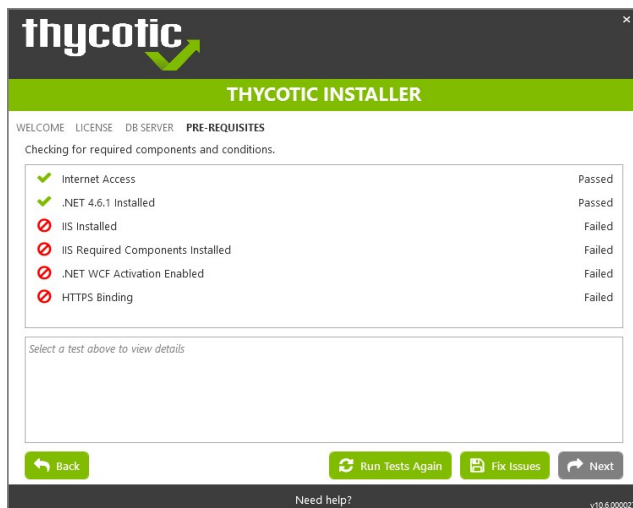
1. Open your Server Manager, in the upper right side of the screen, click Manage, then Add Roles and Features from the dropdown list. This will open your Add Roles and Features Wizard. Verify that the correct Destination Server is listed in the upper right-hand side of the screen.
2. Click Next through the Wizard steps until you arrive on the Features page.
3. Check the box next to the latest .NET Framework, here it is the .NET Framework 4.6 Features, click Next.



Follow the rest of the Wizard's steps until the install is completed. Once .NET 4.6 or greater framework is installed on your server, then run the pre-requisites check again.

IIS not installed

Don't have IIS installed yet? This is what you will see:



To Resolve:

Click the Fix Issues button on the Thycotic Installer. Then run the pre-requisites checks again.

HTTPS Binding Error

Did you encounter an HTTPS Binding Error? Does it not clear after using the Fix Issues button?

To Resolve:

Close and re-open the Thycotic Installer and run the pre-requisites checks again.

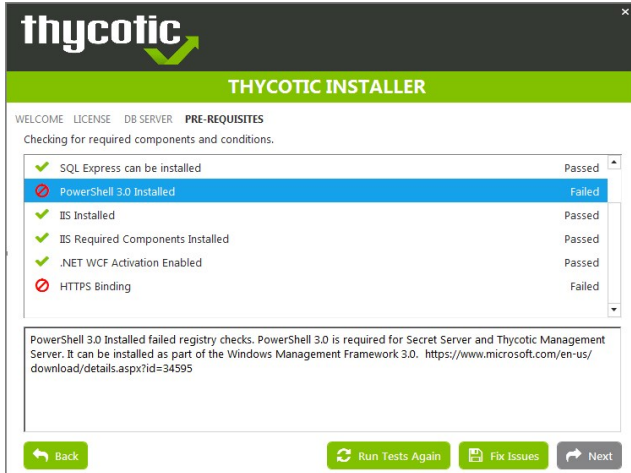
If the Binding Error persists, verify the following:

For combined Privilege Manager and Secret Server installations, did you previously move the Secret Server app pool in IIS to its own website, rather than allowing it to reside under the Default website? [see this KB for details](#).

The installer checks the Default Web Site for an HTTPS binding, and whether there is a certificate assigned to it. This means that if you pre-created the Secret Server Web Application and assigned the HTTPS binding to that site, you may need to manually move your previously installed Secret Server IIS site to reside back under the Default Web Site in IIS when installing Privilege Manager.

PowerShell Error

Are you receiving a Powershell error? You may be trying to install Privilege Manager on an outdated server! Here's what you will see:



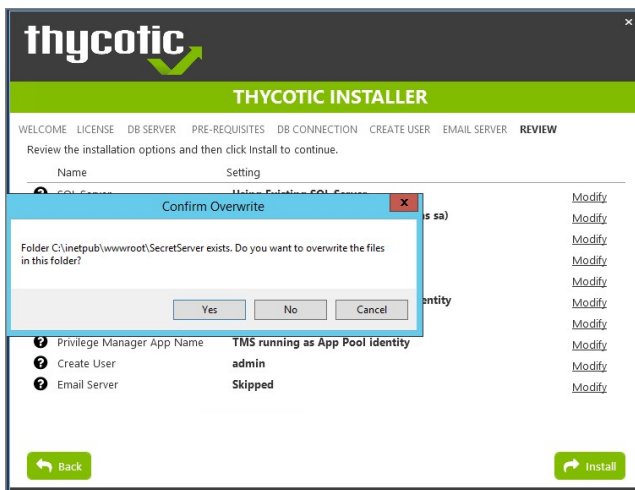
To Resolve:

You may need to update the server you are installing on. Please see our System Requirements Guide for supported servers. You can also manually download Powershell 3.0 and install it from Microsoft's website here.

Once Powershell is properly installed on your server run the pre-requisites checks again.

Secret Server and Privilege Manager Installed

Already have Secret Server installed on your server? Here is what you will see:



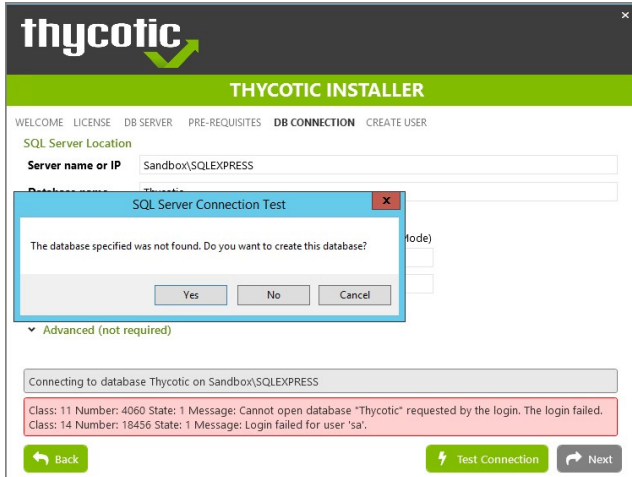
To Resolve:

We recommend installing new instances of Secret Server and Privilege Manager on a clean server.

If you do not already have an instance of Secret Server or Privilege Manager on this server to your knowledge, these files may exist due to an incomplete install. Check with anyone with access to this server who may have attempted this install previously. Only if you are confident that this is your first and only existing Secret Server or Privilege Manager instance click Yes to overwrite the existing files.

Error in DB File Path

Trying to test your connection to an existing SQL database? Here's what you will see:



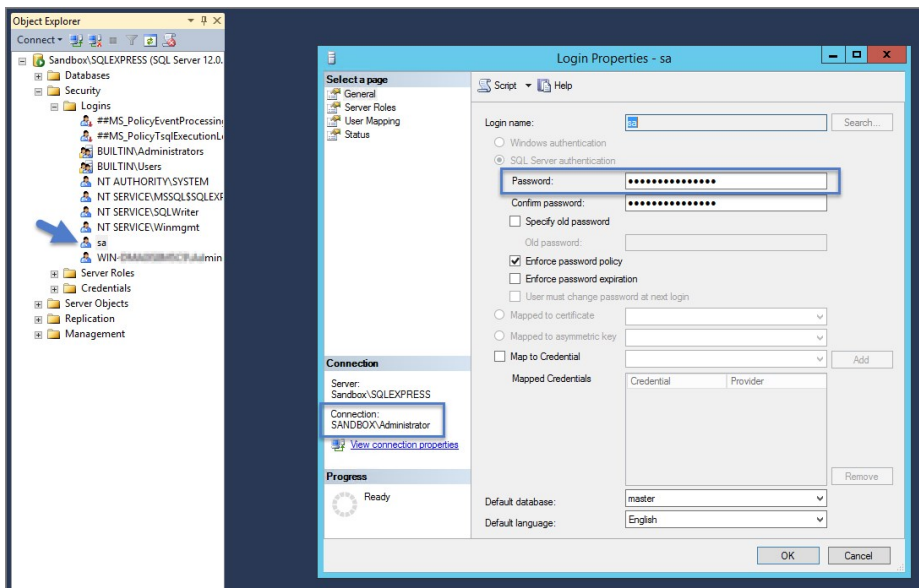
To Resolve:

This message means that your file path to your database is incorrect or your account does not have the correct permissions to access it.

If you have an existing database,

1. navigate to your SQL Server Management Studio and login.
2. Navigate to Security | Logins and right click on the account you are using for your Thycotic product, click Properties.

The information you need to enter in the Thycotic Installer for the connection path is listed in the bottom left corner under "Connection." You will also need to provide this account's password. Note that this account must have **db_creator** permissions.



Outdated Browser

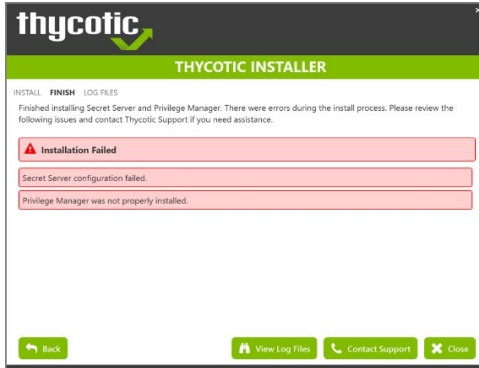
Are you trying to open your newly installed Privilege Manager in an outdated version of Internet Explorer? Here's what you will see:



To Resolve: Try opening Privilege Manager in a different browser, or update your Internet Explorer browser.

Integrated Authentication Error

Are you using Integrated Authentication and your installation failed? Here's what you will see:



To Resolve:

For clients using Windows Integrated Authentication, the Thycotic installer does not validate your database connection, so entering the wrong database server, database name, or if the user account provided does not have access to the database, your install will fail without warning you in advance. To resolve, please verify your database connection settings and enter them correctly under the **DB Connection** tab during the installation process.

While attempting to upgrade Privilege Manager, you receive an error message when accessing [https://\[YourInstanceName\]/TMS/Setup](https://[YourInstanceName]/TMS/Setup).

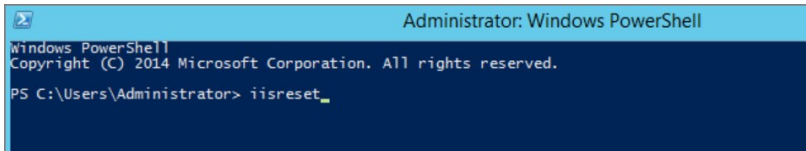
The window is unable to load with the following error message:

"Server Error in '/Tms/Setup/' Application.

Retrieving the COM class factory for component with CLSID (228FB8F7-FB53-4FD5-8C7B-FF59DE606C5B) failed due to the following error: 800703fa Illegal operation attempted on a registry key that has been marked for deletion. (Exception from HRESULT: 0x800703FA)."

Resolve

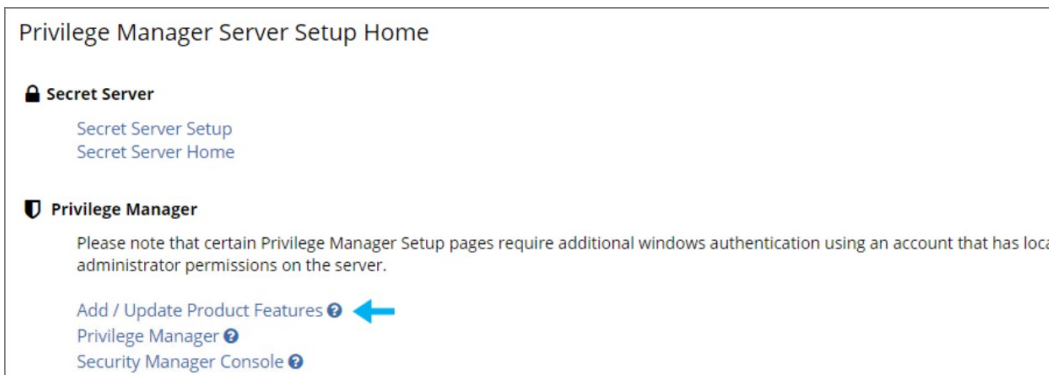
1. Close the browser window.
2. Complete an IIS reset by searching for the Windows Powershell application.
3. Right-click and select Run as Administrator.
4. Enter in: **IISreset** | hit **Enter**.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\Administrator> iisreset_
```

5. Once the IIS reset has completed navigate back to [https://\[YourInstanceName\]/TMS/Setup](https://[YourInstanceName]/TMS/Setup).

6. Click **Add / Update Product Features**.



Privilege Manager Server Setup Home

Secret Server

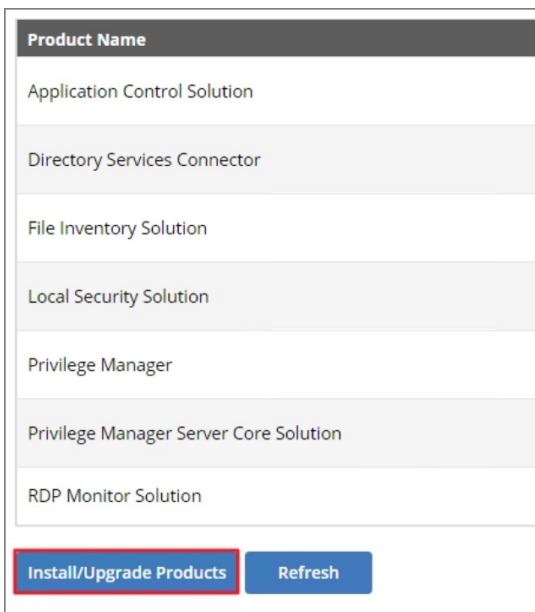
- Secret Server Setup
- Secret Server Home

Privilege Manager

Please note that certain Privilege Manager Setup pages require additional windows authentication using an account that has local administrator permissions on the server.

- Add / Update Product Features ? ←
- Privilege Manager ?
- Security Manager Console ?

7. Click **Install/Upgrade Products**.



Product Name
Application Control Solution
Directory Services Connector
File Inventory Solution
Local Security Solution
Privilege Manager
Privilege Manager Server Core Solution
RDP Monitor Solution

Install/Upgrade Products Refresh

8. Select **ALL** required solutions.

9. Click **Install** and the upgrade process will begin.

This section provides a collection of possible performance issues and their remediation options.

The following topics are available:

- [Improve Boot-up Performance](#)
- [Unable to access Privilege Manager](#)

In environments with policies having many filters, starting policy analysis during boot-up can impact the overall boot performance.

If this is an issue in your environment you can pause the policy analysis during boot. Pause analysis during the boot-phase decreases CPU utilization and delays to the boot process.

The end of the boot-phase in which policy analysis is paused, is defined as the CPU utilization after start-up being below 25% for a minimum of 120 seconds. Once that benchmark is reached, policy analysis will start.

Warning: Using this feature opens your systems up to vulnerabilities during the boot-phase due to policies not being enforced for a certain amount of time, until the above mentioned condition is met.

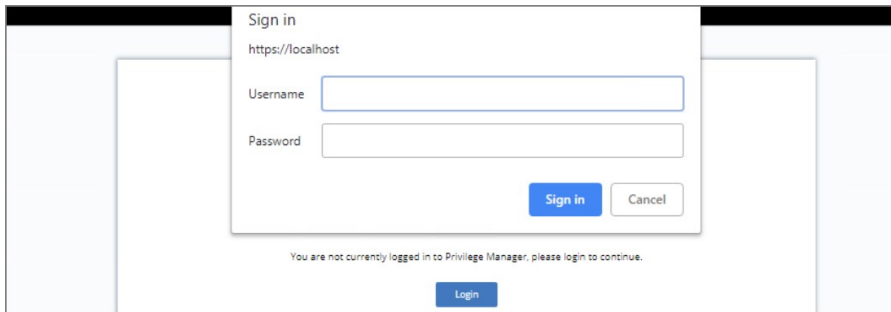
Enable Pausing Policy Analysis during Boot-up

Each policy by default has a list of policy enforcement options on the policy enforcement tab.

The screenshot shows a management console interface with a tabbed menu at the top: General, Conditions, Actions, Policy Enforcement (selected), Deployment, and Change History. Below the tabs, the text reads "Determine how this Policy is enforced." followed by a list of five checkboxes: "Continue enforcing policies after enforcing this policy", "Continue enforcing policies for child processes after enforcing this policy", "Stage 2 processing", "Pause Policy Analysis During Boot" (highlighted with a red box), and "Applies to all processes". At the bottom of the panel are five buttons: Back, Edit, Enable, Create a Copy, View as XML, and See Events.

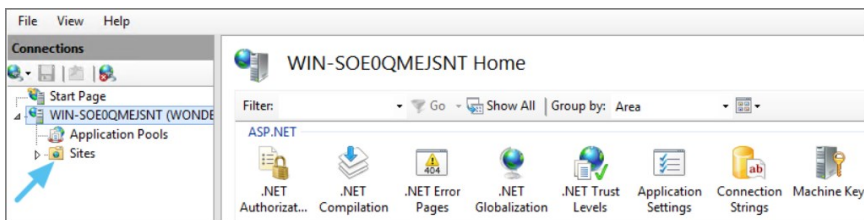
To enable pausing policy analysis during boot-up on filter-rich policies, select the checkbox next to **Pause Policy Analysis During Boot**.

When attempting to log in to Privilege Manager, you are unable to access the application window and see the following screen.

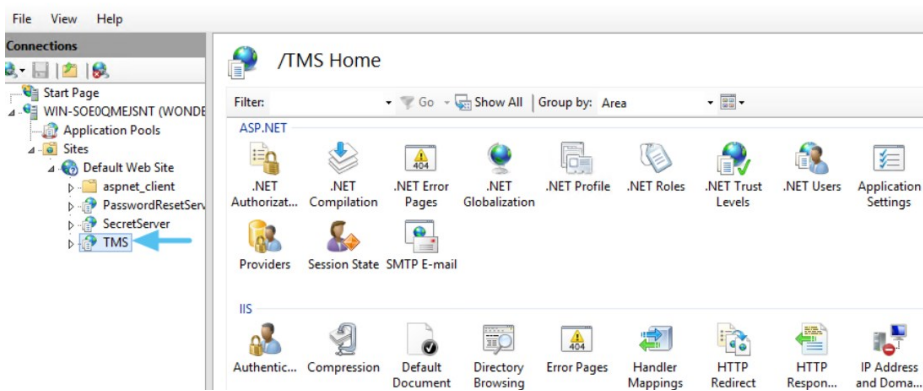
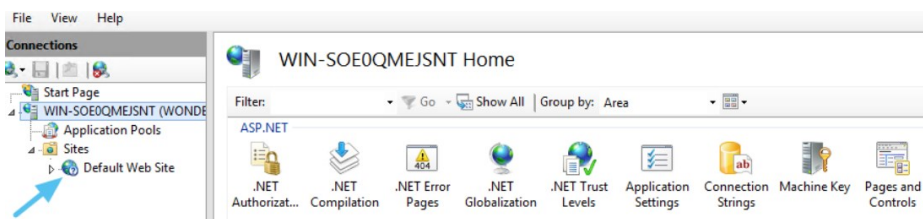


Resolve

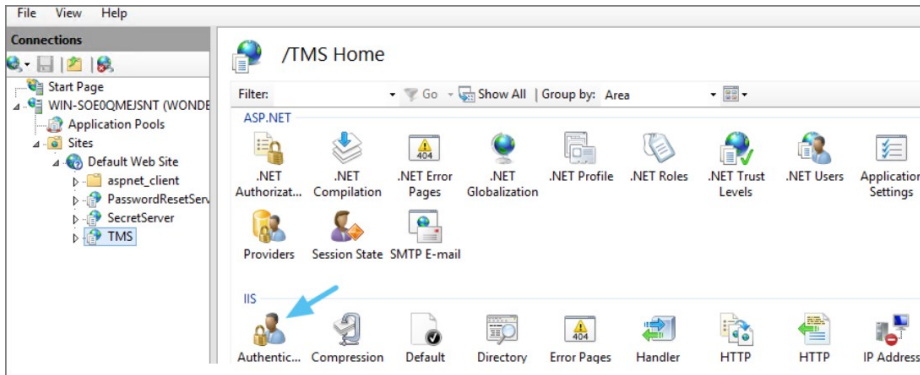
1. Open **Internet Information Services (IIS) Manager**.
2. Expand **Sites**.



3. Click the **TMS** Site.

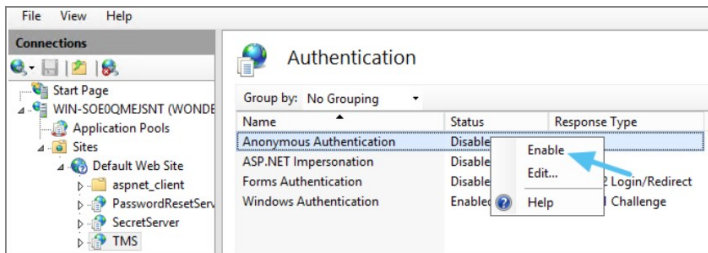


4. Click on **Authentication**.



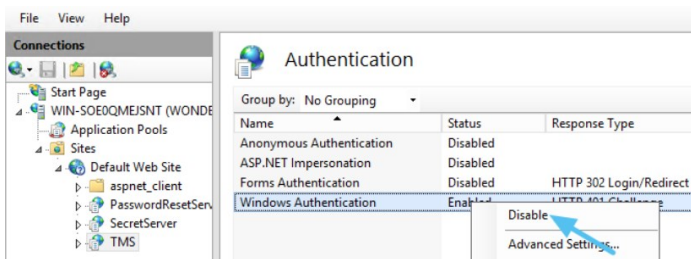
5. Right-click on **Anonymous Authentication**.

6. Click **Enable**.

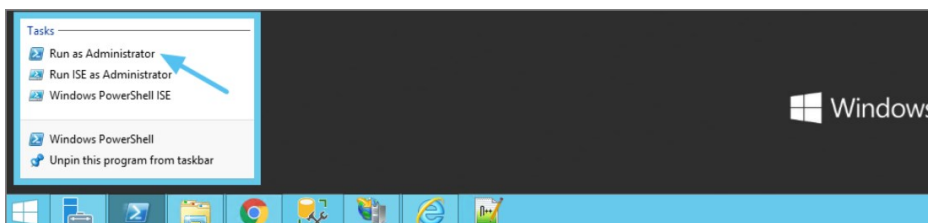


7. Right-click on **Windows Authentication**.

8. Click on **Disable**.



9. Open **Powershell**, type `iisreset` and press **Enter**.



10. Launch **Privilege Manager**.

The following topics dealing with logs in Privilege Manager are available:

- [Where are My Server Logs?](#)
- [Where are My Agent Logs?](#)
- [SQL Server Transaction Logs](#)
- [User Interface and Ports](#)

When something goes wrong in any technological platform, the best clues about 'why' are usually buried in log files. In Privilege Manager, it depends on 'what' is happening to know where to look for clues first, but server log files are usually a good are to start.

All Server-Side Privilege Manager Logs are written to %PROGRAMDATA%\Thycotic\Logs. Usually that means the folder path on your server is C:\ProgramData\Thycotic\Logs.

Keep in mind that the shared folder ProgramData can be hidden. You can enter this path directly in your file explorer's navigation bar to find the logs.

Within the Logs folder, you will find one log file for each web app. (e.g. Tms.log, Tms-Setup.log, Tms-Worker.log, etc.). When submitting a case to Thycotic's Support team, it is always a good practice to send these log files.

```

TMS - Notepad
File Edit Format View Help
INFO - 2017-08-16T14:46:58 Searching for server cert in bindings for site "Default Web Site"
INFO - 2017-08-16T14:46:58 Using server certificate thumbprint "A6528C9D0866F8485D451F876E124C9F91DE3DC3" - demonmain.
INFO - 2017-08-16T14:46:58 Registering Service Locators
INFO - 2017-08-16T14:46:58 Database is configured
WARN - 2017-08-16T14:47:02 No proxy server is specified
INFO - 2017-08-16T14:47:02 Have 6 Console items
INFO - 2017-08-16T14:47:02 Mapping console 62a7e338-e2cd-47ac-bde8-45b5edebed174 route "HelpDesk" from url "HelpDesk/{*queryv:
INFO - 2017-08-16T14:47:02 Mapping console f2e19194-9b58-40b9-b508-b9d9bdc461d4 static route "PrivilegeManager" from url "Pri
INFO - 2017-08-16T14:47:02 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorer" from url "ResourcE
INFO - 2017-08-16T14:47:02 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorerAspx" from url "Resou
INFO - 2017-08-16T14:47:02 Mapping console 352214ad-df09-4842-aa6e-bc47451b6c59 route "SecurityManager" from url "SecurityMar
INFO - 2017-08-16T14:47:13 SignalR:Stream 0 : SQL notification change fired
INFO - 2017-08-16T14:47:14 Platform Environment for Virtual App Default Web Site - /TMS (/TMS) Closing. Shutdown Reason Host:
INFO - 2017-08-16T14:47:14 SqlMessageBus got !immediate stop message, closing down SignalR processing.
INFO - 2017-08-16T14:47:14 SignalR: SQL message bus disposing, disposing streams
WARN - 2017-08-16T14:47:44 SqlMessageBus got immediate stop message.
INFO - 2017-08-16T14:47:44 SignalR Stream 0 : SqlReceiver disposed
INFO - 2017-08-16T14:53:18 Searching for server cert in bindings for site "Default Web Site"
INFO - 2017-08-16T14:53:18 Using server certificate thumbprint "A6528C9D0866F8485D451F876E124C9F91DE3DC3" - demonmain.
INFO - 2017-08-16T14:53:18 Registering Service Locators
INFO - 2017-08-16T14:53:18 Database is configured
INFO - 2017-08-16T14:53:19 Have 6 Console items
INFO - 2017-08-16T14:53:19 Mapping console 62a7e338-e2cd-47ac-bde8-45b5edebed174 route "HelpDesk" from url "HelpDesk/{*queryv:
INFO - 2017-08-16T14:53:19 Mapping console f2e19194-9b58-40b9-b508-b9d9bdc461d4 static route "PrivilegeManager" from url "Pri
INFO - 2017-08-16T14:53:19 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorer" from url "ResourcE
INFO - 2017-08-16T14:53:19 Mapping console fc32a7ad-eb80-409c-81c6-587ba3ec8012 route "ResourceExplorerAspx" from url "Resou
INFO - 2017-08-16T14:53:19 Mapping console 352214ad-df09-4842-aa6e-bc47451b6c59 route "SecurityManager" from url "SecurityMar
WARN - 2017-08-16T14:53:20 No proxy server is specified
INFO - 2017-08-16T14:54:29 SignalR:Stream 0 : SQL notification change fired
INFO - 2017-08-16T14:55:40 AuditManager worker starting.
INFO - 2017-08-16T14:55:44 SignalR:Stream 0 : SQL notification change fired
INFO - 2017-08-16T14:56:55 SignalR:Stream 0 : SQL notification change fired
  
```

By default, these log files will contain informational events, warnings, and errors.

Not included in your default logs are verbose/trace/debug errors, but this is configurable via the web-logging.config file in each web app directory discussed below. If interested in changing your log settings, you can find more information about the Log4Net Core "Level Value" options here: <https://logging.apache.org/log4net/log4net-1.2.11/release/sdk/log4net.Core.Level.html>

To edit log settings (i.e. Log trimming by size, type of recorded Log4Net Events) you can edit the code in your web-logging file, usually located in C:\inetpub\wwwroot\TMSweb-logging. By default, this file looks like this:

```

<?xml version="1.0" encoding="utf-8" ?>
<log4net>
<root>
<level value="INFO" />
<appender-ref ref="Thycotic.LogFileAppender" />
</root>
<logger name="Thycotic">
<level value="INFO" />
</logger>
<appender name="Thycotic.LogFileAppender" type="log4net.Appender.RollingFileAppender">
<file value="$([ProgramData])\Thycotic\Logs\TMS.log" />
<rollingStyle value="Size" />
<maxSizeRollBackups value="34" />
<maximumFileSize value="1 MB" />
<lockingModel type="log4net.Appender.FileAppender.MinimalLock" />
<layout type="Thycotic.Platform.Logging.Log4NetSimpleLayout,Thycotic.Platform"></layout>
</appender>
</log4net>
  
```

If something is going wrong on specific endpoints, another place to look for answers is in your Agent's Event Log Viewer.

In your endpoint machine, navigate to your Thycotic Agent files. This is usually located in C:\Program Files\Thycotic\Powershell\Arellia.Agent. Right-click on AgentLogViewer and select Run with Powershell. This will open your Agent Event Log Viewer, which shows updates in real time as the agent communicates with the Privilege Manager server.

For remote access, Agent logs are also viewable through the Windows Event Viewer.

Scroll all the way to the top of the page to see the most recent activity from your Thycotic Agent. Uncheck the Information box on the upper righthand corner to narrow search results for any Errors and Warning messages that may be occurring. You can also double-click any line item for more detailed information about each event.

TimeGenerated	Message	Source	Module
10/08/2017 14:15:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:16:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:15:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:14:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:15:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:14:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:56	Received SSL Policy error for CN=DemoMain : RemoteCertificateChainErrors	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:56	The Thycotic Agent configured certificate B48F78D48559A38B3E808124EAB3001500BEE6D5 is invalid. The certifi...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	The Thycotic Agent configured certificate B48F78D48559A38B3E808124EAB3001500BEE6D5 is invalid. The certifi...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	Completed TaskInstance f19311c0-00af-4401-804e-f3c21c91db7e - Client Command 'Resource Discovery Command'...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	Resource discoverer 0120439e-267b-422a-bbd8f3e659534785 did not return any discovery/xml	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:52	Unable to locate a file with hash f1a2Tr2LVB0gk3cGv8WmJA0b4+ for Resource (7f58334e-7d8b-5620-9EEA-99...	CFieResourceDisc...	ArelliaFileInvt.Agent.d...
10/08/2017 14:13:52	Received SSL Policy error for CN=DemoMain : RemoteCertificateChainErrors	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:14:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:51	Initiating taskinstance f19311c0-00af-4401-804e-f3c21c91db7e with clientCommandId 'Resource Discovery Command'...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:13:47	Queued Task f19311c0-00af-4401-804e-f3c21c91db7e - Command 'Resource Discovery Command' (77582ef2bd52...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:12:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:13:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:12:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:51	Next wakeup for ACS SendEvents set to 8/10/2017 2:12:51 PM	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:51	The Thycotic Agent configured certificate B48F78D48559A38B3E808124EAB3001500BEE6D5 is invalid. The certifi...	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:51	Performing ACS ProcessEvents	Arellia Agent	Arellia.Agent.Service
10/08/2017 14:11:47	Policy 'Event Discovery Testing Computers Audit Policy (Windows)' (398d5118-13ad-4425-9877b513bc4903db) (prior...	CASMonitor	ArelliaACSvc.exe

SQL Server maintains a history of all operations using a Transaction Log. If this transaction log becomes full, you may receive one or more of the following errors:

- System.ArgumentException: Cannot add two background tasks with the same name.
- Thycotic.Data.DataAccessorException: The transaction log for database "" is full. To find out why space in the log cannot be reused, see the log_reuse_wait_desc column in sys.databases

By default, a transaction log can grow to an unrestricted size. A transaction log may become full under the following circumstances:

- The drive where the transaction log file is kept is out of disk space.
- The transaction log file hits its growth limit.

Possible solutions include:

- Backing up the log.
- Freeing disk space so that the log can automatically grow.
- Moving the log file to a disk drive with sufficient space.
- Increasing the size of a log file.
- Adding a log file on a different disk.
- Completing or killing a long-running transaction.
- Switching to simple recovery mode and truncating the log.

For more detailed information on transaction logs in SQL, see <http://technet.microsoft.com/en-us/library/ms345583%28v=sql.90%29.aspx>

When something goes wrong in Privilege Manager, the UI has a few places worth checking:

- **Admin | Diagnostics** - this will give you information on Agents and Operating Systems, click **Console Logs** for more details.
- **Reports | Diagnostics** - A great place to look for some useful programmed reports on Agents, Remote Tasks, Policies Not Received by Agents, Summary of Gauge States, and Licensing.

Connectivity

Are you having Connectivity issues? A few things to keep in mind:

- Outbound access from the agent to the server is done by default over port 443 (the standard port for HTTPS communication), but you may specify a different port if desired.
- The only port that the agent listens on is port 5593. This is not required. For example, you can block this port and agents will pull from the server on a set schedule.

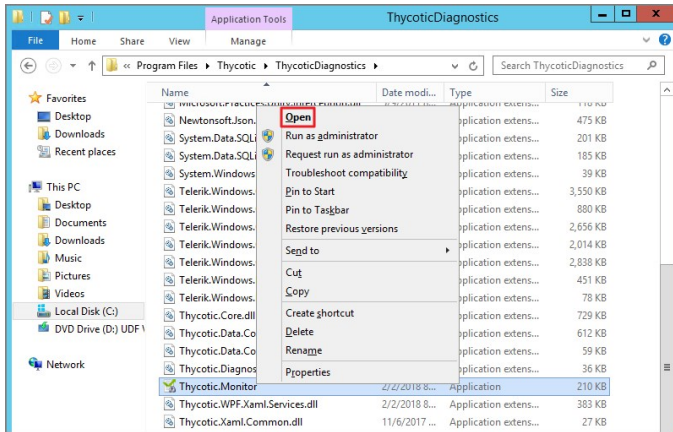
Using certain tools for troubleshooting purposes can help locating issues and finding a solution to a problem.

The following troubleshooting tools topics are available in this section:

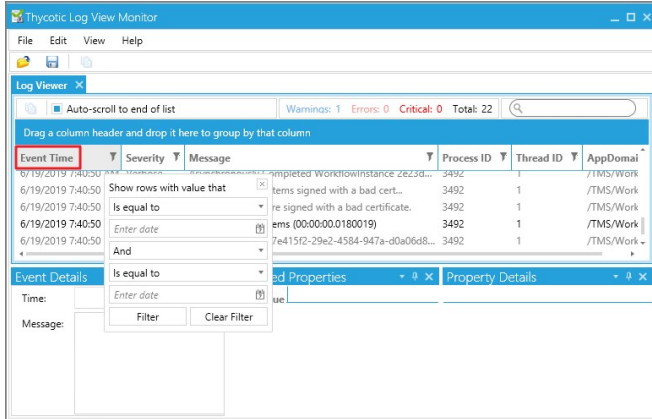
- [How to use the Thycotic Monitor for Troubleshooting](#)
- [Using Process Hacker for Troubleshooting](#)
- [Troubleshooting a Policy with Process Explorer](#)

While using Privilege Manager, you can utilize the Thycotic Monitor to help troubleshoot issues that occur on the web console.

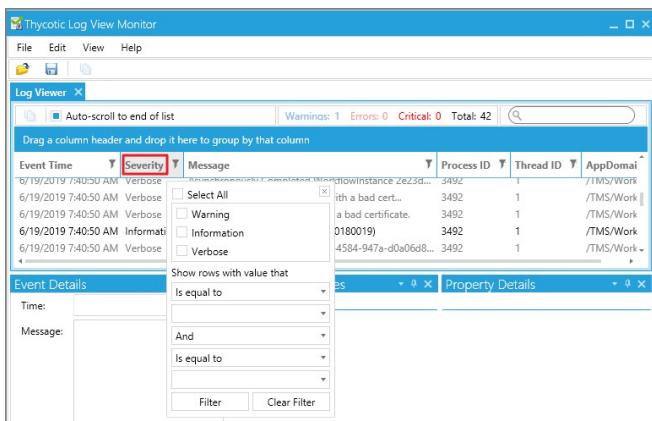
1. On the server with the Privilege Manager installation navigate to C:\ProgramFiles\Thycotic\ThycoticDiagnostics and open the Thycotic Monitor.
2. Right-click on Thycotic Monitor and select Open.



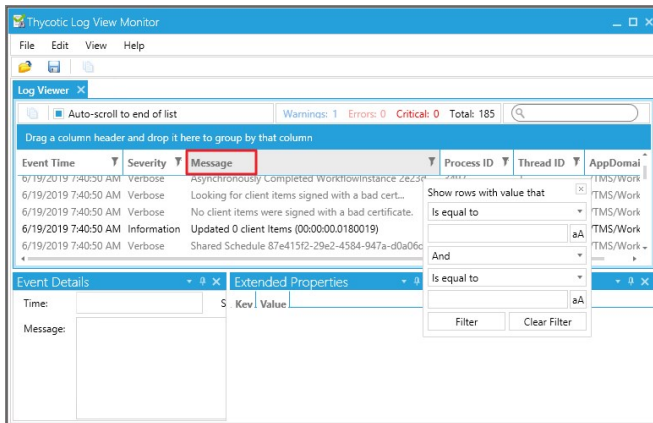
3. Left-click on the filter icon for Event Time to filter for specific times in order to better help find a specific event.



4. Left-click on the filter icon for Severity to filter for specific severity levels.



5. Left-click on the filter icon for Message to narrow down specific messages and GUID's to help find errors.



Note: If you're attempting to troubleshoot an issue open the Thycotic Monitor and replicate the issue on the server that Privilege Manager is installed on. It may also be helpful to grab a screenshot including a time-stamp from when you replicate the error in order to better help with troubleshooting.

1. Open the Thycotic Monitor.
2. Replicate the issue server-side.
3. Select **File**.
4. Select **Save**.

The file saves as a .tracelog file type. You can upload the tracelog to your support case or review the event details for further information.

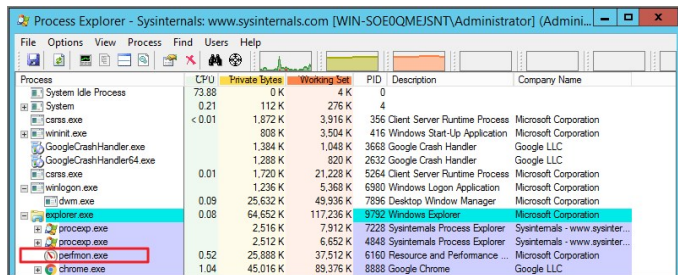
This topic describes how to troubleshoot a policy with Process Explorer. Process Explorer is used to look at policies that grant administrative privileges, but don't seem to work when

- an application is accessed, or
- actions are supposed to run.

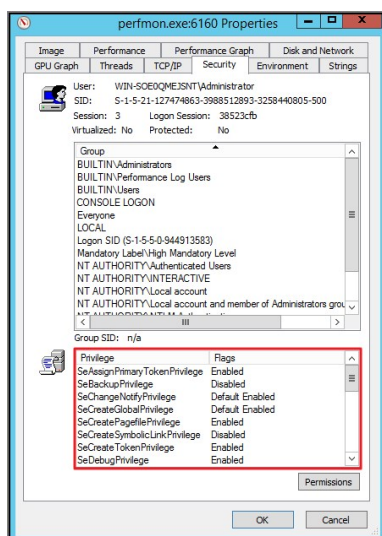
In the example below the policy allows resource monitor to run but the application is blank due to not having sufficient Windows Privileges. You can use Process Explorer to determine the correct Windows Privileges to add to the policy in order to use the resource monitor application.

Detailed Troubleshooting Steps

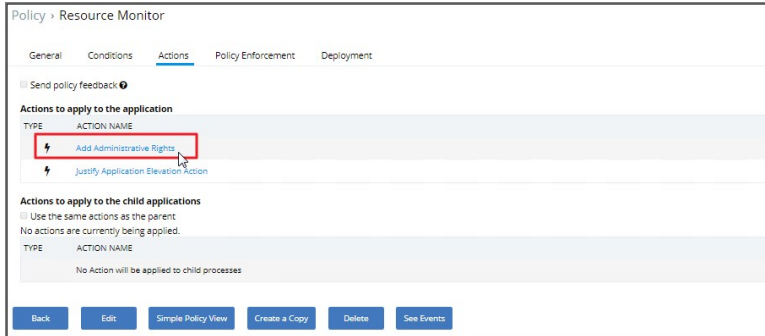
1. Download [Process Explorer from the Microsoft website](#) and extract the downloaded ProcessExplorer.zip file locally on your system.
2. Open **Process Explorer**.
3. Next open **Resource Monitor** as the Administrator.
4. Navigate back to the Process Explorer Window and find the Resource Monitor application (perfmom.exe).



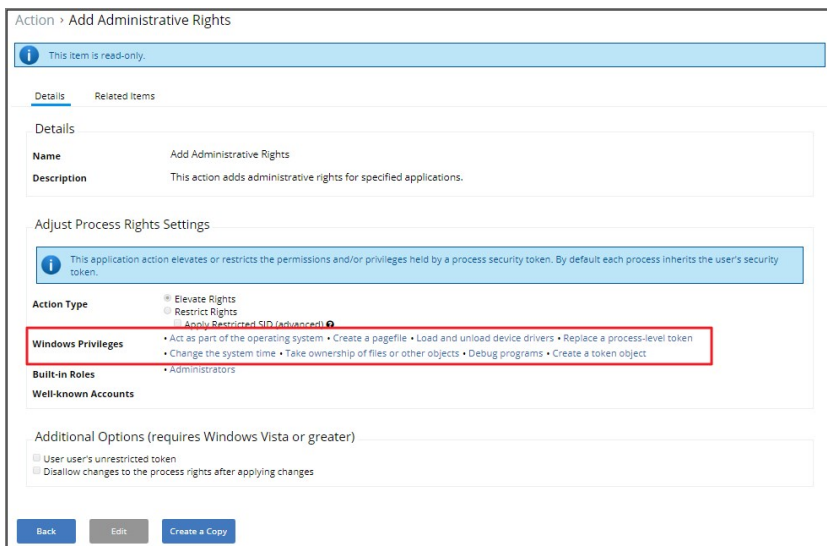
5. Right-click and select **Properties**.
6. Select the **Security** tab.
7. Under the Privilege section, you can see all the flags that are enabled in order to use the application.



8. Launch Privilege Manager and navigate to **Admin I Policies**.
9. Select the policy that elevates privileges to run Resource Monitor.
10. Select the **Actions** tab.
11. Select Add Administrative Rights or the elevation action you are using.



12. The new window will display what Windows Privileges the action is using.

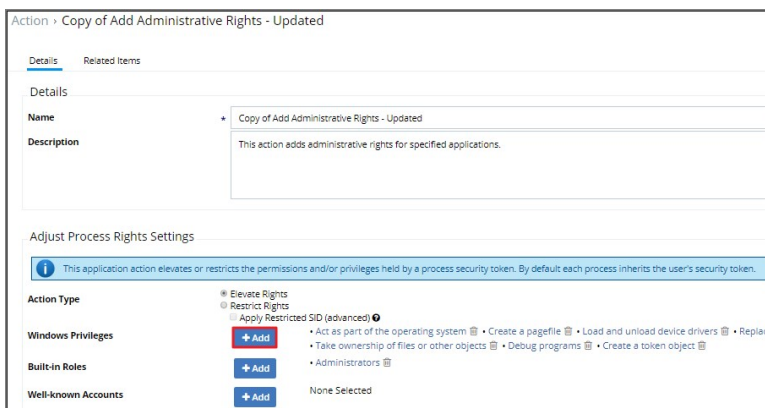


13. Click Create a Copy.

14. Enter a Name, click Create.

15. Click Edit.

16. Select **Add for Windows Privileges**. (For this step you will have to determine which flags are enabled in Process Explorer in order to add the additional Windows Privileges to the action.)



17. In another window navigate to the following Microsoft web site @ <https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants>. The site will show the name of the Windows Privileges, along with the user right information that needs to be added to the action in Privilege Manager.

For Example: The privileges listed under the properties security tab show **SeCreateGlobalPrivilege** as enabled. On the Microsoft website for Privilege Constants @ <https://docs.microsoft.com/en-us/windows/win32/secauthz/privilege-constants> the user right for SeCreateGlobalPrivilege privilege is: **Create global Objects**.

18. Enter the User right into the search box and then select the user right from the returned list. In this example enter in Create global objects.

Action > Copy of Add Administrative Rights

Details Related Items

Details

Name Copy of Add Administrative Rights

Description This action adds administrative rights for specified applications.

Adjust Process Rights Settings

i This application action elevates or restricts the permissions and/or privileges held by a process security token. By default each process inherits the user's security token.

Action Type

- Elevate Rights
- Restrict Rights
- Apply Restricted SID (advanced)

Windows Privileges **+Add**

- Act as part of the operating system
- Create a pagefile
- Load and unload device drivers
- Replace a process-level token
- Change the system time
- Take ownership of files or other objects
- Debug programs
- Create a token object

Built-in Roles **+Add**

- Create Global Objects
- Create permanent shared objects

Well-known Accounts **+Add**

- Create symbolic links

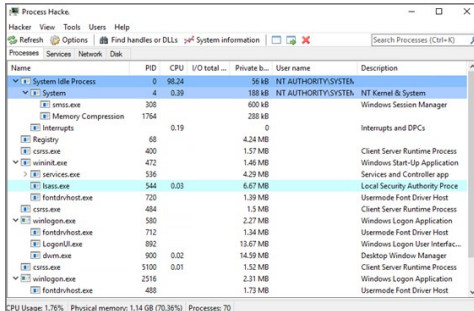
19. Click **Save**.
20. Navigate back to the Policy and open the Actions tab.
21. Click **Edit**.
22. Delete the original action by clicking on the recycle bin.
23. Click **+ Add Action** and search for the new action (you may have to select the refresh icon next to the search box in case the new action doesn't appear).
24. Select the new action and click **Add**.
25. Click **Save**.
26. Navigate to the Deployment tab and trigger a policy update on the endpoints.

Once the agent has received the updated policy, the additional Windows Privileges will be applied to the application next time it is launched.

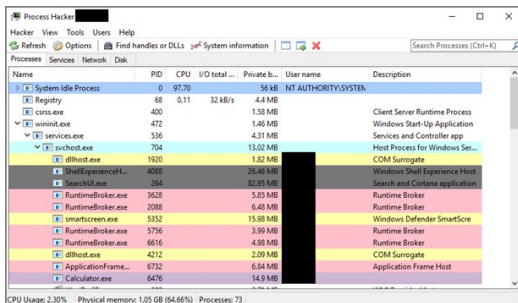
Process Hacker is a third-party tool that can be useful for troubleshooting as well. Please note that since this is a third-party tool, Thycotic is not responsible for any part of the application and has no control over it.

It can be used to determine whether a process you are trying to apply an action to is a parent process or a child process of another application. If you do not want to install Process Hacker on the endpoint you are troubleshooting from, there is a portable version available as well that does not require it to be installed on the machine.

When you open Process Hacker, you will notice a screen like the one below that shows the running processes on the machine.

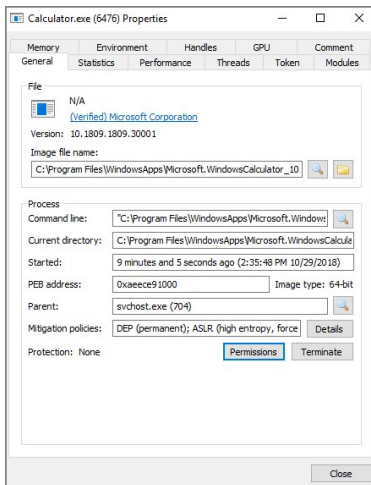


You will notice that some processes are listed underneath other processes. The processes listed under other processes are child processes of the top parent one. For example, after opening up the Calculator app on a test machine, the Process Hacker window looked like the screenshot below.



You can see at the bottom of the screenshot above that the Calculator.exe process is actually a child process of the svchost.exe process, which itself is a child process of the services.exe process, which is a child process of the wininit.exe process. Not all processes will be nested underneath as many parent processes as in this example.

You can also double-click on the process to open a window with more information about the process. You can find the parent process that way as well on the General tab of that window. The screenshot below is what the General tab shows for the Calculator.exe process.



You can see the Parent field, which shows you that the svchost.exe process is the parent of the Calculator.exe process. If you are viewing the parent process, then in the Parent field you will see "Non-existent process" instead of seeing a parent process listed.

You will also notice a Token tab in the screenshot above. That tab is useful in showing you whether the process is running elevated; it shows an "Elevated" field, with values Yes or No. It will also show you the process security tokens that the application needs to run. You normally do not need that information, but it is good to know where to find it, just in case.

As you can see from the information above, Process Hacker is a third-party tool that can be useful when troubleshooting why a policy is not applying like you think it should. For example, if you are trying to elevate a specific application or process, it might not be working correctly if that process is actually a child process. In that case, you can configure the policy to target the parent process and apply that same action to the child processes. You might not need to target the parent process in all situations, but sometimes it will be necessary.

Privilege Manager Mobile Application

The Privilege Manager Mobile console allows you to process approval requests, disclose passwords, and see alerts via the Privilege Manager Mobile Application on iOS and Android smartphones.

For the mobile app to work you must install the Privilege Manager Mobile Console, have Azure Active Directory setup to add an application registration, configure the Microsoft Azure Service Bus, and then install the Privilege Manager Mobile App.

The instructions are provided based on the assumptions, that

1. our customer is using Azure AD and has already configured the [Azure Active Directory App Registration](#) according to the docs to allow them to authenticate as an Azure AD user. The mobile application registration must be added to that **same domain**.
2. our customer has the ability to create an Azure Service Bus service.

To get started with the setup of the Privilege Manager Mobile Console, review and follow the instructions under the following topics in the order provided:

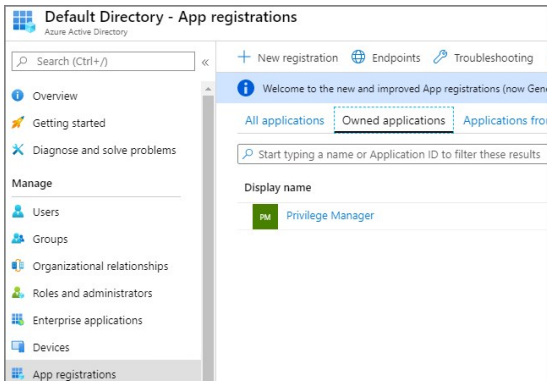
1. [Add the mobile application registration to your Azure Active Directory integration with Privilege Manager](#)
2. [Configure the Service Bus for Mobile](#)
3. [Install and Configure the Privilege Manager Mobile Console Solution on the Privilege Manager Server](#)
4. [Install the Privilege Manager Mobile App on a Mobile Device](#)
5. [Use the Mobile Application](#)

Configure Azure Active Directory

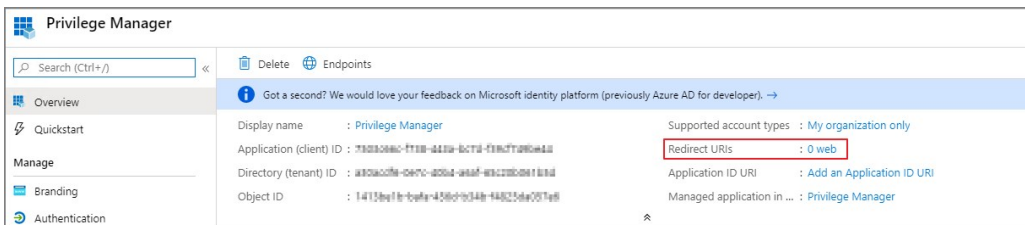
As a prerequisite for running the Privilege Manager Mobile Console, you must configure Azure Active Directory integration with Privilege Manager. Refer to [Setting Up Azure Active Directory Integration in Privilege Manager](#).

Once Azure AD integration for your Privilege Manager instance is configured, follow these steps to add an additional Redirect URI for the mobile application to the Azure AD application registration:

1. Open the **Azure Management Console**.
2. Navigate to your **Active Directory** instance.
3. Select **App registrations** from the menu.
4. Click the **Owned applications** tab.
5. From the list under Display name select your Privilege Manager registration.



6. Either select the **Redirect URI** links or the **Authentication** menu.



7. Select **Add a platform**.
8. Select **Mobile and desktop applications**.
9. Set the Redirect URI to exactly `http://ArelliaMobileClient`. There are two access points to do this either via:
 - o Redirect URI or
 - o Authentication menu.

The following table shows the steps you will see for each option:

<ol style="list-style-type: none"> 1. Click Add URI. 2. Enter <code>http://ArelliaMobileClient</code>. 	<ol style="list-style-type: none"> 1. Enter <code>http://ArelliaMobileClient</code>. 2. Click Configure.

Important: The URI value needs to exactly match `http://ArelliaMobileClient`.

10. Click **Save**.

On the **App registrations** page under **Owned applications**, take note of the **Application (client) ID**. You will need to use the client ID when you [Configure the Mobile Console in Privilege Manager](#).

The screenshot shows the Microsoft Privilege Manager interface. On the left is a navigation menu with 'Overview', 'Quickstart', and 'Manage' (subdivided into 'Branding' and 'Authentication'). The main content area shows the details for an application named 'Privilege Manager'. The 'Application (client) ID' is highlighted with a red box. Below it are the 'Directory (tenant) ID' and 'Object ID'.

Display name	: Privilege Manager
Application (client) ID	: 7803098c-7118-441a-8c7d-f19c7195e41d
Directory (tenant) ID	: a80a0c0e-047c-4004-86a7-88c278e08188d
Object ID	: 14135e18-7c9e-458c-b348-f4625da907e9

Configure the Service Bus for Mobile

For this a Service Bus Queue needs to be created, always refer to the latest instructions as outlined by Microsoft [here in Quickstart: Use Azure portal to create a Service Bus queue](#).

For this a Service Bus Queue needs to be created, refer to the latest instructions as outlined by Microsoft [here in Quickstart: Use Azure portal to create a Service Bus queue](#).

If you already have an existing Service Bus in Azure, you are welcome to use the existing setup. You just need to create a new queue within your existing Service Bus to be used by the Mobile App.

The following steps explain what is required for the Mobile App integration:

1. In the Azure Service Bus portal go to the **Shared access policies** page.
2. Find the policy called **RootManageSharedAccessKey**. If you don't have one yet, create one by that name and select the **Manage** option and save it.
3. On the **RootManageSharedAccessKey** policy you can see the **Primary Key** field. Make note of where this is. We have to use it in a step down below.
4. Next, navigate to the **Queues** page and create a new queue.
5. Do not check any of the options, using the defaults is fine. Take note of the queue name you gave it.

Next you will need to follow the instructions below to create a credential for the Service Bus and add the Service Bus as a foreign system in Privilege Manager.

The Azure Service Bus requires a Foreign Systems configuration in Privilege Manager. To configure a Service Bus instance with a custom URL and credentials follow these steps:

1. In the Thycotic Privilege Manager Console, click **Admin | Configuration**.
2. Click the **User Credentials** tab.
3. Click **Add New**.
 1. Enter a **Name**, for example *Azure Service Bus Credential*.

2. Set the Account name to **RootManageSharedAccessKey**.
3. Set the Password to the value of the **Primary Key** obtained during the Azure Service Bus configuration procedure **step 3** under "Creating a Service Bus and Queue in the Azure Portal" above.
4. Click **Save**.
4. Navigate to **Admin | Configuration** and select the **Foreign Systems** tab.
5. Click the **Azure Service Bus** option.
6. Click **Add New**.

1. Enter a **Name**, for example *Mobile App Azure Service Bus...*
2. Set the **ServiceBus Name** to the namespace of the Service Bus from the Azure Portal. To find this value, open the Azure Portal, locate the Service Bus that is being used for this integration (refer to the intro above). Go to the

Properties page and locate the Name property (generally, this is the same name as the instance you just located in the list of Service Bus instances).

3. Deselect the **Enabled** box for now.

4. Click **Create**.

7. Click **Edit** to provide more Settings details.

Foreign System > Mobile App Azure Service Bus

Configuration Change History

Details

Name	✦ Mobile App Azure Service Bus
Description	Provides Internet client connectivity via the Azure Service Bus

Settings

Credential	<input type="text" value="Type the name of a user credential..."/> Q
Enabled	<input type="checkbox"/>
URL	✦ [YourServiceBus]
QueueName	✦
QueuePolicyName	✦
QueuePolicySecret	✦

Save
Cancel
Export

1. Set the credential to the credential created in step 3 of this procedure (*Azure Service Bus Credential*).

2. Enable the Service Bus.

3. Leave the URL field as is (and ignore the fact that it's called URL – it's just the Service Bus name).

4. Make sure the URI matches the first part of the namespace created in Azure.

5. Set the QueueName to the same queue name created above in **step 4** under "Creating a Service Bus and Queue in the Azure Portal".

6. Set the Queue Policy Name to **RootManageSharedAccessKey**.

7. Set the Queue Policy Secret to the **Primary Key** as obtained in **step 3** under "Creating a Service Bus and Queue in the Azure Portal" above.

8. Click **Save**.

8. Recycle the App Pools on the Privilege Manager Instance following any changes for this integration. Without the recycle, the new settings won't be applied.

Cloud customers, please contact support for assistance to get these recycled. Unfortunately, this is a "must-contact" situation.

9. To verify everything is working correctly, open your browser and point it to the ServiceBus worker service:

- **On-Premises:** <https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc>
- **Cloud:** <https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc>

Wait for the page to respond.

You are now ready to install the Thycotic ACS application on your mobile devices.

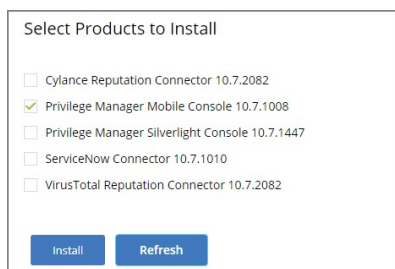
Install and Configure the Mobile Console in Privilege Manager

To configure the Mobile Console in Privilege Manager, you must:

1. Install the Privilege Manager Mobile Console.
2. Set the Client ID and Tenant ID.
3. Configure the notification settings.

The Privilege Manager Mobile Console needs to be installed on the same server that is running the Privilege Manager instance.

1. Navigate to your Privilege Manager setup page or select **ADMIN | More...** and select the **Add / Update Program Features**.
2. Click **Select Products to Install**.



3. Select **Privilege Manager Mobile Console** and click **Install**.

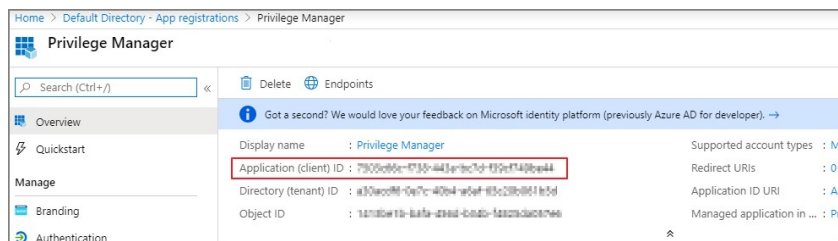
Once the installation completes click **Home** to navigate back.

After you have installed the Privilege Manager Mobile Console, set the Client ID and Tenant ID.

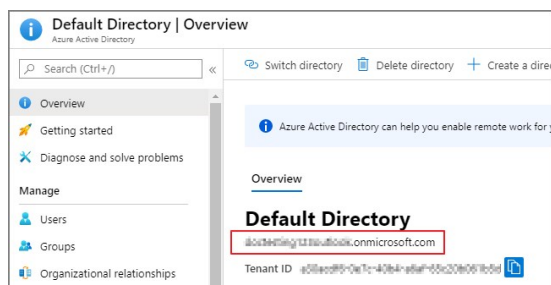
1. Navigate to **ADMIN | Configuration**.
2. Select the **Advanced** tab.
3. Scroll down and click **Edit**.

4. In the Thycotic Mobile Console Solution section under General enter values for:

1. **Your client id**: In the **Your client id** field, enter the Client Id that you generated when you configured the Microsoft Azure Active Directory. In the Azure AD portal, you find this under App Registration. Look for the **Application (client) ID** value.



2. **Your tenant id**, is the DNS name of the Azure Active Directory instance. You find it on the Azure AD Home page, between the friendly name and the Azure Tenant ID, for example **name.myinstance.com** or **MyCompanyName.onmicrosoft.com**.



Enter that DNS in the **Your tenant id** field.

Thycotic Mobile Console Solution

General

Your client id * 00000000-0000-0000-0000-000000000000

Your tenant id * -your-tenant-id-.onmicrosoft.com

Save Cancel

5. Click **Save**.

The notification settings for the mobile app are available via general configuration and task automation.

1. Navigate to **ADMIN | Configuration**.
2. Select the **General** tab.

Configuration

General Discovery Reputation Credentials Foreign Systems Roles

Policy Targeting

Run Policy Targeting Update

Approval Types

Default Execute Application Request Type

Default Offline Execute Application Request Type

Approval Processes

Default Manual Approval Process

Mobile Message Approval Process

Maintenance Settings

3. Under Approval Processes click **Mobile Message Approval Process**.

Approval Process > Mobile Message Approval Process

Details Change History

Details

Name Mobile Message Approval Process

Description Manual Approval Process that sends alerts to mobile devices in the chosen approver role. Alerts can be further scoped to first-responders via the Scope to Collection parameter.

Settings

Approval role allowed

Scope to collection (optional)

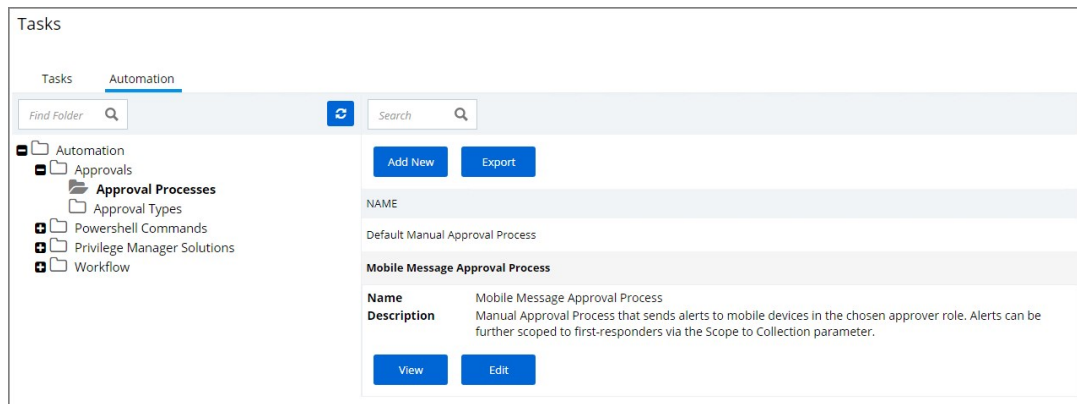
Message New approval request for %AmsFileName% with a %AmsReputation% reputation on computer %AmsAgentName%.

Start activity

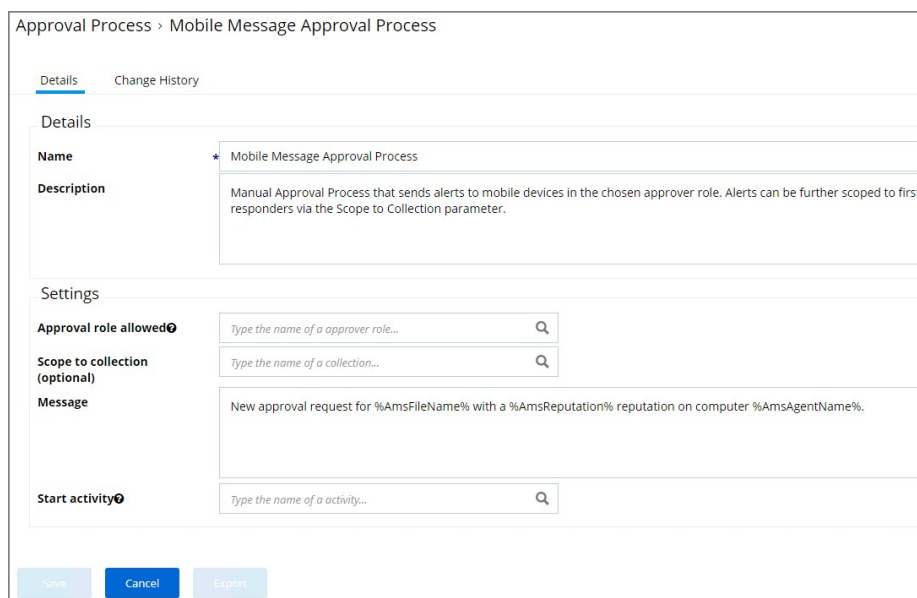
Back Edit Create a Copy View as XML Export

This task can also be accessed via **ADMIN | More... |**

Tasks, selecting the **Automation** tab and then in the folder tree **Automation | Approvals | Approval Processes | Mobile Message Approval Process**.



4. For customization, create a copy of the default task. Give it a meaning full name for your purpose, save the copy and click **Edit**.



5. Under the Settings section, you specify in the

- Approval role allowed field, which roles have approval permissions. By default the alerts for new approval requests will only be sent to mobile users in the Administrators role. You can change this setting by adding the approver role to a different role.
- Scope to collection field, which is an optional setting, to scope these messages to a subset of users in that role.
- Message field, what message will be displayed to the approver when an approval request was triggered.
- Start activity field, which is an optional setting, any activity you wish to start as part of the approval.

6. Click **Save**.

To start sending notifications to phones, select the **Default Execute Application Request Type** and change the **Approval Process** from the **Default Manual Approval Process** to the **Mobile Message Approval Process** and save the changes.

Note: The approval process change to Mobile Message Approval Process is only for the notification message that an approval was requested. The actual approval has to be followed through via HelpDesk interface. Currently approval requests cannot be approved via the Mobile app.

You can also send notifications based upon report data. These can be used to send alerts for suspicious activity, etc. An example of this can be found under **Tasks | Server Tasks | Mobile Messaging | Mobile Message Alert for Password Disclosures on VIP Systems**.

Task > Mobile Message Alert for Password Disclosures on VIP Systems

i This item is read-only.

General Parameters Schedules

Name Mobile Message Alert for Password Disclosures on VIP Systems

Description This task will send a mobile message alert when a password on a VIP System has been disclosed

Back Edit Run Task History Create a Copy Delete View as XML Export

This message can be executed on a schedule to send alerts for any password disclosures on VIP Systems. VIP

Systems are configured via the Monitored Computers parameter that allows you to choose a Collection of computers.

The Privilege Manager Mobile Console does currently not work with Secret Server as the authentication provider. If Secret Server is configured as the authentication provider in Privilege Manager, a warning message is shown on the Mobile Message Approval Process configuration page.

Approval Process > Mobile Message Approval Process

Details Change History

Details

Name Mobile Message Approval Process

Description Manual Approval Process that sends alerts to mobile devices in the chosen approver role. Alerts can be further scoped to first-responders via the Scope to Collection parameter.

Settings

⚠ The current selected authentication provider (Secret Server) is not compatible with mobile.

Approval role allowed

Scope to collection (optional)

Message New approval request for %AmsFileName% with a %AmsReputation% reputation on computer %AmsAgentName%.

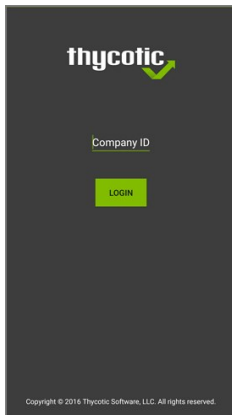
Start activity

Back Edit Create a Copy Export

Mobile App Install and Sign In

After installing and configuring the server components, help desk users can download the Mobile app for their smartphone via the appropriate app store by searching for **Thycotic ACS**. After you install the app, do the following:

1. Open the application on the mobile device.



2. When prompted for the **Company ID**, enter the name of your **Service Bus**. To find the name, open the Azure Portal, locate the Service Bus that is being used for this integration. Go to the **Properties** page and locate the Name property (generally, this is the same name as the instance in the list of Service Bus instances).
3. Next enter the Azure Active Directory user credentials.
4. Create a pin to secure the Mobile app.

If you experience any issues completing those steps, try the following to solve the problem:

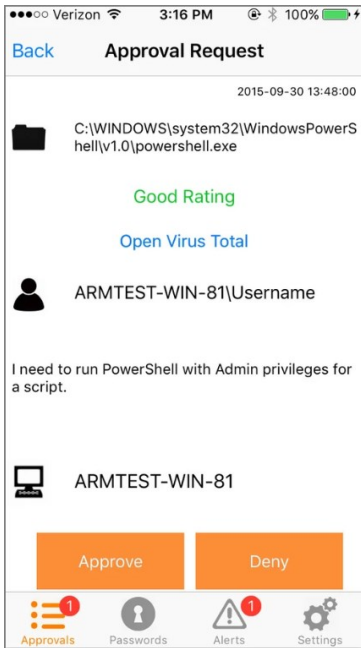
1. Verify that you can reach the Service Bus worker service by pointing your browser at the ServiceBus worker service. Enter the URL into your browser navigation bar:
 - **On-Premises:** <https://yourinstance.privilegemanager.com/Tms/ServiceBus/WorkerService.svc>
 - **Cloud:** <https://yourinstance.privilegemanagercloud.com/Tms/ServiceBus/WorkerService.svc>

Wait for the page to respond.

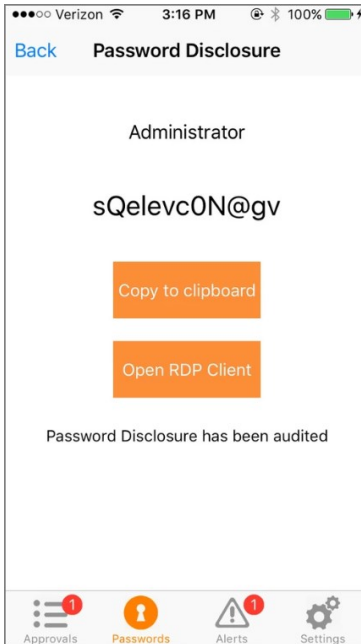
2. Verify the Redirect URI setting in your Azure AD application registration matches the configuration values in Privilege Manager.
3. **Recycle the App Pools on the Privilege Manager Instance** following any changes for this integration. Without the recycle, the new settings won't be applied.
Cloud customers, please contact support for assistance to get these recycled. Unfortunately, this is a "must-contact" situation.

Use the Mobile Application

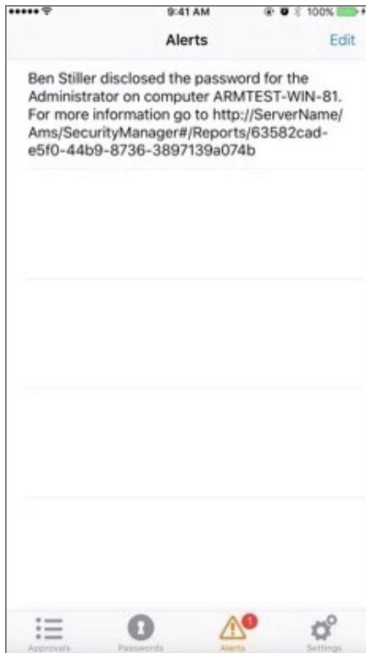
Approval Requests area provides the ability to approve/deny pending approval requests and the ability to view recently approved requests.



Password Disclosure area provides the ability to disclose managed user passwords that the mobile user has access to.



The Alerts area provides the ability to view non-approval request alerts, such as the Password Disclosures on VIP Systems. These alerts can be forwarded via e-mail or removed.



Release Notes

This section includes the most recent Privilege Manager Release Notes.

- [10.7.1 Release Notes - On-prem/Cloud](#)
- [10.7.0 Release Notes - On-prem](#)
- [10.6 Release Notes - On-prem](#)
- [10.6 Release Notes - Cloud](#)
- [10.5 and previous releases Release Notes](#)

10.7.1 Release Notes

Release Date: Cloud 2020-03-05, On-premises 2020-03-12

Enhancements available with the 10.7.1 release of Privilege Manager. Enhancements are for both versions, On-premises and Cloud, unless otherwise outlined under a specific On-prem or Cloud subtopic.

- The Secret Server Vault integration does not require Secret Server to be set up as the authentication provider. Any supported authentication provider can be used, independent from using Secret Server as a Password Vault. Refer to [Setting up Integration between Privilege Manager and Secret Server](#).
- Computers in Domain Groups can be leveraged as resource targets to be used in policies. Computer groups can be set up to utilize Active Directory security groups and organizational units (OUs). These so called domain security groups and OUs can be imported via Active Directory or Azure AD. However, OUs do not exist in Azure AD. Refer to [Create New Computer Group](#).
- General in product user guidance improvement for Mobile Application configuration. Refer to [Privilege Manager Mobile Application](#).
- The policy **Agent Service Start / Stop Control (Windows)** is now obsolete. Users should disable that policy and/or delete it. We have added a new policy named **Restrict Account Permissions on Agent Services (Windows)**. Users should clone that policy, to edit and assign to the desired targets, and enable. Refer to [Agent Hardening](#)
- Improved verbose logging during token validation logic.
- Report export options allow to select all data sets vs. data sets currently displayed on the page. Refer to [Reports](#).
- On-premises only support for deployments with Amazon RDS database systems.

macOS Specific Features

- New Configuration Feed to ignore macOS Catalina Software Updates. For details refer to [Ignoring macOS Updates](#).
- Best Practices for macOS system preference panes have been added, refer to [Best Practices System Preferences](#).
- Improved and new macOS event discovery filters, refer to [List of Default Filters for Event Discovery](#). Beginning with macOS Catalina, Apple changed the location of the application bundles that ship with the operating system. Traditionally, these applications were located in /Applications. Now they are located in /System/Applications. That location however is masked by Finder. The new and improved filters work with both locations.
- It is no longer necessary to include the **.app** extension for the Bundle Name property of an App Bundle Filter (e.g. Console.app). The agent will account for its presence while performing policy evaluation and properly match the filter if it is applicable. Refer to [App Bundle Filter](#)

Cloud Specific Features

- Data centers in Canada and Singapore have been added.
- Secret Server can be used as a password vault independent from the authentication provider.
- ServiceNow connector is automatically installed for all new cloud instances.
- The integrated SMTP server is automatically configured for all customers during the cloud instance setup, alleviating the need for customers to connect their own SMTP server.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix. Bug Fixes are addressed for both versions On-premises and Cloud unless otherwise outlined under a specific On-prem or Cloud subtopic.

- Long lists of resource items are not scrollable when trying to view or select items. For example when adding a user to Local Security Groups or when looking at the password history of a user, the form cannot scroll down the entire list of users.
- The 10.7 agent fails and prevents execution on certain Java based applications.
- Reports exported to CSV only include information of the data currently displayed in the UI and not all data records from that report.
- Grids in reports are not properly sorting date column data.
- The offline approval picker is not displaying parameters and computer list does not fit into page.
- When editing an Import Directory or Import Directory Computers task, the Directory ID and the Query parameters cannot be saved.
- Secondary file filters are ignoring items with spaces in their name and not triggering appropriate policy actions.
- Exporting a FileParameterCollectionFilterContract does not export the underlying file resources.
- When creating Filters for Windows systems and the user has the Privilege Manager macOS Administrators role, an exception is shown.
- Misleading counts when built-in local Admin users are backed-up by provisioned user.
- When creating a copy of an **Approval Request (with ServiceNow Request Item Number) Form** action, the contents cannot be edited.
- Security ratings reports pagination is not working correctly.
- macOS latency in updating a VNODE structure on disk is resulting in application execution being denied.
- Cannot add new policies with application targets and enable.
- Selected credentials on AD foreign system cannot be edited.
- Changing authentication providers throws an exception.
- A Privilege Manager client license count is exceeded message is displayed when it exceeds the 90% threshold and valid licenses are still available.
- Any domain groups added as a local administrator in the LSS Computer Groups disappear after being added.
- Creating a user context filter with a properly formatted SID that does not exist fails. A malformed SID results in an unfriendly error message.
- Users cannot add new machines to a managed computer group.
- For policies using a Group Member Authenticated Message Action, members in nested groups are not validated during the authentication process.
- Users in nested groups don't get the proper application role.
- Cross site anti-forgery token validation was using an email as a match, but the value was configured as a name.
- The Resource Target Computer List removes previously selected items when attempting to add additional computers.
- Privilege Manager installs prior to 10.5 cannot be upgraded to 10.7.0.
- Preferences cannot be fetched or saved by non-administrative users.
- Agent hardening removes permissions to modify/delete Agent Services.
- ServiceNow connector fails when upgrading Privilege Manager from 10.4 to 10.7.0.
- The **Domain Users as Local Administrators** and **Summary of Domain Users as Local Administrators** reports are timing out when run in large environments.
- Changes to the default file inventory from the Event Discovery page are not saved.
- UNC share policies imported from Config Feeds are not displayed under policies.
- Application control agents installed on Windows 10 machines are not reported on the **Application Control Agent Summary** report.

Agent Updates

Refer to [Software Downloads](#) for the latest available agent software downloads.

Core Thycotic Agent	10.7.2266	Rebuild with bundle to include Application Control Agent updates.
Application Control Agent	10.7.2257	Secondary file filter pre-filtering performance is causing slowness when there are large numbers of child processes launched (such as git.exe for each file).
	10.7.2256	System experiencing poor performance for the Group Member Authenticated Message Action.
	10.7.2239	Send SysLog ... template based tasks to send logs to server fails.
	10.7.2219	Initial 10.7.1 release version.

Privilege Manager macOS Agent	10.7.29	Users are locked out of their macOS device user account and unable to log in again, if the option to reopen the application on next login is enabled.
	10.7.27	The download filter policy is not triggering due to invalid URL partial match logic.
		Local groups on macOS without a SID prevents local user inventory from completing.
		MacOS agent experiences database contention when Office for Mac is installed or updated.
	10.7.21	Initial 10.7.1 release version.

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.7 and newer macOS endpoint agent.
- When installing Privilege Manager on a Windows Server 2012 pointed to a DB that is running on SQL Server 2017 or above, SSDT binaries will need to be leveraged, which are only available in .NET 4.6 or above. If your Server 2012 has .NET 4.5.1, make sure to update it to the recommended .NET 4.6.1 version.

10.7 On-prem Release Notes

Release Date: 2019-12-09

Enhancements available with the 10.7 On-premises release of Privilege Manager:

- [Security Manager migration support](#) has been added. The migration path to the latest Local Security implementation provides an analysis report of issues like missing account credentials, or accounts that are not unique across targets, which can then be remediated before the migration.
- [Change History auditing](#) is available for resource items providing information on who initiated the change, at what date and time, and what type of change was made.
- The [Remove Programs Utility](#) in previous versions available via Configuration Feeds has been fully integrated with Privilege Manager Server and the Agents installation packages. The functionality has been expanded to also include Windows 10 App Store applications.
- [Export and import of policies](#) - including all dependent filter, action, and user context type items.
- A new [Reset Licensing task](#) was added.
- Support filtering on the subject name of a signed digital certificate allowing for much more generic certificate management.
- Dependency checks have been added to Privilege Manager for:
 - [Deleting Items](#)
 - [Task Parameter and Schedule Parameters](#)
- Agents Enhancements:
 - [Agent Hardening](#)
 - Agent will only receive new and updated policies that are relevant to that endpoint.
 - Enhance [Client Item Cache Log View](#) in Agent Utility.
- Support for [configurable session and inactivity timeouts](#) was added to the product.
- Allow right-click as a Thycotic Admin for .msu and .msc files.
- ServiceNow ticket request numbers are displayed within Privilege Manager's prompts.
- Restrict access rights of File-Open dialogs that are launched from elevated processes.
- Domain User support in User Context Filters.
- When choosing a resource target, if an OU (Organizational Unit) is synced, the UI will display the computer and site names in their proper hierarchical structure
- When choosing a domain user for a Role, the picker now shows the domain and group membership of that user.
- Ability to [bypass policy inspection during endpoint boot-up time](#) in order to not affect boot-up time.
- Performance improvements during agent registration.
- Admin controlled list of extensions that are excluded from agent hashing.
- Application's friendly name displayed in approval workflow prompts.
- The default log size can be set using configuration settings in the administrative policies tab.
- The default permissions on the Application Control Agent Configuration Policies have been updated as follows:
 - TMS Admins and Windows Admins have read/write to the Application Control Agent Configuration Policy (Windows)
 - TMS Admins and Mac Admins have read/write to the Application Control Agent Configuration Policy (MacOS)
 - TMS Admins, Windows Admins, and Mac Admins have Read/Create/Revoke access to Install codes
- MacOS specific features:
 - Target specific commands on macOS using wildcards (starts with, ends with, contains) and regular expressions.
 - [Secure Token](#) support.
 - MacOS discovery settings are more readily accessible on the discovery configuration page.
 - [PKG files can now directly be uploaded](#) within the Privilege Manager UI, alleviating the need to first perform file inventory of those applications on the endpoints. The application policy manager has added ability to inventory a PKG file to allow building of policies prior to the discovery of the package.
 - MacOS Catalina support.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- Changing the selected collection for an SCCM collection does not correctly update membership.
- Page goes blank when navigating to Admin I Configuration and "Enable Automatic Refresh of Privilege Manager Alerts in Browser" is disabled.
- Clear remote scheduled policy parameters when the command is changed.
- Message Action text editor in UI should support formatting included in XML.
- Double-clicking on column width adjustment in the Agent Log Viewer gives an Unhandled Exception.
- The Advanced Display Message Action is running in the background.
- New schedule updates do not display clearly in the schedule.
- The Application Justification Report returns no results.
- The Resource Monitor doesn't show counters after elevation.
- The COM Objects Elevation showing Windows UAC after canceling Thycotic prompt.
- The "folder" view in the item selector does not work.
- The Event Counts on the Privilege Manager home are incorrect.
- Events are duplicated in the Event Discovery view.
- Win32Exe filter correctly handles files that have the internal attributes stripped.
- Remote/cloud connected clients that pull tasks are broken with service hardening tasks.
- The Password Age chart is broken and does not return any results.
- The Agent falls back to using legacy services and no longer retries to connect to current services.
- Offline Approval access is not available for the Privilege Manager HelpDesk User role.
- MacOS Resource Targets are not updating when trying to add to a policy.
- On mouse-over the Statistics | Changes Period to Past Month report throws an exception.
- Changing an Azure User's Role membership in Azure is not reflected in Privilege Manager.
- An exception is thrown when navigating back to the Privilege Manager home after a session timeout.
- System does not handle logins to a machine without standard SIDs.
- The horizontal scrollbar is showing in the table for Windows Privilege Personas.
- The Policies table is congested when opened in smaller resolution.
- Reports displayed from the homepage may scroll pass the pagination controls.
- The Top Applications widget on the homepage throws an exception
- Several reports on the home page are not loading properly in Firefox.
- Updates to an exclusion filter name are not displayed after editing.
- The no licenses installed banner is missing.
- Redundant warnings appear about the anti-virus exclusion settings.
- An exception is thrown when navigating to the Foreign Systems tab on the Configuration page.
- AD synchronization does not work correctly for users with distinguished names in excess of 256 characters.
- The report generated from Purge Maintenance - Files Undiscovered has duplicate messages.
- The Agent configuration form does not show previous values when a user clicks cancel.
- Privilege Manager instances with Secret Server integration:
 - Secrets deleted from Secret Server create duplicate user credentials.
 - The expiration of a Secret Server session does not prevent access to Privilege Manager.

- Changing Secret Server Role Permissions for Privilege Manager requires recycling TMS application pool.

- If you are upgrading from an older Privilege Manager version (pre 10.5) contact Thycotic Support for assistance.
- Agent Hardening does not allow for an automated rollback. The workaround is to manually [Restore Default Agent Permissions](#).
- If an issue is encountered with local UI preferences, Thycotic recommends clearing the local storage cache to remove old preference values. This can be done by going to **Admin | Diagnostics** and clicking the **Clear Local Storage Cache** button.
- Creating copies of a Persona or currently selected task schedule does not work.
- The File Specification Filter definition does not work on macOS 10.15 (Catalina) when the File Names field starts with **com.apple.preference** and/or Path field starts with **/System/Library/PreferencePanes/**. Any Policies leveraging these filter definitions is also impacted.
- In Safari and Edge browsers column filtering for the Agent Policy State and Agent Policy State - Drilldown reports does not work.
- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.7 macOS endpoint agent.
- Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
 - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Server authentication, restarting the Privilege Manager app pools may be required to have this take effect.
 - Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

10.6 On-prem Release Notes

Release Date: 07/11/2019

Enhancements available with the 10.6 On-premises release of Privilege Manager include:

- The **Syslog integration** options have been improved and support for HTTP/HTTPS was added. The HTTPS option specifically supports integrations with DEVO. (Also available in Cloud release.)
- A **Getting Started dialog** provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup.
- An **Offline Approval Process** has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- **Filters/Actions** have been added in support of various new Privilege Manager functionality:
 - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
 - Copy Install Application (macOS)
 - User Requested Run As Administrator Filter (macOS)
 - Executable Declared as Privileged Filter (macOS)
 - Codesign Elevated Application Filter (macOS)
- **Direct approval process selection for ServiceNow** is now available in the Privilege Manager UI, and no longer requires SilverLight.
- The Windows agent supports the **display of the ServiceNow approval request ID** after the approval has been submitted.
- **Integration to use Azure AD as an authentication provider has been improved.** It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. <https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server>. Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. <https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync>
- **New macOS features** refer to the [Mac User Guide](#) for detailed information.
 - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
 - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A setting was put in place to **cap the maximum number of events** that can be sent back to the server at 1 Million events. Once that threshold is reached, the oldest event is purged from the list. This setting can be adjusted in the Advanced section of the Configuration page.
- A **browser-based server Log Viewer** is now available from the Admin menu.
- **Error notification and performance in high latency environments** have been greatly improved in this release.
- **Bulk delete actions** have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to "when ANY match" for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items.

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
 - When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
 - The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
 - Unable to edit configuration of "All Other Users and Groups" for groups in local security from "ignore if found" to "Remove if found". When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the "RemoteScheduledClientCommandContract" for the group that is having the issue, removing the input parameters for the provisioned group, and then retrying the change.
 - Error upgrading to 10.5 US Directory Services for some specific conditions.
 - LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
 - The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
 - The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
 - The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
 - After reboot, the endpoint agent creates a certificate based on the UUIDCache information causing an invalid agentID error.
 - A macOS account with a computed RelativeID (RID) that is null results in an exception that causes Local User Inventory to fail.
 - MacOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
 - After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
 - During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
 - Built-in Privilege Manager User does not have read access to policies.
 - Privilege Manager relies on the Require Folders for Secrets Secret Server setting during integration set-up.
 - Login button is displayed after authentication with Secret Server.
 - Customer upgrading from version 8.x have issues deleting or saving items with GUID 71f3e19c-625c-4696-80e6-c9616554cb3c.
 - UAC Override policy does not go into effect until UAC Override scheduled task is run.
 - Event discovery resources stuck in Pending Assignment status.
 - On macOS endpoints with agent version 10.6.19 installed, depending on the user interaction with the approval dialog, it is possible that after clicking Continue or Cancel the dialog is redisplayed and cannot be dismissed.
-
- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.
 - If a customer implementation uses the Microsoft Azure Service Bus for their Internet connected clients, the clients will **NOT** be able to communicate with the Privilege Manager server after an upgrade to 10.6. Contact Thycotic Support if you are using Microsoft Azure Service Bus and are planning to upgrade. This does not impact implementations using a Reverse Proxy.
 - Privilege Manager macOS Administrator and Privilege Manager Windows Administrator roles:
 - If you are using the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles, you must also add those members to the Privilege Manager Users role or they may not be able to view some of the application filters or actions. If you are using Secret Server authentication, restarting the Privilege Manager app pools may be required to have this take effect.
 - Members of the Privilege Manager macOS Administrator and/or the Privilege Manager Windows Administrator roles may not be able to delete some items such as policies, actions and filters, even though they are editable. Have a member of the Privilege Manager Administrators role delete those items if this occurs.

10.6 Cloud Release Notes

Release Date: 05/30/2019

In this new release, Thycotic expands its Enterprise-Grade Privileged Access Management (PAM) as a Service, offering Privilege Manager in the cloud and building upon its industry-leading cloud-ready solutions.

Enhancements available with the 10.6 Cloud release of Privilege Manager include:

- A Getting Started dialog provides information on initial configuration steps and links to documentation to guide customers through configuration, integration, and setup steps.
- An Offline Approval Process has been implemented so end users can request an approval for an application to continue to execute even if an endpoint is offline. Approval workflows usually require an endpoint to be online to send out the approval request and then receive an approval for an application to continue to run or execute. The offline approval dialog can be customized within the policy action configuration area. Summary reports for offline approvals are available via the Reports page in Privilege Manager.
- Clear communication for regularly scheduled or emergency maintenance tasks:
 - In Privilege Manager Cloud environments regularly scheduled maintenance tasks will be announced via a maintenance banner at least 14 days prior to the maintenance window being in effect.
 - Thycotic will announce any regularly scheduled and emergency maintenance to inform customers when maintenance is performed on the cloud instance.
- Filters/Actions have been added in support of various new Privilege Manager functionality:
 - Application Approval Request (with Offline Fallback) Message Action (Windows, macOS)
 - Copy Install Application (macOS)
 - User Requested Run As Administrator Filter (macOS)
 - Executable Declared as Privileged Filter (macOS)
 - Codesign Elevated Application Filter (macOS)
- Direct approval process selection for ServiceNow is now available in the Privilege Manager UI, and no longer requires Silverlight.
- The Windows agent supports the display of the ServiceNow approval request ID after the approval has been submitted.
- Thycotic One is the access portal to Privilege Manager Cloud and provides data center access/support via Thycotic One US East, EU, and Australia Azure geo locations.
- Integration to use Azure AD as an authentication provider has been improved. It is now possible to specify the Client ID and the Client Secret in the configuration for Azure AD. If not specified, the associated user credential will be used. This enables customers to use just one credential for both import and login, or use separate ones based on preference. <https://thycotic.force.com/support/s/article/PM-How-to-Configure-Privilege-Manager-with-Secret-Server>
Local Active Directory accounts can be imported and synchronized with Azure Active Directory. Tasks have been added to support importing a subset of the directory instead of needing to import the entire directory. <https://thycotic.force.com/support/s/article/PM-Setting-Up-Azure-Active-Directory-Sync>
- macOS, refer to the Mac User Guide for detailed information on the new macOS features.
 - A policy can be created to allow or deny standard users to install specific applications by copying the application into the Applications folder.
 - Just as on Windows endpoints, users can request application self-elevation via a context menu action on macOS system endpoints. The application control is policy based and the macOS system with the endpoint agent must have been online at least once to request its policies from the Privilege Manager server.
- A policy was put in place to cap the maximum number of events that can be sent back to the server at 25000 events. Once the 25000 event comes in, the oldest event is purged from the list. For troubleshooting purposes this can be temporarily adjusted by Thycotic support.
- A browser-based server Log Viewer is now available from the Admin menu.
- Error notification and performance in high latency environments have been greatly improved in this release.
- Bulk delete actions have been added to support the removal of large numbers of file resources without timeouts.
- The Resource Targets on the Conditions tab of an ACS policy has been renamed to "when ANY match" for clarification of scope.
- General improvements to the Groups view within the Local Security area.
- The Privilege Manager feature to support RDP session monitoring is being discontinued.

Listed below are the bugs that have been addressed in this release. The description below reflects the product behavior prior to the fix and specific details about the fix for some of the items

- In the Privilege Manager UI domain users cannot be added to TMS Roles, only groups may be added.
 - When the URI information is deleted from an existing SMTP server configuration, the URI entry box disappears from the UI.
 - The Privilege Manager UI does not correctly load policy details with large numbers of filters configured. Paging functionality has been added, defaulting to 10 items per page viewed. This can be customized on any given list page to a view of up to 100 items per page.
 - Unable to edit configuration of "All Other Users and Groups" for groups in local security from "Ignore if found" to "Remove if found". When this issue occurs, Privilege Manager will show an error, which then allows the user to fix the error by navigating to the "RemoteScheduledClientCommandContract" for the group that is having the issue and removing the input parameters for the provisioned group and then retry the change.
 - Error upgrading to 10.5 U3 Directory Services for some specific conditions.
 - LSS Member filter does not work if the number of members across endpoints and the number of endpoints is large.
 - The Privilege Manager Remove Program Utility displays incorrect buttons for NoModify and NoRepair registry keys.
 - The Add/Remove Programs Utility is preventing repairs to Microsoft Office products.
 - The User Context Filter via SID Filter "create page" validation causes an error, which prevents the SID to be saved.
 - After reboot, the endpoint agent creates a certificate based on the UuidCache information causing an invalid agentID error.
 - A macOS account with a computed RelativeID (RID) that is null results in an exception that causes Local User Inventory to fail.
 - MacOS: The Administrator account (500) is required to be added to the managed Administrators (544) group.
 - After editing a managed local group, the list of members will sometimes expand to include what appears to be the entire list of all users in the system. Refreshing the console will return to showing just the members that were configured.
 - During Event Discovery, if the same file is discovered from 2 policies, only one file entry will be removed but receive an Acknowledge All. The second listing of the same file cannot be removed.
 - Built-in Privilege Manager User does not have read access to policies.
-
- The Local Active Directory features exists, but requires a direct connection to the domain controller, which is often not permissible due to firewall configurations.
 - Secret Server integration for authentication and vaulting of local account credentials is not presently available.
 - All license key management is done via Thycotic and license keys are not visible on the licensing page. There are not presently options for customers to add additional licenses directly.
 - Access to the Security Manager console (Silverlight version) is not available.
 - Personas are not available.
 - Server-side Powershell scripts not signed by Thycotic are not allowed. Custom server-side work can be done via Professional Services engagements.
 - The setup is managed by Thycotic and installations, upgrades, and repairs are unavailable to the customer directly, this includes setup, add/remove feature options, and connection option to existing Secret Server. Upgrade notices and banners are removed with upgrades being handled by Thycotic during maintenance periods.

All other features and functionality of Privilege Manager On-premises and Cloud are the same.

- The macOS self-elevation feature is not supported for systems running macOS 10.11 (El Capitan). The Privilege Manager Finder Extension does not work when installed on macOS 10.11. Thycotic recommends upgrading macOS endpoints to a newer version of the macOS operating system to utilize the latest feature enhancements in the Privilege Manager 10.6 macOS endpoint agent.

10.5 and Previous Releases

Release Date: 12/11/2018

Enhancements

Listed below are the enhancements being provided in this release:

- When creating a resource target for a policy, the "Groups" option is available to allow targeting of organization units (OUs). See article: <https://thycotic.force.com/support/s/article/User-Defined-Resource-Targets-and-Collections>
- A new report called "Server Node Status" will show the version installed on each server node in high availability environment. This report will inform customers of the installed version of Privilege Manager across multiple instances for high availability.

Bug Fixes

Listed below are the bugs that have been * Fixed in this release. (The product behavior is described as it was prior to the * Fix. In a few of the items below, the specific * Fix is also described.)

- Users with the Privilege Manager Helpdesk Users role are unable to approve items; get an error message.
- Authenticated XAML message does not work if agent cannot connect to domain. * Fix: When validating credentials, if the domain is not available Privilege Manager will now authenticate against the operating systems so that (if the domain isn't available) the agent will use the local database SAM cache.
- Purge Maintenance task times out on extremely large tables when performing a deletion of millions of records.
- Exporting the Application Summary Report to CSV fails.
- During upgrade, some servers don't have proper permissions to allow writing new certificates to C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys. * Fix: A new error message was added for Privilege Manager servers that do not have proper permissions during the upgrade to write new certificates to: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys.
- After successfully adding the first license, message saying "No records to display" is still displayed.
- Licensing page does not display an error if importing an invalid or duplicate license.
- On some reports, some valid filterable values are not being displayed as a selectable option after selecting the "Filter Report" button.
- Labels and information displayed when viewing a task does not properly align when the screen size is small.
- Option to "Backup the System" under "Client System Settings" policies does not elevate without selecting to apply to child processing. * Fix: Elevation will now occur automatically without having to change the child processing setting.
- Some Role membership group names are in all lowercase, not Pascal case.
- On the Help page, the link for the user guide is pointing to the Preferences page instead of the actual user guide.
- User is unable to press the 'Cancel' button on the Preferences page.
- When the browser is made smaller, the page to create scheduled tasks has overlapping text.
- When editing a copy of the "Approval Request Form Action", the selected value in the "Approval type" disappears when switching from view mode to edit mode.
- Changing the "Minimum Security Level" field in the console log settings is not limiting the records displayed in the logs.
- "Base URL" field for Privilege Manager server under Foreign systems reads as "Base URI". * Fix: Text of the "Base URI" label in a Foreign System has been changed to "Base URL".
- Selecting options besides the "Upper Case" option when configuring a user's password results in "Undefined" being displayed as a selected option.
- Incorrect error messages are displayed if a new User credential is saved without or with an incorrect password.
- After clicking "Import" on the Import Items page, the import button does not grey out to display feedback that the import is processing.
- Exception is thrown on "Client System Settings" page when the Assign Filter field is left blank.
- Assigning filters to any of the items in "Client System Settings" can cause the page to become unresponsive.
- On the Time of Day filter, changing the time under "Different Periods on Different Days" also incorrectly changes the times under "Same Period Every Day".
- Clicking the Sort column of an empty report causes page to error.
- When deleting a filter or an action that is used in a policy, Privilege Manager correctly prevents the deletion but displays an incorrect error message.
- When building resource target queries, starting with "All Computers" causes poor performance. * Fix: This been removed from the default way resource target queries are built.
- "OU Directory Scope Collection Update" task fails if Collection.LastUpdated is null.
- Applications hang if a new certificate is created and the agent requests new client items before it updates applicable policies or registers with the server.
- Installing a new agent on a Mac endpoint results in a corrupted schedules.plist file.
- Azure AD tokens are expiring within minutes. * Fix: Azure AD will now last as long as normally issued tokens.
- If the "UNC Elevation Policy Template" Config Feed is imported, the "UNC Content Query" is erroring.
- When Secret Server and Privilege Manager are installed together using the combined installer, and a separate domain account without write permissions is used, subsequent upgrades fail if the domain account running the application pool does not have Write permissions on the TMS web folder.
- "Advanced Deny Notification Actions" are not included in dashboard counts and the list of denied files.

Release Date: 9/25/2018

Bug Fixes

- Fixed issue where the Mac agent configuration did not have a default task check in interval saved.
- Fixed issue where queries for reports that are scoped to display only certain resources will fail if the Default Security Descriptor ID is null or empty.
- Fixed issue where large Active Directories caused the Collection and Resource Targeting Update task to run for too long.
- Fixed issue where Privilege Manager's authentication provider screen would crash if incorrectly configured. When Privilege Manager cannot reach an Active Directory domain, a useful error message is now displayed.
- Fixed issue where Privilege Manager task schedules are not properly saved and displayed.
- Fixed issue where the dashboard would display an unexpected error in a modal popup the state of a gauge undefined.
- Fixed issue where the sign-in page URL query string could be used to redirect a user to another URL by only allowing relative URLs.
- Fixed issue where Telerik grids were not able to be resized when zoomed in or out in Chrome, Firefox, and Edge.
- Fixed issue where the GetToken API returned an invalid token for unauthorized requests instead of a 401 response code.
- Fixed issue that allowed Privilege Manager to be embedded inside of an iframe.
- Fixed issue where a New Loaded Resource file is not assigned to an endpoint's agent after the Resource Discovery task is executed once.
- Fixed issue where the Resource Discovery task does not finish and will continue to display a spinner when discovering a New Loaded Resource file that is not assigned to an endpoint's agent.
- Fixed issue where a New Loaded Resource was not discoverable if the location has been discovered but the file has been removed from the endpoint.
- Fixed issue that displayed the HTTP status code instead of the actual server error when bad XML was imported to Privilege Manager.
- Fixed issue where the data grid within a policy that displays all the filters loads slowly.

Mac Agent Updates (version 10.5.12)

- Fixes issue where the Mac agent was not properly logging failed agent registration attempts when an invalid install code was used.
- Fixed issue where Mac agent was writing exceptions to the logs if v4 agent registration fails when connecting to a Privilege Manager version prior to 10.5.
- Fixed issues where initial basic inventory was not being removed after first running.

Release Date: 9/04/2018

Bug Fixes

- Fixed issue where Privilege Manager, when configured with Secret Server for authentication, did not properly fall back to NTLM authentication if Secret Server was not properly configured.
- Fixed issue where Privilege Manager upgrade failed if duplicate IDs existed in [Ams].FileUploads or [Ams.Data].Win32_OperatingSystem tables.
- Fixed issue where Privilege Manager did not prevent deletion of an item referenced by another object. For example, it did not block a filter from being deleted if that filter was also being used by an active policy.
- Fixed an issue where the delete operation of computers did not properly display completion for long-running deletes.

Release Date: 8/15/2018

Overview

Notable enhancements to 10.5 include a new dashboard as the home page, integration with Cylance reputation analysis, support for Azure Active Directory, performance enhancements, and improved agent security.

Important for Secret Server Combined Upgrades

If Secret Server is installed in conjunction with Privilege Manager, Secret Server must be upgraded to 10.5.000001 before you upgrade to Privilege Manager 10.5.000000.

10.5 Agent Upgrades

Unless the "Prevent Legacy Agent Registration (10.4 and older)" option is checked (Admin > Configuration > Advanced), older agent versions will still function in Privilege Manager 10.5.000000, but Thycotic recommends that you do upgrade Privilege Manager agents to the 10.5 version due to security enhancements.

Note: That when installing new 10.5.000000 agents you will be prompted to install with a valid Install Code.

Enhancements

- New dashboard for deep reporting and visibility into the state of Privilege Manager.
- Integration with Cylance for real-time threat intelligence policy checks.
- Support for Azure Active Directory for authentication, resource targeting, and user context filters.
- Excel reports that are exported are sanitized to prevent macro injection attacks against end-users who open the Excel files.
- Cross site request forgery prevention implemented.
- Sensitive data encrypted on endpoint with machine, non-global key.
- Agent installation requires agent install code as a parameter or as a field entered when using the bundled installer for additional security.
- Redesign of agent/server trust requiring shared secret before agent can register with server and receive policies.
- Redesign of client item encryption to improve security.
- "Add new filter" and "Add to policy" buttons are on resource page for MSIs and scripts.
- Support for inventory filters added as secondary file filters to allow targeting of MSIs and scripts by hash.
- Support wildcards in fields of the Win32 executable filter. See inline help for details.
- Added SQL indexes for improved performance.
- Collection update and resource targeting update tasks are combined into task called "Run Policy Targeting Update."
- Allow unattended uninstall of Mac agent by adding command-line option to suppress the user confirmation prompt.
- Reduced the time it takes a newly installed agent to download policies.
- Advanced message options for justification window supports end user authentication.
- Default to validating client item signatures on Windows agents.
- Support and maintenance license are viewable on the licenses page.
- Option to "Apply action to child processes" is unchecked by default.
- Deployment tab of a policy will display a button to update the collection of resource targets on demand.
- EULA not shown upon product upgrade.

Bug Fixes

- Fixed issue where Administrator group incorrectly displayed SYSTEM account as a member.
- Fixed issue where Server URL on agent was not updated if server was changed.
- Fixed issue where setting password rotation for a one-time update failed to rotate the password.
- Resolved error when custom approval process was initiated.
- Processed events are purged up from the [AMS.DATA].FileUploads, [AMS.DATA].FileUploadChunks, and [AMS.DATA].FileUploadSessions tables.
- Fixed issue where changed numeric values on the Advanced tab of the configuration page were not saved.
- Resolved schedule creation error in certain time zones.
- Resolved an issue where provisioning a local user would enable a disabled account and/or disable an enabled account.
- All internal links to support documentation now utilize https.

Known Issues

- If Secret Server is installed in conjunction with Privilege Manager, Secret Server must be upgraded to 10.5.000001 before you upgrade to Privilege Manager 10.5.000000.
- Agent trust is broken if VM UUID changes. Agent must be reinstalled to resolve.
- On the user screen in local security, the text "undefined" will appear if any option for password "Characters" is selected except "Upper Case."

Release Date: 3/28/2018

Bug Fixes

- Resolved issue to ensure the trimming of the table storing data from uploaded files

Release Date: 3/6/2018

Enhancements

- Support for SQL 2017
- Support for agent communication on Windows 7 systems with TLS 1.1 and SSL 3.0 disable
- Checks for a valid maintenance license to allow product upgrades
- Client item cache is cleared automatically
- Clicking the "Run" button for tasks indicates successful execution and prevents kicking off of multiple tasks
- Built-in administrator is prevented from being removed from group and the associated operation will display "Required Account"
- Support "log4net log (.log)" format in the Thycotic Monitor

Bug Fixes

- Reports on "Managed Local Users" and "Managed Local Group" will now allow users to select the account name as a drill through to a report on the computers the account exists on
- Breadcrumbs will display the correct name after renaming a computer group
- Upgrades will retain security ratings setting for VirusTotal
- Custom time of day filter correctly saves
- Simple policy view allows for new filter to be saved inline
- The popup allowing users to add a new account to a group allows sorting
- License correctly determines client and server types during basic inventory
- Ability to clone credentials has been removed when Privilege Manager stored credentials in Secret Server
- Resolved searching for filters from within the secondary file filter
- Upon saving group membership, the operation column correctly displays the action that will be taken on the associated account
- Resolved validation of password field for a managed user when using Edge browser
- Charts on the statistics page scale correctly for both small and large number of endpoints
- Resolved issue that prevented enabling of firewall policy
- Password scheduler saved when UTC is selected
- Allow domain groups to be members of roles
- Resolved issue preventing application inventory on network shares
- Prevent non administrative access to the Thycotic folder on local drive

Release Date: 1/17/2018

Enhancements

- Least Privilege Enforcement for Local Users and Groups
- Provision local users and groups across all endpoints
- Permanently remove accounts from privileged local groups
- Prevent group membership from being changed directly on the endpoint, even by an administrator
- Local Account and Credential Management
- Uniformly apply user properties to local accounts
- Set secure and unique passwords for local accounts by defining character requirements and password length
- Rotate local account passwords automatically on a scheduled basis
- New and Enhanced User Interface
- Least Privilege features are built on top of a new easy to use and manage interface within the Local Security section of the application.
- Policies are easily deployed to groups of users or endpoints, making it easy to deploy least privilege in a phased approach
- Dashboard, reporting, and statistics are built into the interface to understand the current state of local users and groups on the endpoint and any changes. Easily spot vulnerabilities and trends.
- Actionable tips will appear inline when the environment is not following best practices
- Usability enhancements to application control functionality
- All grids have filtering options to narrow down large datasets
- Integration with Secret Server
- When using both Privilege Manager and Secret Server, passwords can be stored in Secret Server's vault
- Intended for use on endpoint workstations where remote management of local or non-domain accounts is not possible
- Secret Server enterprise PAM features can be used upon secrets that are managed by Privileged Manager
- Role Based Access
- Define users of the Privilege Manager application: set administrators, read only users, Mac OS users, Windows OS users, and helpdesk users
- Security trimmed access specifically designed for help desk users, who's responsibility it is to disclose passwords and approve/deny applications
- Reporting and Dashboards
- New reports provide visibility into local user and group membership, an audit of passwords that have been disclosed, a summary of local administrators, and all computers with passwords being managed by Privileged Manager
- Contextual reporting for each group of users and computers where least privilege policies are being applied to understand the affect of policies on users
- Simple charts provide an understanding of all endpoints with each individual user or group
- Dashboard will display trends of user's group membership changes, users being added and removed from groups, and passwords being disclosed. Trends provide insight into understanding outliers and potential rogue activity.
- Endpoint Visibility Utility
- Simple console deployed directly on the endpoint to check the communication status, register with the server, get the latest policies, view and export the logs.
- Ideal for enhanced visibility and understanding, especially when working directly with internal Thycotic support or professional services.

Bug Fixes

- Language and text * Fixes on installer screens for non-English systems
- Issue where Privilege Manager's MacOS copy helper would perform the copy without waiting the approval to complete. After * Fixing, we can now target .pkg files with policies.
- Secondary file filter will detect scripts being executed on Windows 10, after changes were made on how PowerShell scripts are launched on the OS
- Allow install (and pre-req install) to succeed if PowerShell Execution Policy is set to RemoteSigned in Group Policy
- Editing the Application Control Configuration policy will not set some values as blank
- Allow for configuration of "days" parameter for Purge Old Computers Task
- On MacOS, track which certificate Privilege Manager received the most recent time it was registered.
- Ability to assign ServiceNow Process in Execute App Type through Privilege Manager UI

Known Issues

- On Windows 10 Enterprise edition with patch version 1709 (released October 26, 2017), UAC is not suppressed, and thus end users are prompted to enter admin credentials
- Unable to Clone Credential when Secret Server is used as vault
- Agent is not communicating to server on Windows 7 over TLS 1.1
- Creating a File Hash specific filter fails if there are spaces at the end of the hash

Release Date: 8/29/2017

Enhancements

- Implemented automatic and continuous server-side logging
- Incorporated sandbox actions, allowing policies to limit the environments in which applications can execute
- On demand retrieval of a newly discovered file after event discovery. When "New Loaded Resource" is displayed, the user can click a new button called "Discover Now" to retrieve resources data.
- New check box added to the Event Discovery configuration to find all applications that require administrator rights to run ServiceNow configuration improvements
- Option to run the installation just for Secret Server, without installing Privilege Manager
- Upgrade of Privilege Manager will not require local admin rights when installed in conjunction with Secret Server
- Display warning if policy does not target any application
- Policy creation screen will remember simple or advanced view preference
- Paginate Resources list view
- Improved error handling on installation and the addition of an error icon indicating an issue

- Fixed issues in the VirusTotal reputation calculation and service call handling
- Upgrading a product within the setup app will also update dependent products
- Log files are now being stored to disk
- Installation Summary report now includes the last time agents registered
- Enhancements within installer for web applications to run as a user account
- Enhancements to better show report rows and chart sections that can be clicked into for drill-down into another report

Bug Fixes

- HTTP binding is not required on Privilege Manager website
- VirusTotal configuration is retained after upgrade or repair
- Issue installing the file inventory with machines using non-US date/time
- Trailing slash () will not affect the path field in Win32 and File Specification filters
- Future changes to agent configuration policies will be preserved and not overwritten
- All system policies are prevented from being edited so the user can create a copy

Release Date: 7/12/2017

Enhancements

- Added an agent to allow whitelisting, blacklisting, approvals, and elevation on Macs.
- Added "easy Policies" to allow for simple ways of creating whitelists and blacklists.
- The dashboard is now a series of tiles designed to give a simpler experience.

Release Date: 4/12/2017

Enhancements

- Updated Installer
- New installer to handle more prerequisites for HTTPS Bindings, WCF, and SQL
- Updated setup home for managing product upgrades going forward
- Session Monitoring Agents
- A new agent and policy is available to record RDP and console sessions. Note that this requires a Secret Server installation and licenses.
- For more information on RDP monitoring policies see this KB article

Release Date: 1/18/2017

Enhancements

- Added page specific help into Privilege Manager console
- Added options in the Discovery for kicking off inventory tasks to expedite policy testing
- Brought EMET policy options into the Privilege Manager console
- Brought the Application Firewall policy options into the Privilege Manager console
- Added configuration feeds for uploading policies and other items from support.

Bug Fixes

- Fixed issue where adding a new Persona and going back to the persona home required a browser refresh to see the new Persona
- Fixed issues in IE where the Report title text on the report home was not a link.
- Fixed issues with configuring Active Directory domains.

Documentation Changelog

This topic provides a chronological list of documentation changes. Minor content alterations are not tracked.

- Added [Legacy System Extensions](#) topic.
- Updated [10.7.1 Release Notes](#) to reflect Agent software version updates and associated bug fixes.

Support

Thycotic customers have access to support by phone and email. You also can open a case in Thycotic's support ticketing system, which promotes follow-through to issue resolution.

Note. Please see our [Support Services Guide](#) for details about our support policy. This page provides a high-level summary of portions of that guide.

Use the means you prefer, except for Severity 1 issues—for those, always use phone support.

Severity 1 means a critical problem that has caused *complete loss of service* and work cannot reasonably continue at your worksite.

To obtain support by email or phone, first log in to the Support Portal to obtain a PIN. The PIN validates that your license includes support, and you must provide the PIN in your email or when you call. The PIN also makes it easier for the person helping you to locate your customer records and give you better support.

- Visit the [Support Portal Login Page](#) using the credentials you received when you became a customer.
- After logging in, you will be on the main page. Click on the large blue bar labeled PIN to obtain a PIN number.

Thycotic delivers support by phone worldwide. Select the applicable number from this list:

AMERICAS	all	+1202 991 0540
EMEA	UK	+44 20 3880 0017
	Germany	+49 69 6677 37597
APAC	Australia	+61 3 8595 5827
	Philippines	+63 2 231 3885
	New Zealand	+64 9-887 4015
	Singapore	+65 3157 0602

Send your email to support@thycotic.com **with the PIN number as part of the subject line** of your email, for example:

- PIN 345 Workflow Stopped Unexpectedly

Include this information:

1. company name
2. contact name
3. contact phone number
4. product name
5. details of the issue

You must send your email using an email address already noted in your account with Thycotic.

- Sending a support request from an email address not on file may delay our response.

As an alternative to support by email or phone, you can open a support ticket and track your issue to resolution.

- Visit the [Support Portal Login Page](#) using the credentials you received when you became a customer.
- After logging in, you will be on the main page. Click the **Cases** tab, then **Create a Case**.
- Follow the instructions to complete your case.