Delinea

Connection Manager

Administrator Guide

Version: 2.9.x

Publication Date: 7/24/2026

© Delinea, 2026

Connection Manager Administrator Guide

Version: 2.9.x, Publication Date: 7/24/2026

© Delinea, 2026

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Administrator Guide i

Introduction to Connection Manager 1

Installing Connection Manager 1

Permissions Required to Install/Uninstall Connection Manager 1
Product Versioning 1
Connection Manager Hashes 2
Version 2.8.3 2
Version 2.8.0 2
Version 2.7.1 2
Version 2.7.0 2
Version 2.6.1 2
Version 2.6.0 3
Version 2.5.4 3
Version 2.5.3 3
Version 2.5.2 3
Version 2.5.0 4
Version 2.4.0 4
Version 2.3.1 4
Version 2.3.0 4
Version 2.2.0 5
Version 2.1.0 5
Version 2.0.1 5
Version 2.0.0 5
Version 1.9.6 6
Version 1.9.5 6
Version 1.9.2 6
Version 1.8.0 6
Version 1.7.1 Hashes 6
Version 1.7.0 Hashes 7
System Requirements 7
Installing on Windows 7
Installing Connection Manager for All Users on a Machine 7
Installing Connection Manager Per User 11
Updates 16
Installing on MacOS 16
Delinea Encryption Key 17
Command Line Arguments 17
Per User Installation via Quiet Mode 19
Changing the Location of the .DAT File 19
Changing the Installation Path 20
Pre-Configuring Vault Connections on Install 20

Disabling Local Vault on Installation 21
Enabling/Disabling Auto Reauthenticate 21
SSH Authentication Method Setup on the Target Host 22
Setting the Screenshot Queue Limit 22
Disabling Update Check on Startup 22
Specifying Custom Logo Images to Copy to the Proper Location 22
Delinea Platform Connection 23
Pre-Creating a Secret Server Connection 23
Customizing External Browser Authentication 23
External Browser Connection 25
Local Connection 25
Internal Browser Connection 25
Disabling Local Vault 26
Disabling Local Vault via Admin Enforcement 26
Disabling Local Vault via Admin Enforcement on Windows 26
Disabling Local Vault via Admin Enforcement on MacOS 29

Getting Started 30

Creating a Password 30
Signing into Connection Manager 31
User Interface Components 33
Display Themes 33
Main Screen 33
Menus 33
Stack Menu 33
Right Click Navigation Menu 35
Work Area Menu 35
Search 35
Template Search 36
Global Search 36
Configuration 36
Navigation Tree 36
Active Sessions 36
Favorites 37
Shared With Me 38
Recent 38
Connections 39
Local Connections 40
Shared with me 41
Configuration 41
Properties Area 41
Work Area 42

Authenticating to a Vault 42

Authenticating to a Delinea Platform Vault 42

Authenticating to the Delinea Platform via External Browser 43
Authenticating to the Delinea Platform via Internal Browser 47
Enabling Internal Browser Authentication 55
Authenticating to Secret Server 55
Secret Server Requirements 56
Authenticating to Secret Server via External Browser 56
Authenticating to Secret Server via Internal Browser 61
Enabling Internal Browser Authentication 65
Authenticating to Secret Server via Local Username 66
Authenticating to a Local Vault 73
Local Vault Enabled 73
Local Vault Disabled 73
Enable or Disable Local Vault on Installation or Upgrade 73
Windows 74
Mac 74
Enable or Disable Local Vault When Authenticating to Secret Server 74
Enable or Disable Local Vault at Any Time 75
Default Local Vault Location 76
Changing Local Vault Location 76
Re-authenticating to a Vault 76
Modifying a Vault 78
Removing a Vault 81

Session Connections 82

Remote Systems 82
Creating Connections 83
Opening Connections 84
Editing Local Connections 86
Deleting Connections 90
Duplicating Connections 91
Integrated Connections 91
Credentials 91
Map a Vault Secret to a Folder 92
Map a Vault Secret to a Connection 94
Importing and Exporting Connections 95
Exporting Connections 96
Importing JSON Files 96
JSON Example 97
Importing Devolution Files 98
Importing RDG Files 100
Importing RDP Files 101
Importing CSV Files 105
Import Local Connections 106
Field Values and Types 110
Import Completed Reports 113

CSV Import Differences ... 113

Global Configuration Settings ... 113

Windows Shortcuts ... 114
Map Windows Shortcuts on MacOS ... 115
Audio Playback and Audio Recording ... 116
SSH Global Settings ... 117
Globally Enforced Secret Server Settings ... 121
Using a Custom Logo in the Connection Manager Interface ... 124
Manual Procedure ... 124
Command Line Procedure ... 124
Protocol Handler Approved URLs ... 125
Protocol Handler Allowed Domains in the Registry Editor ... 125
Desktop Size and Auto Expand ... 126
Automatic Back Up for .DAT Files and Configurations ... 128
Default Settings ... 128
Adjusting the Default Settings ... 129
Restoring .DAT Files From Backup Location ... 129
Backup Locations ... 130
Authenticating With WebAuthn ... 130
Enabling WebAuthn ... 130
Enforcing Vault Authentication for WebAuthn on Windows ... 132
Enforcing Vault Authentication for WebAuthn on MacOS ... 133
Using Smart Cards With Connection Manager ... 133
Smart Card Settings ... 133

Launchers ... 137

Proxy Tabs Show Remote Host Name ... 138
Screen Resolution for New Session Window Views ... 138
Moving and Reorganizing Session Tabs and Windows ... 138
Session Recording ... 139
Working With Third-Party Applications (Preserve SSH Client Process) ... 140
Launching from Secret Server without Connection Manager Open ... 140
Signing In After the Launch ... 141
Creating a New Local Storage File ... 142
Solution Guide: Launching SSH Sessions with Mac-Native SSH Client ... 143
Use Cases ... 143
Prerequisites ... 143
Setup ... 144
Step 1: Create a Custom Launcher in Secret Server ... 144
Step 2: Map the New Launcher to the SSH Secret Template in Secret Server ... 145
Step 3: Launch SSH Secret from Connection Manager ... 146
Known Issues ... 149
Fingerprint Confirmation ... 149
Attaching Files to Secret Launchers ... 149

Attaching Files to Secret Launchers on Windows ... 149
Step 1: Creating a Custom Launcher ... 149
Step 2: Creating a Custom Template ... 150
Attaching Files to Secret Launchers on MacOS ... 152
Step 1: Creating a Custom Script for Your Application ... 152
Step 2: Creating a Custom Launcher ... 152
Step 3: Creating a Custom Template ... 153
Launching Websites and Auto-Filling Credentials with the Web Password Template ... 154
Prerequisites ... 154
Supported Browsers ... 155
Launching Secrets ... 155
Setting the Default Launcher via Registry ... 157
Registry Key Scope ... 158
Selecting the Launcher ... 158
Use Delinea Connection Manager ... 158
Use the Secret Server Protocol Handler ... 158
Notes ... 158

Common User Activities ... 158

Connections ... 159
Batch Opening Connections ... 159
Batch Opening Connections Using Multi-select ... 159
Batch Opening All Connections in a Folder ... 160
Batch Editing Local Connections ... 161
Batch Editing Local Connections Using Multi-Select ... 161
Batch Editing Credentials for All Connections in One or More Folders ... 162
Application Configuration via Windows Registry Editor ... 163
Disabling Update Check on Startup ... 164
Enabling/Disabling Auto Reauthenticate ... 164
Enabling the Session Status Popup ... 165
Setting the Screenshot Queue Limit ... 166
Configuring RDP Connection Timeout Over TCP ... 166
Configuring SSH Connection Timeout Over TCP ... 167
Enabling WebAuthn Authentication for All Users on Windows ... 168
RDP Rendering Settings ... 169
Disabling Local Vault via Admin Enforcement ... 173
Unidirectional Clipboard Enforcement on Windows ... 174
Pre-Trusting SSH Host Fingerprints ... 175
Pre-Approving Secret Server URLs ... 175
Deprecated Settings ... 176
Application Configuration File ... 176
Windows Configuration File Location ... 176
macOS Configuration File Location ... 176
Unidirectional Clipboard Enforcement on MacOS ... 177
Enabling WebAuthn Authentication for All Users on MacOS ... 177

Preserving Configuration Changes During Upgrade on Windows ... 177
Disabling Update Check on Startup for Windows ... 178
Disabling Update Check on Startup for macOS ... 178
Enabling Software Rendering for the Internal Browser on Windows ... 178
Enabling/Disabling Auto Reauthenticate ... 178
Enabling the Session Status Popup on Windows ... 179
Configuring Proxy Settings ... 179
Setting the Screenshot Queue Limit ... 180
Configuring RDP Connection Timeout Over TCP ... 180
Configuring SSH Connection Timeout Over TCP ... 181
Adjusting the SSH Scrollback Buffer Size on MacOS ... 182
Backing Up .DAT Files and Configurations ... 182
Configuring Special Characters in SSH Connections on MacOS ... 182
Incorrect Handling of System Keys ... 183
User Configuration File for Windows ... 183
Windows Configuration File Location ... 183
Enabling/Disabling Auto Reauthenticate on Windows ... 184
Re-enabling the Web Launcher Training Dialog ... 184
Re-Enabling the Browser Extension Not Found Dialog ... 184
User Settings on MacOS ... 184
User Settings File Location ... 184
Re-enabling the Web Launcher Training Dialog ... 185
Re-Enabling the Browser Extension Not Found Dialog ... 185
Folder: Creating, Editing, Moving, Deleting ... 185
Creating a New Folder ... 185
Editing a Folder ... 187
Moving a Folder ... 187
Deleting a Folder ... 187
Transferring Files Using Local Drives ... 188
Using SSH Session Groups ... 189
Creating and Naming an SSH Group ... 189
Sending Commands to the SSH Group ... 191
Options for Displaying SSH Sessions on the Group Tab ... 192
Building an SSH Group ... 193
Closing an SSH Group ... 193
SSH Tunneling ... 193

Secrets with Workflows ... 194

Accessing Secrets Guarded by Multi-Factor Authentication ... 195
Secret Check Out Timer ... 196

Troubleshooting ... 200

Log Files ... 200
Windows Log File Location ... 200
CEF Browser Log File Locations ... 200

MacOS Log File Location ... 201
Installer Log File Locations ... 201
Changing the Log Level ... 201
Generating Additional Log Entries ... 203
Advanced Log Entries ... 203
MacOS Installer Log Entries ... 204
Troubleshooting Website Launcher Issues ... 204
Troubleshooting Unhandled Errors ... 207
Downgrading to an Older Version of Connection Manager ... 208
Delinea Vault Connections ... 208
Local Connections ... 208
Custom Settings ... 209
Fixing the .DAT File Location After Upgrading on macOS ... 209
Expected File Location ... 209
Possible Solutions ... 209
Solution 1: Move the File Manually to the Correct Location (Recommended) ... 209
Solution 2: Reinstalling Connection Manager (Not Recommended) ... 209
Troubleshooting Auditing Issues ... 210
Password Displayed Events Occurring in the Audit Log or System Log ... 210
Vault Authentication Issues ... 210
Troubleshooting Vault Authentication Timeout ... 210
DPI Scaling Issues ... 212
Display Column Issues ... 212
The Machine Field is Not Visible in the Connection Manager Grid View ... 212
Troubleshooting SSH Connections ... 213
Troubleshooting RDP Connections ... 213
Resolving Flickering Issues in MECM and SCVMM Consoles Launched via Connection Manager ... 213
Dragging Credentials from an External Password Manager ... 215
RDP Connection Timeout Issues ... 215
Troubleshooting Proxies ... 215
Issues With the Clipboard Functionality ... 215
Troubleshooting ... 216
AVBlock Error with Session Recording ... 218
Problem ... 218
Workaround ... 219
CM Crashing When Offline and Checking Certificates ... 219
Issue ... 219
Resolution ... 219
Encryption ... 219
General ... 219
What are the default locations for the Connection Manager application and log files? ... 219
Is there a local session timeout for sessions within Connection Manager (CM)? ... 219
I'm seeing a Connection failed error message while trying to connect to SS ... 219
Is there a way to refresh the SS connections? ... 220

Where and how is the data for Connection Manager stored? 220
Is there a way to push scripted code out to multiple SSH sessions at one time for updates or commands? 220
What happens if the SS Heartbeat fails? 220
Is there any current performance data for Connection Manager? Including: general memory, amount of space needed, number of open connections that can be made at one tie, etc. 220
While recording a session, if a user isn't on tab, what's the behavior? Do we reduce what we record and send? Or does it stay the same? How can we tell if it's the "focus"? 220
Host Names 220
Licenses 221
Does a Current Customer Drop in the Platinum Trial License Key Into Their Current Secret Server Instance to Receive the Connection Manager Feature? 221
Does it Matter, if Connection Manager is Working With a Different Secret Server Instance Than the One Aligned With the Trial Key? 221
Is it Okay to Add a Trial License to a Production Server? Will it Overwrite or Add to the Current License? 221
Are There Any License Restrictions to connection-manager? 221
Manually Cleaning the Connection Manager File System 221
Instructions for Windows Users 221
Remove files and folders 221
Clear entries from the Registry 222
Instructions for macOS Users 222
Troubleshooting MacOS Certificate Errors 222
Disable Certificate Revocation Check 223
Secret Server Certificate Validation Fails When Using OCSP 223
Incorrect Trust Policy in Root Certificate Authority 225
Troubleshooting Issues With Smart Cards 226
Smart Card Force Use 226

Release Notes 226

Connection Manager Version Compatibility with Secret Server 226
Release Notes History 226
2.9.0 EA Release Notes 227
Features 227
Improvements 228
Windows Specific 228
MacOS Specific 228
Fixed Issues 228
Windows Specific 228
MacOS Specific 229
2.8.3 Release Notes 229
Features 229
Fixed Issues 229
Windows Specific 230
MacOS Specific 230
2.8.0 Release Notes 230

Features 230
Windows Specific 230
MacOS Specific 230
Improvements 231
Windows Specific 231
MacOS Specific 231
Fixed Issues 231
Windows Specific 231
MacOS Specific 231
Known Issues 232
2.7.1 Release Notes 232
Features 232
Improvements 232
Fixed Issues 232
2.7.0 Release Notes 232
Features 232
Improvements 233
Fixed Issues 233
MacOS Specific 233
2.6.1 Release Notes 233
Improvements 233
Fixed Issues 233
MacOS Specific 233
2.6.0 Release Notes 233
Features 234
Improvements 234
Fixed Issues 234
Windows Specific 235
MacOS Specific 235
2.5.4 Release Notes 235
Improvements 235
Fixed Issue 236
Windows-Specific 236
MacOS-Specific 236
2.5.3 Release Notes 236
Improvements 236
Fixed Issues 236
Windows 237
macOS 237
2.5.2 Release Notes 237
Bug Fixes 237
Windows Specific 237
macOS Specific 238
Known Issues 238

2.5.1 Release Notes (Windows Only) 238
Bug Fixes 239
2.5.0 Release Notes 239
Features 239
Improvements 239
Deprecations 239
Bug Fixes 239
Windows Specific 240
macOS Specific 240
2.4.0 Release Notes 240
Features 240
Improvements 240
Bug Fixes 240
Windows Specific 241
2.3.1 Release Notes 241
Improvements 241
Bug Fixes 241
2.3.0 Release Notes 242
Features 242
Improvements 242
Bug Fixes 242
2.2.0 Release Notes 242
Features 242
Improvements 243
Bug Fixes 243
Windows Specific 243
macOS Specific 243
2.1.0 Release Notes 243
Features 243
Improvements 244
Bug Fixes 244
2.0.1 Release Notes 244
Improvements 244
Bug Fixes 244
2.0.0 Release Notes 245
Features 245
Bug Fixes 245
Known Issues 245
1.9.7 Release Notes 245
Bug Fixes 245
1.9.6 Release Notes 245
Features 245
Bug Fixes 246
1.9.5 Release Notes (Windows) 246

Features 246
General Improvements 246
Maintenance Improvements 246
Bug Fixes 247
1.9.2 Release Notes 247
Features 247
General Improvements 247
Security Improvements 247
Bug Fixes 248
iOS Specific 248
1.8.0 Release Notes 248
Features 248
General Improvements 248
Bug Fixes 248
iOS Specific 249
1.7.1 Release Notes 249
Bug Fixes 249
1.7.0 Release Notes 249
Product Enhancements 249
SSH Grouping 249
General 249
Bug Fixes 250
macOS Bug Fixes 250
Known Issues and Workarounds 251

Introduction to Connection Manager

Connection Manager provides secure connections to remote servers using RDP and SSH, allowing IT teams to launch ad-hoc connections to manage sessions with remote resources. Management of multiple active sessions is easy. You can store and organize connections by adding them to your favorites and import any folder structure or connections used in other tools for a single management hub.

It marks an expansion of Delinea's product line to include remote connectivity tools closely integrated with Secret Server. It permits technical staff to quickly access resources using the convenience of a familiar, rich desktop interface while maintaining all the safeguards and workflows included with Secret Server.

This manual includes instructions for installing and using Connection Manager as a stand-alone product or in conjunction with a Secret Server installation.

Installing Connection Manager

Connection Manager is a desktop client application that can be downloaded and installed on Windows and Mac machines. While the client application does not need to be installed in the same location as Secret Server, if users are planning to use the Secret Server integration, the machine on which Connection Manager is installed must be able to reach Secret Server. Connection Manager creates a local encrypted file storage for saving local connections and Secure Server(s) connectivity information.

For details on system requirements and the installation of Connection Manager, please follow the procedures below:

- System Requirements
- Windows Installation
- MacOS Installation
- Command line Arguments to Create a Secret Server Connection on Install

Permissions Required to Install/Uninstall Connection Manager

In order to install or uninstall Connection Manager for all users of a machine, you must have local administrator privileges.

Windows users have the option to install Connection Manager just for themselves, in which case local administrator privileges are note needed. See "Installing Connection Manager Per User" on page 11 for more information.

Product Versioning

Connection Manager versions 1.9.2 and older will only include the release version in a three-digit format. Connection Manager versions 1.9.5-20221219.1 and newer will include the following elements:

- Version number
- Release date (YYYYMMDD)
- Build number

Connection Manager Hashes

This section lists the installer hashes for different versions of the product.

Version 2.8.3

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 2489a87fe017f7af1a4bae75a8cbc29e7737b96e
- SHA256 6f1946c09034f466a47e4358185f317eb74d1bee624e4c43ee627c473e755921

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 77db185d242021c79984290043a49b69dbd9673e
- SHA256 3be04f4cbaa14026980c67cd217992645ab00c9570ea5dcf4e3cffc144c4460a

Version 2.8.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1: 44a1aa928d49d9aa53054242eb0661fe1a141672
- SHA256: 65a383fc1dde7d248ca8711941d8aa7d9e046de28f2573f83566f16612544a0e

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1: a8eaadb06a7ce2a03d3b0a59b56dddc7930e9caa
- SHA256: 66cd78c04486e2ba4d50dd18cbcb80295da964857217bca58cd1c68c7383646f

Version 2.7.1

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 17687334ea90d5103dba1aaff85c21c6f8df5225
- SHA256 0698d3a4c746a0186b6043c15918c8ed3b3e0f467b5543f3dec4e8df465c3ef5

Version 2.7.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 e7fc1e68ee546d019266bfb7cabb7ab2f986c29c
- SHA256 ee9754ed7b0f11b7fa9e8ba113a0580e8f16c15ec32fec558ec4228848376fa1

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 230b94f2c3d812c5d06318cad71a6d4a4ae4afaa
- SHA256 56bbc61b14047b298fbde3c1343ab340adaf7a91d2d5702de1e983990bbae3da

Version 2.6.1

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 e9850c7cc165affb02c1e0219454928ebd1a3889
- SHA256 dcfed77d1a525881447cae028003dbfeab6ed0ee84074fbf3ac9b276efa966a7

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 d03d261ab3edc9d1396e930ca3721201b614c4ca
- SHA256 18aa9b6f89529468a220b692f230598b8633d28705f6494775dff91821639d30

Version 2.6.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 3ef6574807e32d176805c978a5b5b706780ebe94
- SHA256 2789ec06e2ee6df7ca560dc27e0d4659225e7e85b5632a52836baabc89bdb944

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 dda6ef527638881fef3d2c875bdef645ad764c22
- SHA256 05240520ca74d77f02cd2a540a788cecd7c9e084ff98c02fb1c43f42a00e319b

Version 2.5.4

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 744322a9875789edc3817365a0e65df28b20e1e7
- SHA256 182852ad7bc64c5551341d351f0cf2d22a2dd5bc4f53a7dd78ff0dfcb2515133

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 b6c95a9fb705d54905ffc8a406a7bfb1bb131e32
- SHA256 8fb170402502dd743ce9d6657e71a15d25b6ca647464b92d1ce83f40488ac195

Version 2.5.3

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 e3046243e72f5cabae95cf63e287f376f629e629
- SHA256 e19b6b66bb18ded2e3a8e86bdac1514bf13f4d2aec88eae7366487ee8018cf2a

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 b53b4f46d90a5b804495270d1669c203cd56dc22
- SHA256 f7065e116fb2da88c0638d8ad9509e904aeeeeb8e6d608a2f8f7e56445ce8d3f

Version 2.5.2

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 1346d7e83193ecaecc818dc42e8fc2156a1d6bf2
- SHA256 29b394b0571dd53fbe5ddc6fe1068efc34fb227c08c182a2e9a80a044a55e04e

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 7993aa44672b32cb3e3f564bfb9b7e0803971991
- SHA256 c6c6d3c318f19dbac75e830ef8a1e3c9dfed4957bdf4aaf00e722911b51354b2

Version 2.5.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 18182facd4e1e07afb7085684bf9b2c2ce37aade
- SHA256 5a34df053be757b2f0f2a4a0475b1496c2dbaaacd28e7cd9597ee06c37e69dcc

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 506fc1e74e089420b8eb48cde1189817896db436
- SHA256 bf2547e4eb2202ac403f290ff3cae9db5efc359d95785b2e93ef5c3c73bcb504

Version 2.4.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 42ed43e0c01e8397d8adb9ec5e05b8176d865b2d
- SHA256 feeb76984963971b01c82cab4b39493a32848676e9aa20838cadbc00d5973516

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 ff0b7e445d62ec8b00ddd006cb220fbbd217a31b
- SHA256 add856e68ebcd9782a729a689ac99a654f4366102d733ee5d041c6049127eba5

Version 2.3.1

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 fbefd08eb6230455938d73fad36bffdeae587bf1
- SHA256 0b1eb3925bdb4b4707a2285bd2629012c5b526013e7ad37bd3c23fd387e10bad

Version 2.3.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 aedde832f7c34d79b31e88421d63e9496da4933a
- SHA256 63630fad8f528325cd2f0b5192164109a922432f4c30c937ea8b9ecc58098b82

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 f5f17217f4d209c6b7d3557ba8409da3affca6ec
- SHA256 e1dced949523e37491cd00e125d85b3da8609e3bb056b7616f448029e66b5468

Version 2.2.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 2ec4505043d7335802dc367fbc7d0a65f7637775
- SHA256 1bc9ebcf525d3a0c9714114915259b0d30b249e456eb286f85f4cff8f37091a8

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 f093d6be323c2e37b978819e2861137d012df713
- SHA256 9bc8cc637c768fcf97095edd982a28b8a2d83bb10f3fc8635b67dca10762a27c

Version 2.1.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 91c7a23bced911a1c3adda58d37a6b44a3630213
- SHA256 3494ab7f2c655371e83632142d423cdd4460abadd6938b75a39cae304d27898d

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 ebbaf553311f10406d5b90312256a2d464736615
- SHA256 b3a80893ddd8edcf7c6b297e186836d6fdc4712c9230f91948192fd96393cd69

Version 2.0.1

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1: fb2b89d80ed4dc5d0be6b7b50aec27d1c921d25d
- SHA256: f6c354bc4c809665b7149d6f64d1c73fc882773b31a916d39ba53be750416c64

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1: 02b364f3e3732ea9e0ff135427b8c9c0806bb952
- SHA256: 666f677c4ff3f4178af2b60c5681ecd7232c2f44b1900ea01753f73474ab5a73

Version 2.0.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 e82ee65d82f5285772fc8ba99d88da3f78e4da23
- SHA256 dd466d665a5b07426783a1cb65b3a116c4369a71434bf109021f6db099f433d8

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 6dd1554632cf9169b3037e3faa453d52c62095b4
- SHA256 b78f4fceb367f92a74345088ae2fda8512f55fcda77edbb4acc6d2c464be07a3

Version 1.9.6

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1– 1eafddb64e3adb59b0064c011b84415b42c13852
- SHA256 – 2c700193690249a4f19fea0a32e68125e5167437016a3d8eb0738a6fd9fa50c4

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 – 939bd5397823c257e37c76e203451bb35b4b5bf4
- SHA256 – 20898cc7e1cb8789cc8311e06d7c3d946962e4ea7ad445e3cd78f838a27efe96

Version 1.9.5

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 – ef4877367d6b7f85747a2f0f54b2830de5221aad
- SHA256 – 66fa4fa4e8818f405cbd6b36be2a89dc0965e112810e9db42b575b4722f02274

Version 1.9.2

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 – 91a5c9648d59bedbf13b0afe857eb9741dba335c
- SHA256 – 6a6925b848637292cf576d242db5af35259269d8abb87d89ecb576d46721ae2b

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 – e5a2dd007aaa764e568d5f4e9af603eb026b8c74
- SHA256 – fcd0c3e03607e8ee75a8e4127d74c6f68b29d42f83dfefd095367ec4356887e0

Version 1.8.0

Windows Installer Hashes for **Delinea.ConnectionManager.WindowsInstaller.msi**

- SHA1 – e4989e93fc2d1a3f5d0bc92a298b99be2cd0ce1e
- SHA256 – d5352367df30e254678026c6724a80bb2761b96c726b78b11ef61a556c59e44b

Mac Installer Hashes for **Delinea.ConnectionManager.MacOSInstaller.pkg**

- SHA1 – da39a3ee5e6b4b0d3255bfef95601890afd80709
- SHA256 – e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Version 1.7.1 Hashes

Windows Installer Hashes for **Thycotic.ConnectionManager.WindowsInstaller.msi**

- SHA1 – c0e269a41fc8ac974f445d6769ae28b9bd2008ff
- SHA256 – 22387c20a1620938a642906f2c103b43ea5c608975722d8a1f1a0db4d30d9cc5

Mac Installer Hashes for **Thycotic.ConnectionManager.MacOSInstaller.pkg**

- SHA1 – 4ede9f06111d11fc77900427e416b8f7a0cf0c25
- SHA256 – 088aa3c6ec903e04ced12871198a40d0dfc1a2028c7f8bcc21dc916786986ef2

Version 1.7.0 Hashes

Windows Installer Hashes for **Thycotic.ConnectionManager.WindowsInstaller.msi**

- SHA1 – 343c82d10b79abcff9302b7b1772f4caa8637047
- SHA256 – 3cf0ed060bc2b9d2639b779dd6e9c90c48adcd268646b9c3408726eac5bb1d05

Mac Installer Hashes for **Thycotic.ConnectionManager.MacOSInstaller.pkg**

- SHA1 – 9ae109074bffade9e2e3e0bca241db23457e0c50
- SHA256 – b04fa74e41f522c3f13913b05194026b17ef329ba470e0200318cabf84b4962b

System Requirements

Connection Manager is a desktop application that can be installed on either Windows or macOS operating systems.

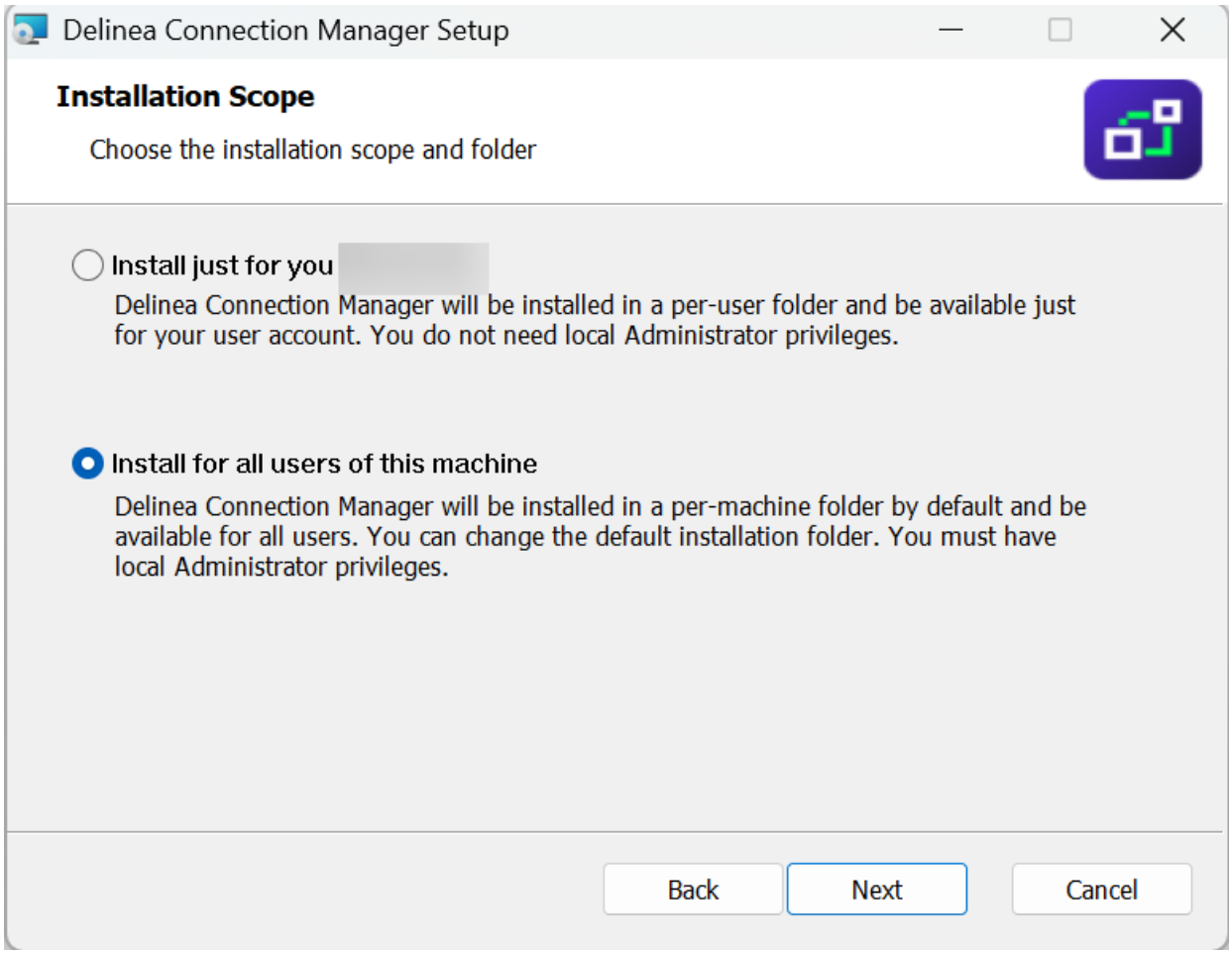
For Unicode characters, Connection Manager supports UTF-8 encoding. Minimum system requirements:

- Microsoft Windows: Windows 10 or later, Windows Server version 2016 or later; 8GB RAM.
- Apple macOS: 13 (Ventura), 14 (Sonoma), 15 (Sequoia), 26 (Tahoe); 8GB RAM.
  - Both Intel and Apple based systems are supported.
- Minimum requirements for connectivity to Secret Server vaults:
  - Secret Server Version: 10.7 or later
- Minimum upgrade version: 1.9.2 or newer is required to upgrade to version 2.8

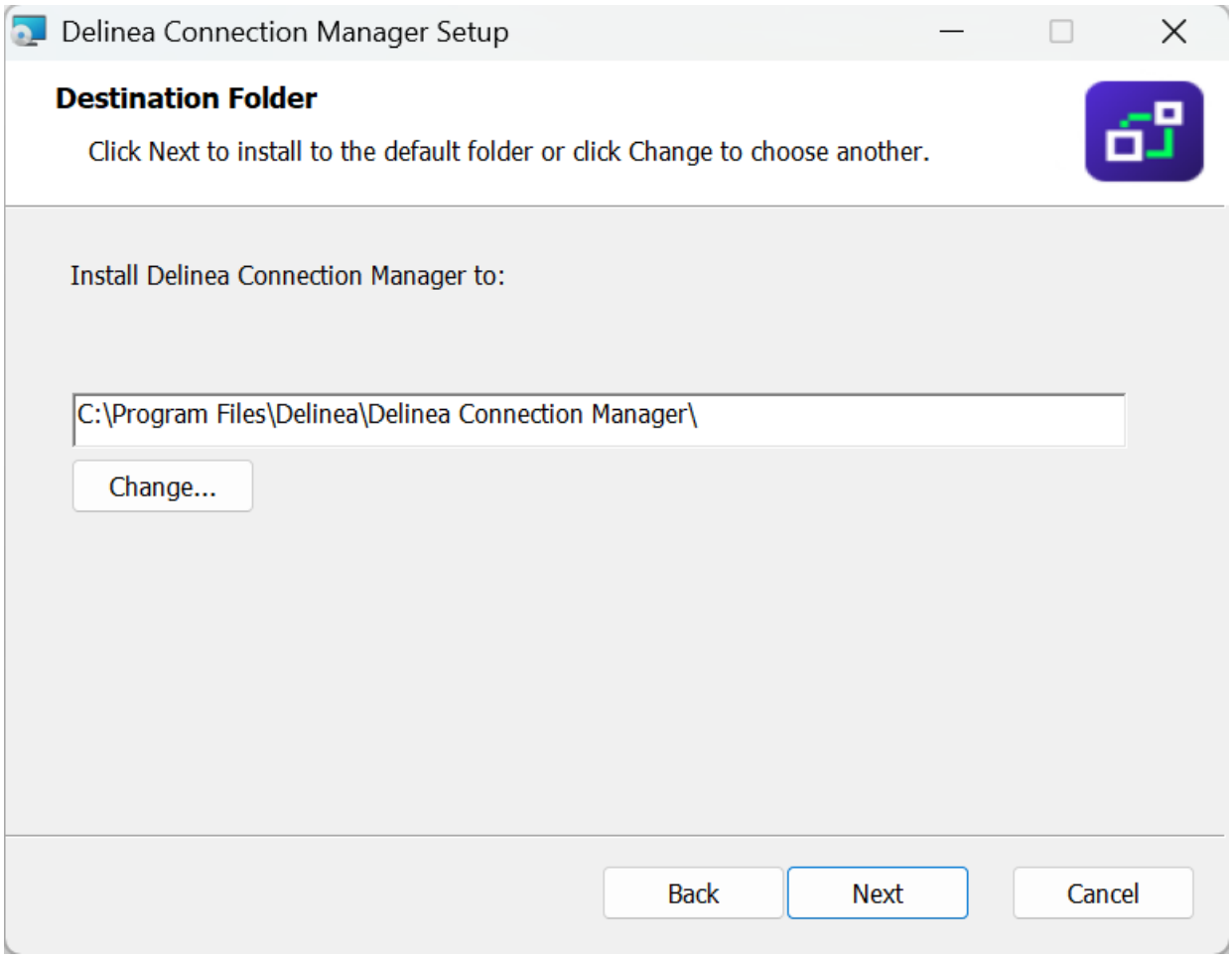
Installing on Windows

Installing Connection Manager for All Users on a Machine

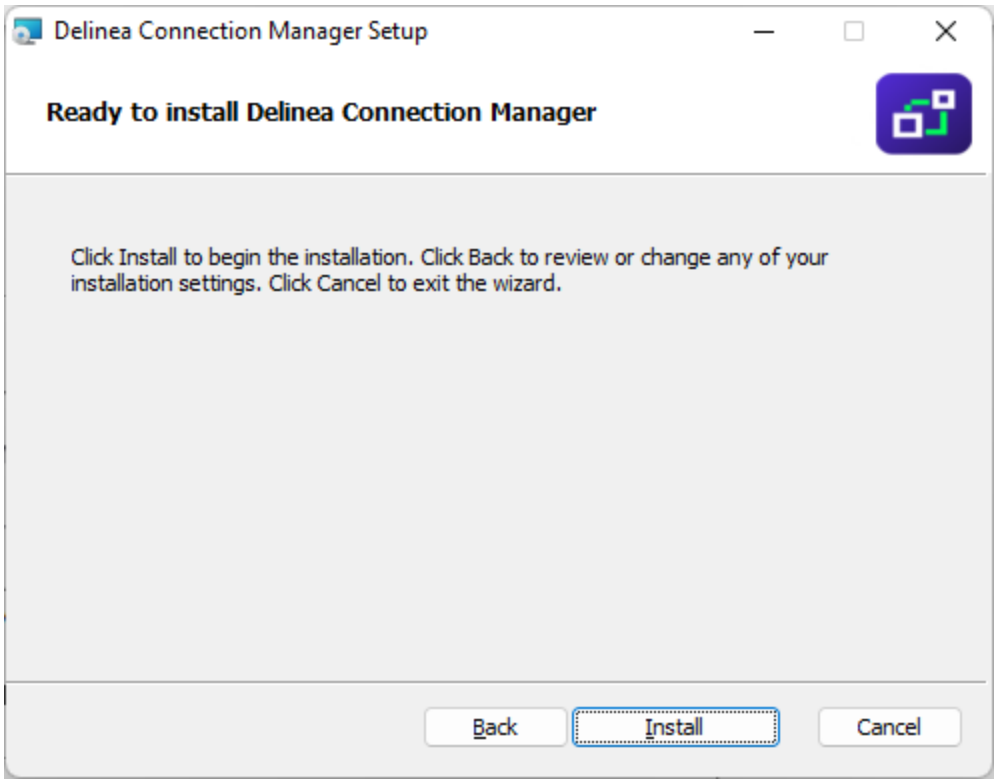
1. Download the Windows Installer File (MSI) for Connection Manager.
2. Double-click the MSI file to start the install process.
3. Click **Next** to continue.
4. Click **Install for all users of this machine**.



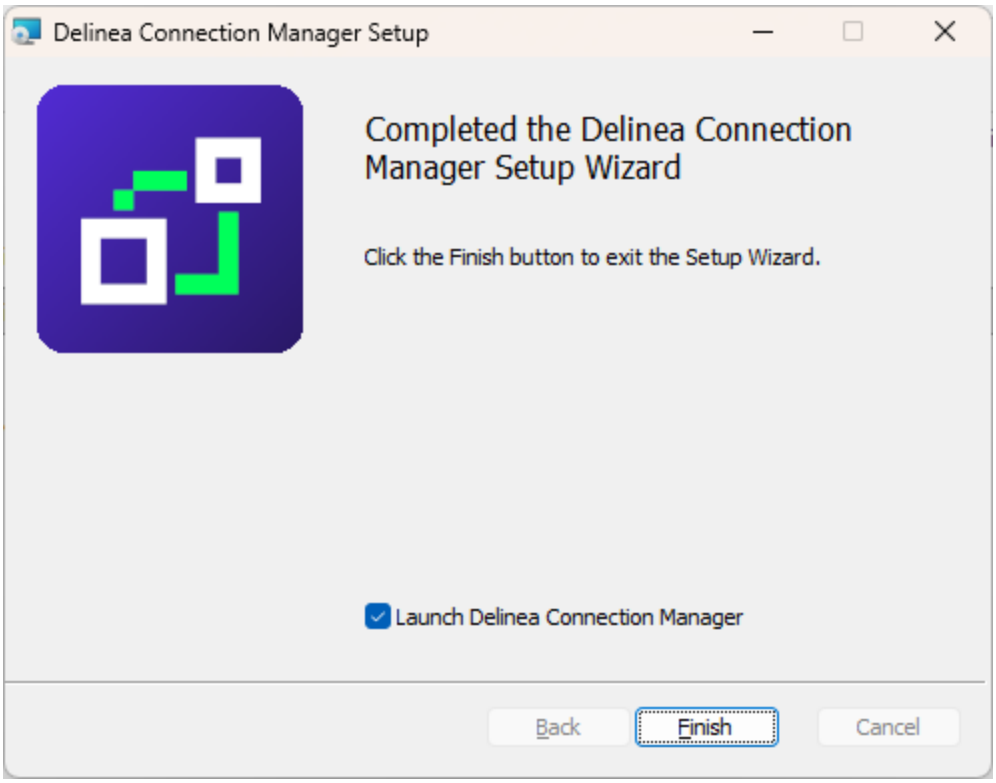
5. The default installation path will already be filled in, but you can change it to another location.



6. Click **Next** to confirm the location and accessibility for the install.



7. Click **Install** to start the installation. A progress bar will be displayed while the installation is in progress.
8. If you would like to launch Connection Manager when the installation is complete, make sure the Launch Delinea Connection Manager box is checked before clicking **Finish**.

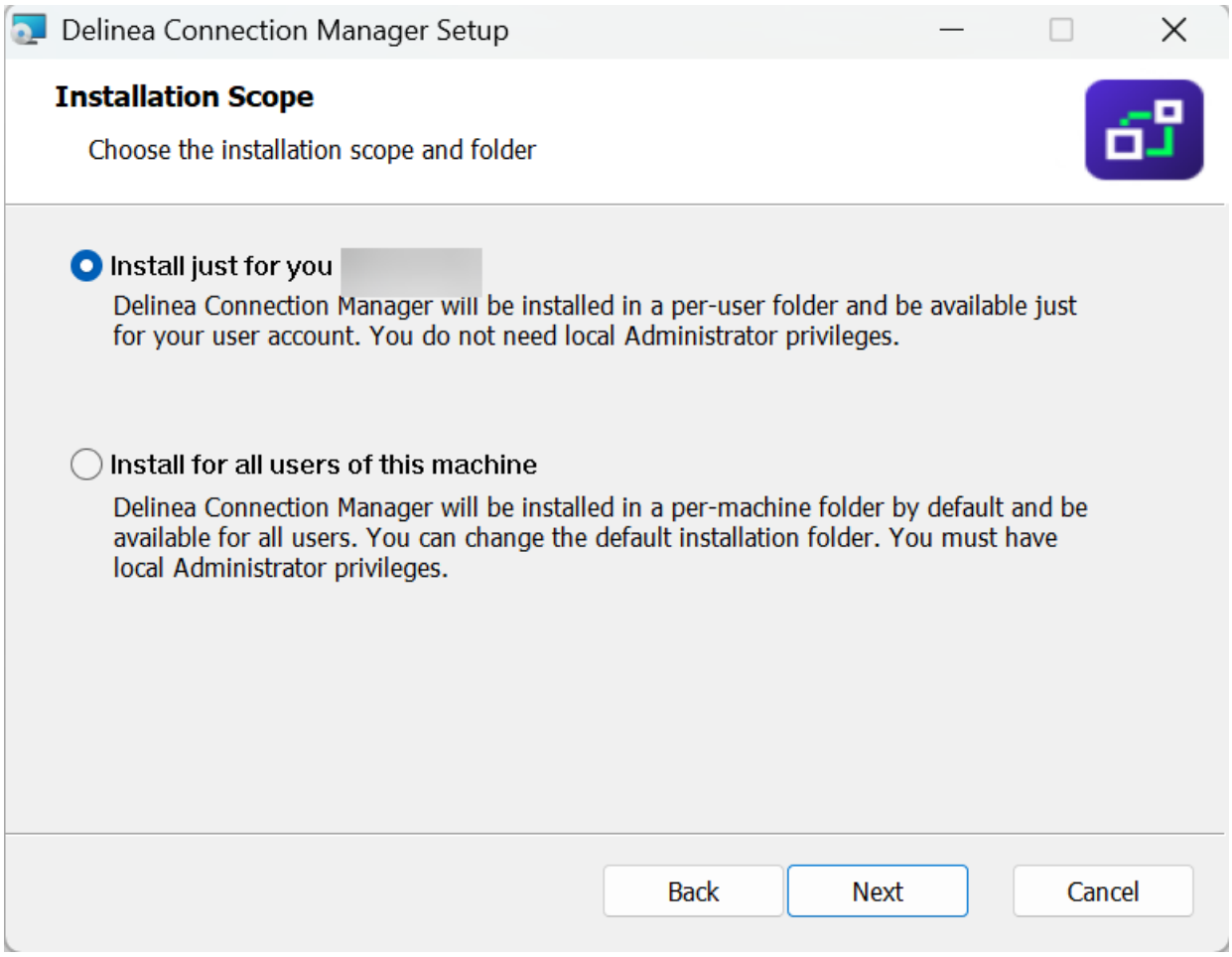


The install is complete, and the Connection Manager icon will be added to the desktop for easy access.

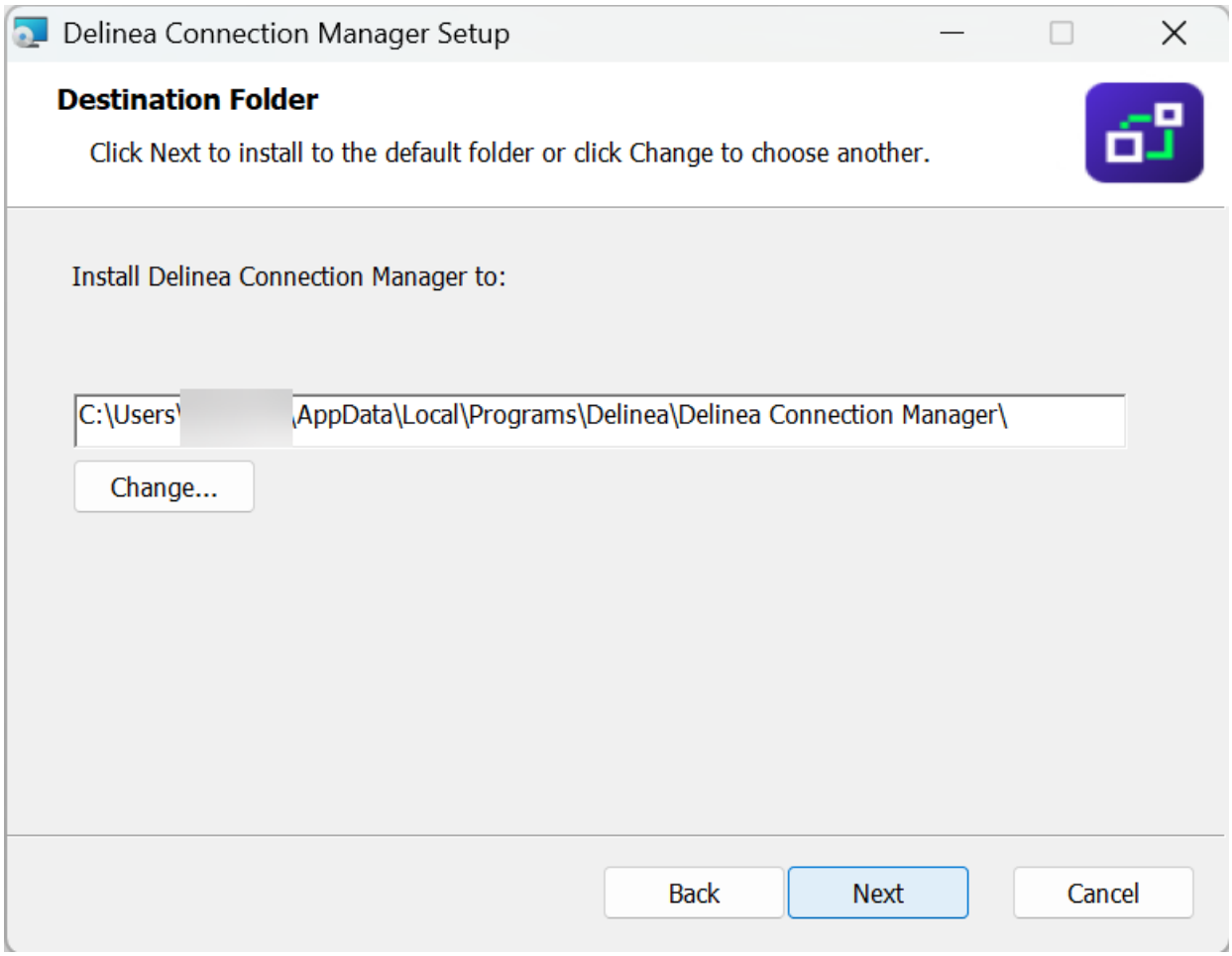
Note: If an existing administrator installation is detected, the setup will proceed with the administrator installation by default. To access the user installation option, you must first completely uninstall Connection Manager and then perform a fresh installation.

Installing Connection Manager Per User

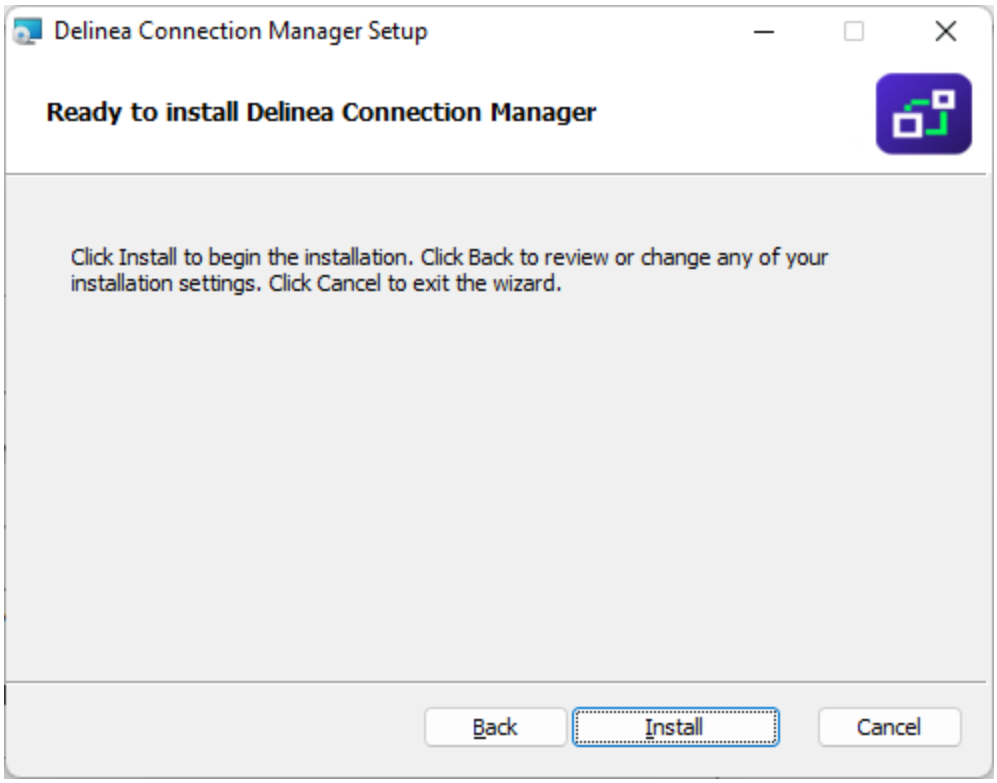
1. Download the MSI Windows Installer File (MSI) for Connection Manager.
2. Double-click the MSI file to start the install process.
3. Click **Next** to continue.
4. Click **Install for all users of this machine**.



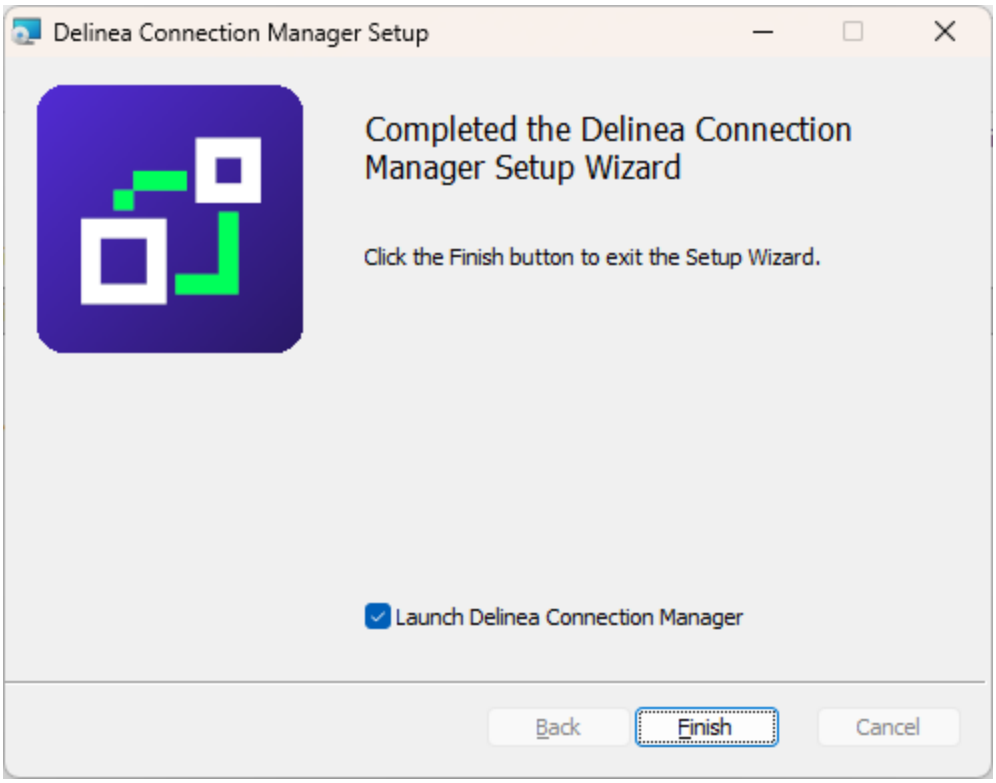
5. The default installation path will already be filled in, but you can change it to another location.



6. Click **Next** to confirm the location and accessibility for the install.

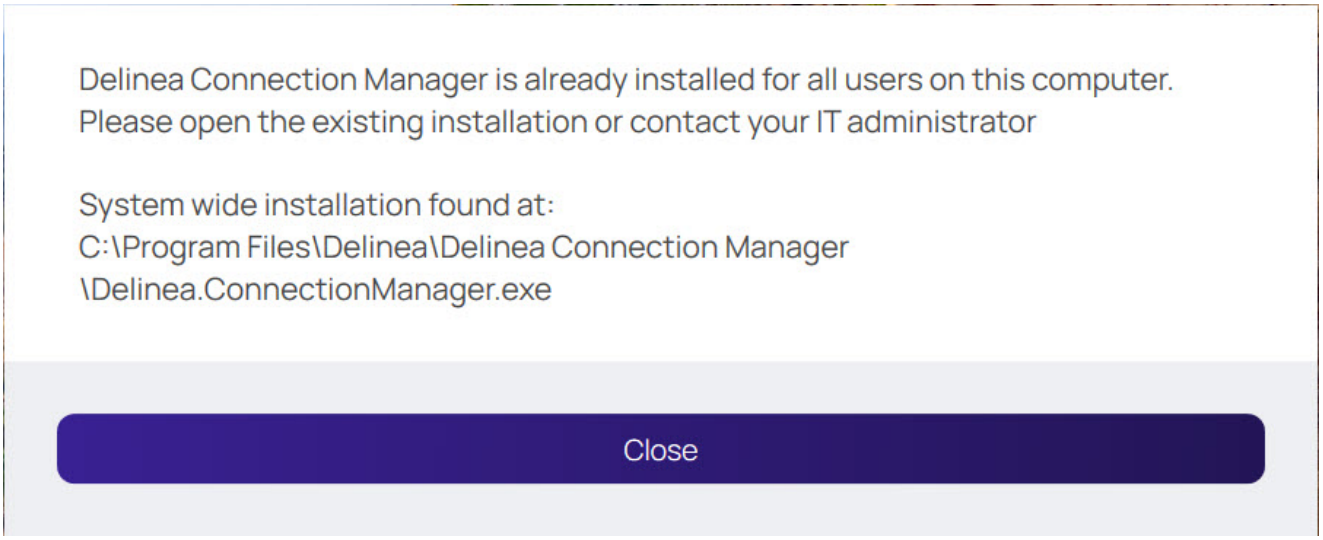


7. Click **Install** to start the installation. A progress bar will be displayed while the installation is in progress.
8. If you would like to launch Connection Manager when the installation is complete, make sure the Launch DelineaConnection Manager box is checked before clicking **Finish**.



The install is complete, and the Connection Manager icon will be added to the desktop for easy access.

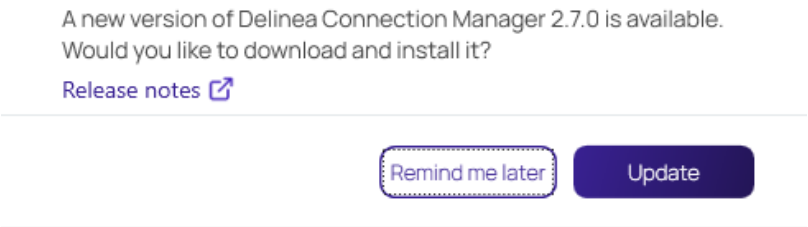
Note: Per user installation is only possible if Connection Manager was not previously installed for all users of a machine. Otherwise, you will see the following error:



Important: If you previously installed Connection Manager per user, but later on an administrator installed Connection Manager for all users of a machine, the per machine installation overrides the per user installation. You will have two instances of Connection Manager installed, but you will no longer be able to access the one installed per user.

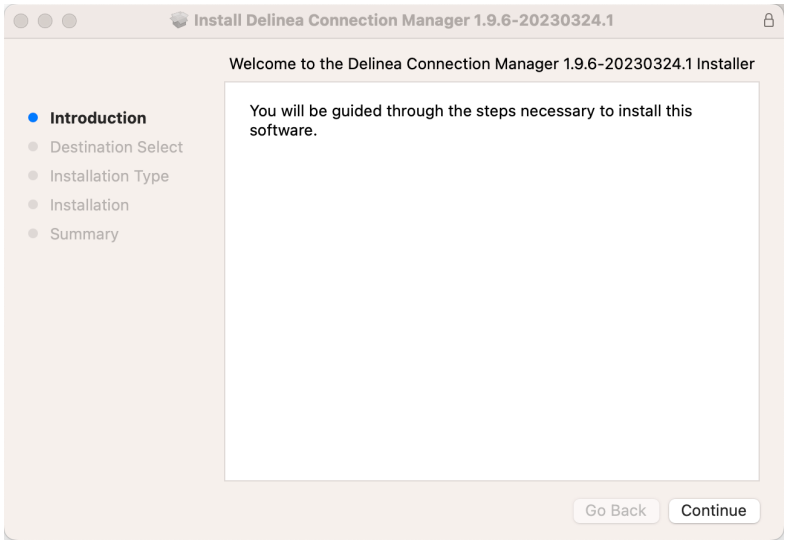
Updates

When the Connection Manager application is launched, users are prompted with an update message if a new release is available. If you would like to update, click **Update** or choose **Remind me later**. Starting with the 2.7 release, the update window will also contain a link to the release notes of the latest version. Once the update is complete, Connection Manager will launch automatically.



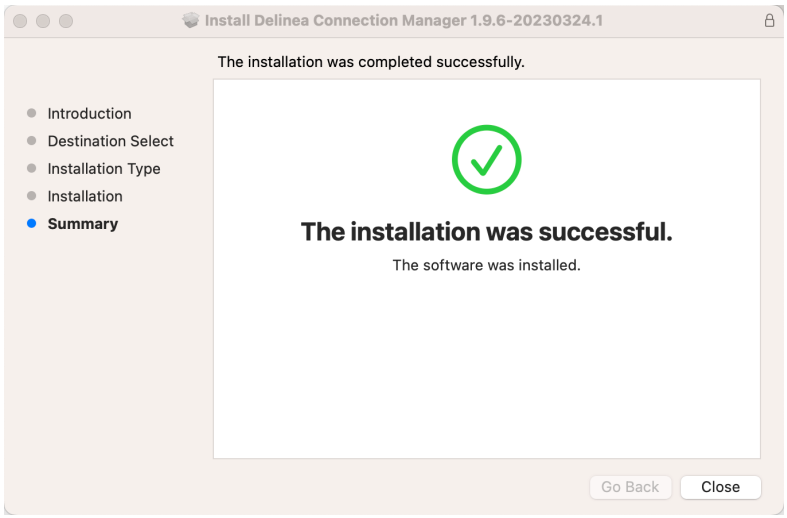
Installing on MacOS

1. Download the PKG file .
2. A PKG file will download to your system.
3. Navigate to the DMG file and double-click to open, or right-click and select **Open**. The install window opens.
4. Click, drag, and drop the Delinea Connection Manager logo to the Applications folder. The installation begins.



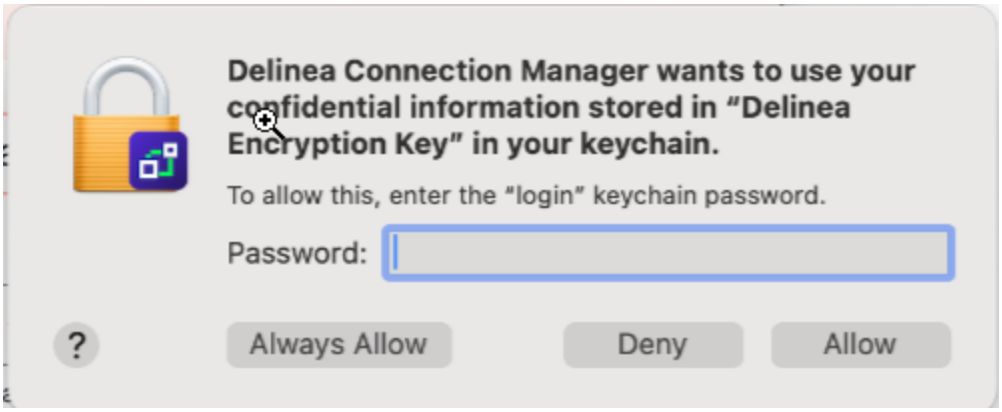
5. Once Connection Manager has been added, close the installer window.

   Note: If you receive the following message on your install, click **Open**.



Delinea Encryption Key

Prior to launching Connection Manager version 2.5.3 or later for the first time, you will be asked to input your computer password to allow Connection Manager to use the confidential information stored in the Delinea Encryption Key in your Keychain. To prevent this message from appearing again, click **Always Allow**.



Command Line Arguments

The following command line arguments are supported by Connection Manager during installation only. They should not be used after installation to start the Connection Manager.

Note: Application settings were moved to the Registry in the 2.8 release. The command line arguments below apply to installation only. To view or change application settings after installation, see "Application Configuration via Windows Registry Editor" on page 163. If you are using an older version of Connection Manager, refer to the "Application Configuration File" on page 176.

- `-disablelocalvault`
- `-logo`
- `-logocollapsed`
- `-ssauth`

  Note: The `-ssauth` option supports two values: `local, external .`
- `-ssname`
- `-ssurl`
- `-ssautoclosebrowserlogin`
- `-reauthenticate`

  Note: The `-reauthenticate` option supports the following two values: `y` and `n`
- `-preferredAuth`
- `-screenshotsQueueLimit`
- `-updateOnStartup`

Note: You must use double quotes inside the KEYS parameter because the value of the KEYS parameter is quoted itself.

Important: `/quiet` mode installation works only with Administrative privileges. If a user without administrator privileges runs the MSI with `/quiet` mode, nothing happens. If you would like to install the latest version of Connection Manager via quiet mode installation, you must first remove the previous version before installing the new one.

Note: When installing Connection Manager via command line options to set the Secret Server URL, these options will only be applied to the first user who logs in to Connection Manager. If you would like to make them the default options, you can use the following workarounds:

1. Prior to their initial log in, new users need to run Connection Manager via command line with `args -ssurl "your ss url" -ssname "your ss name" -ssauth "your auth type"`
2. Prior to their initial login, each user admin should create a file in path `C:\ProgramData\Delinea\Connection Manager\repository.dat` with the following content:

```
[
{     "$type":"Delinea.ConnectionManager.Common.Models.SecretServerRepository,
Delinea.ConnectionManager.Common",
    "Url":"Your SS url",
    "PlatformUrl":null,
    "UserName":null,
```

```
    "Password":null,
    "Domain":null,
    "AuthType":"Local",
    "TwoFactorAuthType":"None",
    "PinCode":null,
    "StoreCredentialsInLocalStorage":false,
    "SecretTempletes":null,
    "LoadAllTemplates":true,
    "Token":null,
    "PlatformToken":null,
    "ConnectionManagerSettings":null,
    "Id":null,
    "Name":"your SS name",
    "Type":"SecretServer",
    "IsAutoload":false
}
]
```

Note: If your command line parameter includes any spaces or parentheses, be sure to place quotation marks around the MSI file. An example is below.

For example: `"C:\Users\MyUser\Downloads\Connection Manager\Delinea.ConnectionManager.2.5.0.WindowsInstaller.msi" /quiet RUNCM=runCM`

Per User Installation via Quiet Mode

When installing Connection Manager for yourself only, you will need to add the following parameter: `USERMODE=1`:

Example:

```
"C:\Users\MyUser\Downloads\Connection
Manager\Delinea.ConnectionManager.2.8.0.WindowsInstaller.msi" /quiet RUNCM=runCM
USERMODE=1
```

The following command line arguments are not supported for per user installation via quiet mode:

- ssurl
- ssname
- ssauth
- ssautoclosebrowserlogin

Changing the Location of the .DAT File

The default location of the `.dat` file is: `C:User/[UserName]/AppData/Roaming/Delinea/ConnectionManager`

You can change the location of the `.dat` file upon installation by running the following command:

Example for Windows:

```
Delinea.ConnectionManager.2.8.0.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-lsPath
""C:\Users\Username\AppData\Roaming\New Delinea\Connection Manager""
```

Changing the Installation Path

Users can change the Connection Manager installation path by inserting the `INSTALLFOLDER` variable on Windows and `CustomInstallationPath` on MacOS during installation as shown in the examples below:

Example for Windows

```
Delinea.ConnectionManager.2.6.0.WindowsInstaller.msi /quiet RUNCM=runCM
INSTALLFOLDER="C:\work"
```

Example for MacOS:

```
sudo defaults write /Library/Preferences/com.Delinea.ConnectionManager
CustomInstallationPath "/Applications/Delinea12" && sudo installer -pkg D2.7.0-path.pkg -
target /
```

Pre-Configuring Vault Connections on Install

Administrators can pre-configure Delinea vault connections so that users do not have to create connections themselves when opening Connection Manager for the first time. These connections can be pre-configured in the .DAT file:

```
[
  {
    "$type": "Delinea.ConnectionManager.Common.Models.SecretServerRepository,
Delinea.ConnectionManager.Common",
    "Url": "https://yourfirstvaulturl.com",
    "PlatformUrl": null,
    "UserName": null,
    "Password": null,
    "Domain": null,
    "AuthType": "Local",
    "TwoFactorAuthType": "None",
    "PinCode": null,
    "StoreCredentialsInLocalStorage": false,
    "SecretTempletes": null,
    "LoadAllTemplates": true,
    "Token": null,
    "PlatformToken": null,
    "ConnectionManagerSettings": null,
    "Id": null,
    "Name": "First Vault",
    "Type": "SecretServer",
    "IsAutoload": false
  },
  {
```

```
    "$type": "Delinea.ConnectionManager.Common.Models.SecretServerRepository,
Delinea.ConnectionManager.Common",
    "Url": "https://yoursecondvaulturl.com",
    "PlatformUrl": null,
    "UserName": null,
    "Password": null,
    "Domain": null,
    "AuthType": "Local",
    "TwoFactorAuthType": "None",
    "PinCode": null,
    "StoreCredentialsInLocalStorage": false,
    "SecretTempletes": null,
    "LoadAllTemplates": true,
    "Token": null,
    "PlatformToken": null,
    "ConnectionManagerSettings": null,
    "Id": null,
    "Name": "Second Vault",
    "Type": "SecretServer",
    "IsAutoload": false
  }
]
```

Disabling Local Vault on Installation

Use this argument to disable the local vault on installation:

`-disablelocalvault`

Example for Windows

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-disablelocalvault
"
```

Example for MacOS

```
sudo installer -pkg ~/Downloads/DelineaConnectionManager.pkg -target / && open
/Applications/Delinea/Delinea\ Connection\ Manager.app --args -disablelocalvault
```

Enabling/Disabling Auto Reauthenticate

This feature provides the option to configure vault reauthentication behavior in Connection Manager. Users may keep the existing behavior that automatically restarts the authentication flow or force a fresh login when their vault session/refresh tokens have expired--mimicking the existing web API behavior.

The default value is **-reauthenticate y**. If the value is set to **-reauthenticate n**, the behavior will be more similar to the web API which forces a fresh login. The **-reauthenticate n** option is beneficial for users who use SAML configuration through an external identity provider with a longer session/refresh length and enables audit logs to correctly generate upon logout.

Use this argument to disable auto reauthenticate on installation:

`-reauthenticate n`

Example

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-ssurl
""https://secretserver.example.com/ss"" -ss-name ""new server"" -reauthenticate n"
```

SSH Authentication Method Setup on the Target Host

For more information on this command line, see "Troubleshooting SSH Connections" on page 213.

Example:

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-preferredAuth
""keyboard-interactive,publickey,password"""
```

Setting the Screenshot Queue Limit

For more information on setting the screenshot queue limit see "Session Recording" on page 139.

Example:

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-
screenshotsQueueLimit 60"
```

Disabling Update Check on Startup

To disable automatic checking for updates on startup, set the value to `n` as shown below:

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-updateOnStartup
n"
```

Specifying Custom Logo Images to Copy to the Proper Location

The paths to the custom logo files, on Windows, are as follows:

- C:\ProgramData\Delinea\Connection Manager\Resources\logo.png
- C:\ProgramData\Delinea\Connection Manager\Resources\logo_collapsed.png

Use these arguments to specify custom logo images to be copied to the proper location:

`-logo`, `-logocollapsed`

Example for Windows

```
Delinea.ConnectionManager.WindowsInstaller.msi
/quiet /l*v install.log RUNCM=runCM KEYS="-logo ""C:\Users\{username}\Downloads\logo.png""
-logocollapsed ""C:\Users\{username}\Downloads\logo_collapsed.png""
```

Example for MacOS

```
sudo installer -pkg ~/Downloads/Delinea2.7.0-RC7.pkg -target / && open
/Applications/Delinea/Delinea\ Connection\ Manager.app --args -logo "/Users/
[username]/Downloads/logo.png" -logocollapsed "/Users/[username]/Downloads/logo_
collapsed.png
```

Example Powershell Command Line

```
.\Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS='"-logo
""/Library/Application Support/Delinea2/Connection Manager/Resources2/logo.png"" -
logocollapsed ""/Library/Application Support/Delinea2/Connection Manager/Resources2/logo_
collapsed.png"""'
```

The path to the custom logo files, on a Mac, is as follows:

- Users/Shared/Application Support/Delinea/Connection Manager/Resources

Two files are necessary to use custom logos:

- Logo.png - 50 x 250 pixels
- Logo_collapsed.png - 50 x 100 pixels

Delinea Platform Connection

Example for Windows

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-ssurl
""https://mycompany.delinea.app"" -ssname ""MyCompany Platform"" -ssauth web"
```

Pre-Creating a Secret Server Connection

Use these arguments to pre-create a Secret Server local or web connection on installation:

```
-ssurl, -ssname, -ssauth
```

Customizing External Browser Authentication

Users can customize external browser authentication by running a script containing the argument `%url%`, which represents login URL. Any parameters recognized by the browser at startup can be used. These settings only need to be applied once and will be saved by Connection Manager. Both admins and users can apply these settings, but admin settings will override user settings. Examples of possible customization scripts are listed below:

Note: Certain complex scripts that use JavaScript may not work correctly since the browser may truncate the URL. If you are experiencing this issue, consider replacing the `%url%` value with `%eurl%` (escaped URL) where only certain cymbols are escaped.

Note: Using the ampersand (&) in command lines is not allowed.

Selecting a browser to launch the authentication flow

Run the following command:

```
{Browser Name} "%url%"
```

This will set the default browser used for authentication. You can change this by inputting one of the following supported browsers:

- chrome
- msedge
- firefox
- explorer (This option launches the authentication flow via your default browser)

Example for Chrome:

```
chrome "%url%"
```

Note: If this setting is not applied, Connection Manager will use the default browser for the authentication flow.

Opening the Browser in a New Window

Example for Chrome:

```
chrome --new-window "%url%"
```

Launching a Browser in Incognito Mode

Example for Chrome:

```
chrome --incognito "%url%"
```

Example for Edge:

```
msedge -inprivate "%url%"
```

Opening a Browser in Limited Mode

Example for Chrome:

```
chrome --app=%url%
```

Setting Custom Window Size and Position

Example for Chrome:

```
chrome --user-data-dir="C:\Temp\ChromeProfile1" --window-position=200,200 --window-
size=200,200 --app=%url%
```

External Browser Connection

Example for Windows

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-ssurl
""https://secretserver.example.com/ss"" -ss-name ""new server"" -ssauth external"
```

Example for MacOS

```
sudo installer -pkg ~/Downloads/DelineaConnectionManager.pkg -target / && open
/Applications/Delinea/Delinea\ Connection\ Manager.app --args -ssurl
"https://secretserver.example.com/ss " -ssname "new" -ssauth "external"
```

Example Powershell Command Line

```
.\Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS='"-ssurl
https://secretserver.example.com/ss -ssname ""new server"" -ssauth external"'
```

Local Connection

Example for Windows

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-ssurl
""https://secretserver.example.com/ss"" -ss-name ""new server"" -ssauth local"'
```

Example for MacOS

```
sudo installer -pkg ~/Downloads/DelineaConnectionManager.pkg -target / && open
/Applications/Delinea/Delinea\ Connection\ Manager.app --args -ssurl
"https://secretserver.example.com/ss " -ssname "new" -ssauth "local"
```

Example Powershell Command Line

```
.\Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS='"-ssurl
https://secretserver.example.com/ss -ssname ""new server"" -ssauth local"'
```

Internal Browser Connection

Note: Internal browser authentication was deprecated as of the 2.8 release. Use these command lines for versions 2.7 and older.

Example for Windows

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-ssurl
""https://secretserver.example.com/ss"" -ss-name ""new server"" -ssauth web"
```

Example for MacOS

```
sudo installer -pkg ~/Downloads/DelineaConnectionManager.pkg -target / && open
/Applications/Delinea/Delinea\ Connection\ Manager.app --args -ssurl
"https://secretserver.example.com/ss " -ssname "new" -ssauth "web"
```

Example Powershell Command Line

```
.\Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS='"-ssurl
https://secretserver.example.com/ss -ssname ""new server"" -ssauth web"'
```

Disabling Local Vault

Example Powershell Command Line

```
`.\Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS='"-
disablelocalvault"'
```

Example for MacOS

```
sudo installer -pkg ~/Downloads/DelineaConnectionManager.pkg -target / && open
/Applications/Delinea/Delinea\ Connection\ Manager.app --args -disablelocalvault
```

Disabling Local Vault via Admin Enforcement

Starting with the 2.6 release, administrators have the ability centrally to disable users' local vaults after installation. Below you will find links to instructions on how to disable the local vault, for all users, on both Windows and MacOS:

- "Disabling Local Vault via Admin Enforcement on Windows " below
- "Disabling Local Vault via Admin Enforcement on MacOS" on page 29

Disabling Local Vault via Admin Enforcement on Windows

Disabling on Installation

If you are installing Connection Manager for the first time or local vault was previously disabled, follow the instructions below:

1. Install Connection Manager version 2.6 or newer via quiet mode.

```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-
disablelocalvault "
```

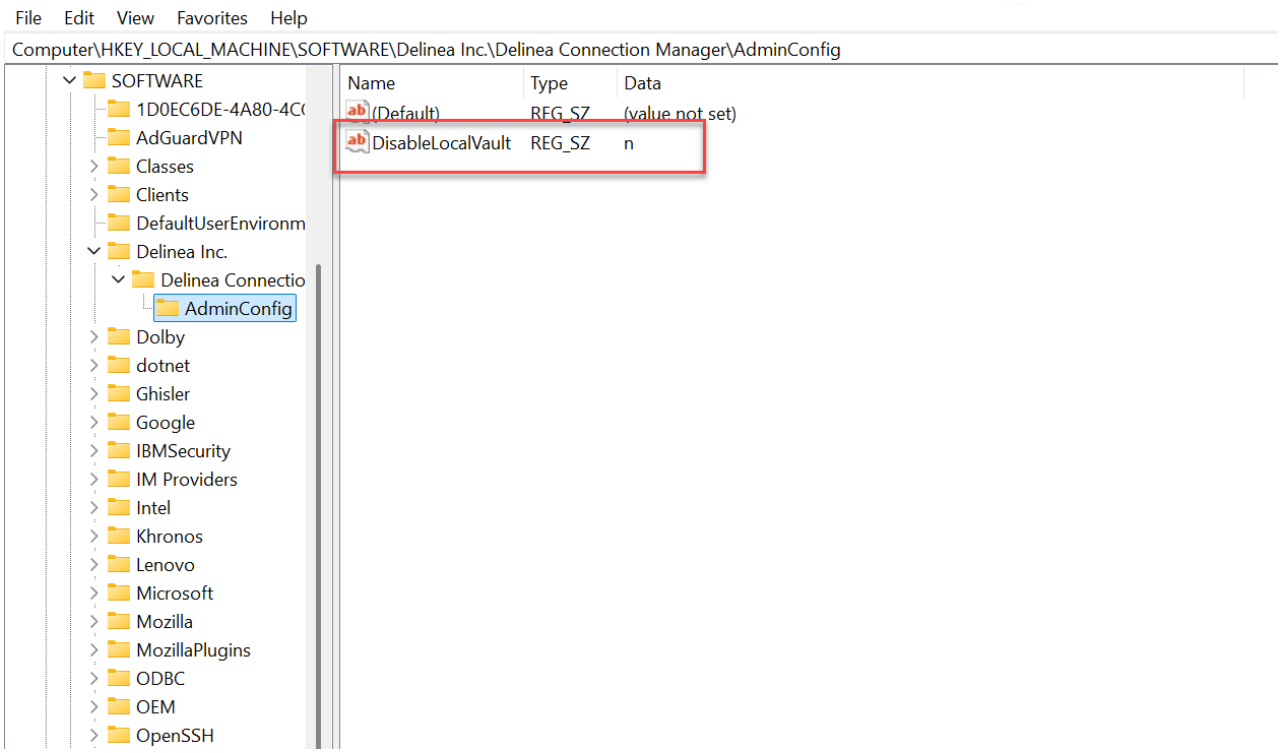
2. Open the Connection Manager registry, which can be found via the following path:

   `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Delinea Inc.\Delinea Connection Manager`

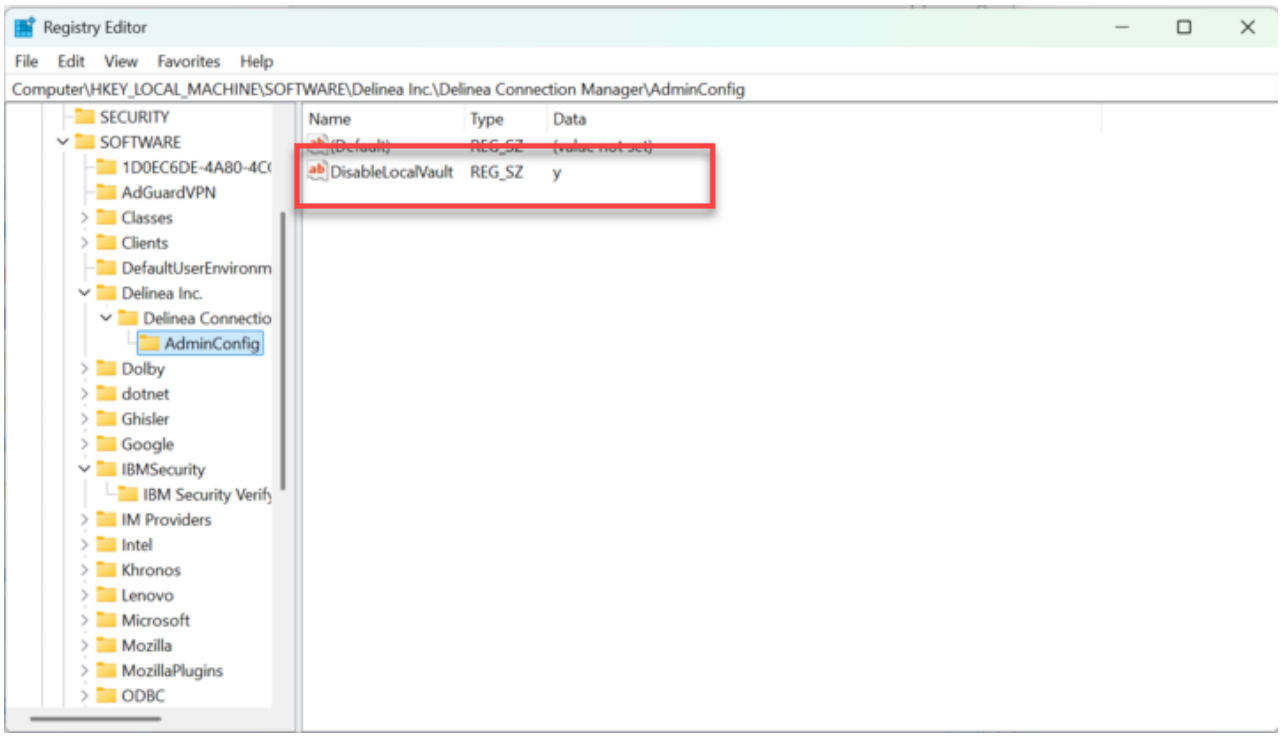
3. Open the AdminConfig folder inside the Delinea Connection Manager folder.

4. **Note:** If you do not have an AdminConfig folder you will need to add the Registry Key and create a string in the Registry Key called `DisableLocalVault`.

5. Inside the AdminConfig folder, you will see a **DisableLocalVault** setting. By default, this setting is set to `n`, meaning that local vault is enabled for local users.



6. Change this value to `y` to disable local vault for all users.



Important: If users already had existing local vaults created, they will be able to continue using them after this setting is applied.

Backing Up and Disabling Existing Local Vaults

If users already had an existing local vault created, administrators can disable these local vaults, before or after installation, by following these steps:

1. Open the Connection Manager registry, which can be found via the following path:
   `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Delinea Inc.\Delinea Connection Manager\AdminConfig`
2. Change the **DisableLocalVault** value to `fy`
3. When users launch Connection Manager, they will need to enter the password to the local vault and they will see a message that their local vault was disabled by administrator.

The local vault option in the left side navigation will be disabled for all users and a backup for the .dat file will be automatically created. This setting will take effect when Connection Manager is relaunched.

Re-Enabling Local Vault After Disabling

Administrators can centrally re-enable local vaults by following the steps below:

1. Change the value in the Registry to `n` or delete this value altogether.
2. In the *Main Menu* left-side navigation click **Enable Local Vault**.
3. Delete the current `ConnectionManager.dat` file.
4. Rename the backup file `ConnectionManager.dat.bak` to `ConnectionManager.dat`.

Disabling Local Vault via Admin Enforcement on MacOS

Disabling on Installation

If you are installing Connection Manager for the first time or local vaults were previously disabled, install Connection Manager version 2.6 or newer via quiet mode using the following command:

```
sudo installer -pkg Delinea.ConnectionManager.2.6.0.MacOSInstaller.pkg -target / && sudo
defaults write /Library/Preferences/com.Delinea.ConnectionManager.plist disablelocalvault
y
```

Note: The following file will be created during installation and can later be used to adjust administrator settings.

`/Library/Preferences/com.Delinea.ConnectionManager.plist`

Important: This file can be edited only by administrators and is read-only for regular users.

Backing Up and Disabling Existing Local Vaults

If users already had an existing local vault created, administrators can disable these local vaults, before or after installation by running the following command:

```
sudo defaults write /Library/Preferences/com.Delinea.ConnectionManager.plist
disablelocalvault fy
```

After users launch Connection Manager, they will see a message that their local vault has been disabled by an administrator.

Re-Enabling Local Vault After Disabling

Administrators can centrally re-enable user access to local vault by running the following command:

```
sudo defaults remove /Library/Preferences/com.Delinea.ConnectionManager.plist
disablelocalvault
```

Getting Started

Connection Manager creates a local encrypted file storage for saving local connections and Secure Server(s) connectivity information.

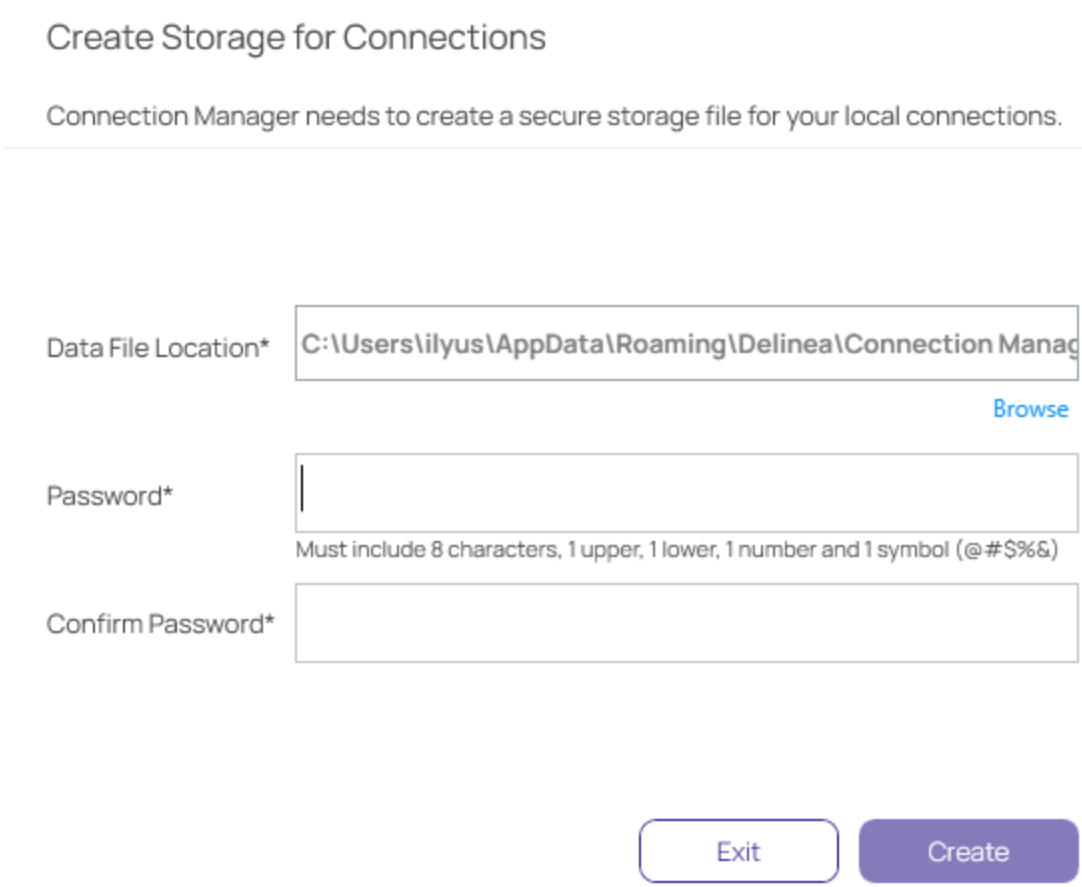
- "Secret Server Requirements " on page 56
- Create a Password
- Sign in
- User Interface Components

Creating a Password

When Connection Manager is launched for the first time, or if no file storage is detected, you must create a secure password for this vault.

Important: If this password is lost, the saved connections are not recoverable and will have to be re-entered.

1. Enter the **local password** and start the application. The following window opens.

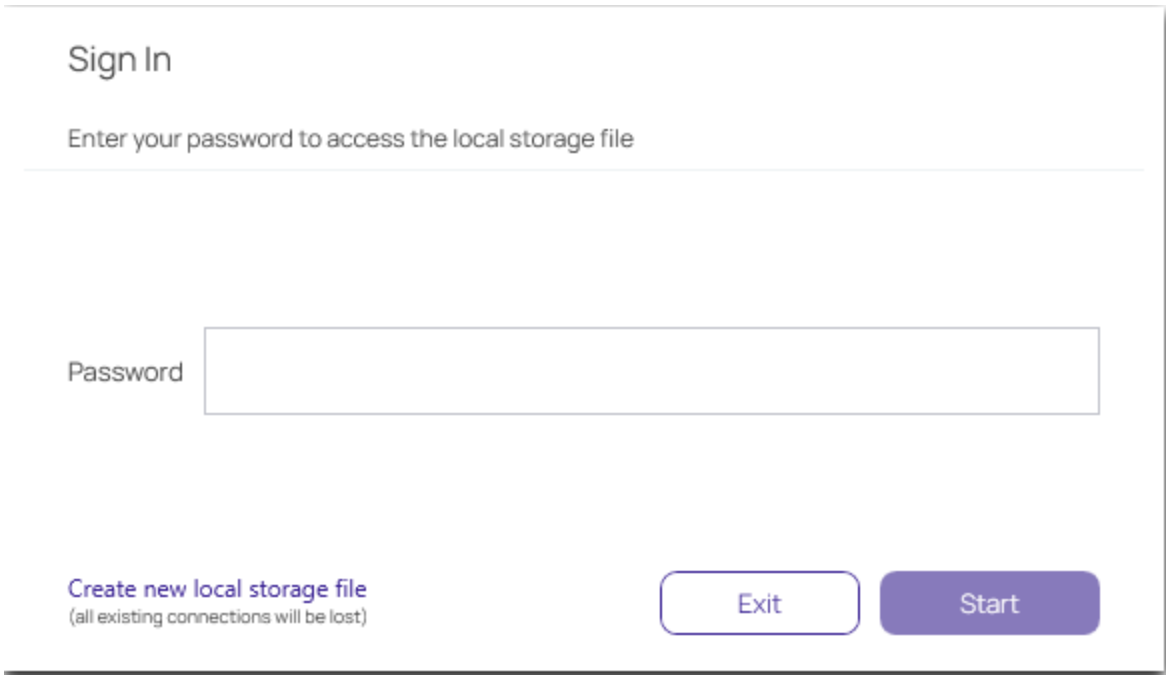


2. Enter the **password** to start the application.
3. Confirm the password and click **Create**.

> **Note:** If a local storage file exists but a user wishes to create a new one, click **Create new local storage file link** at the bottom left of the window. This will overwrite any existing storage file and any data stored there.

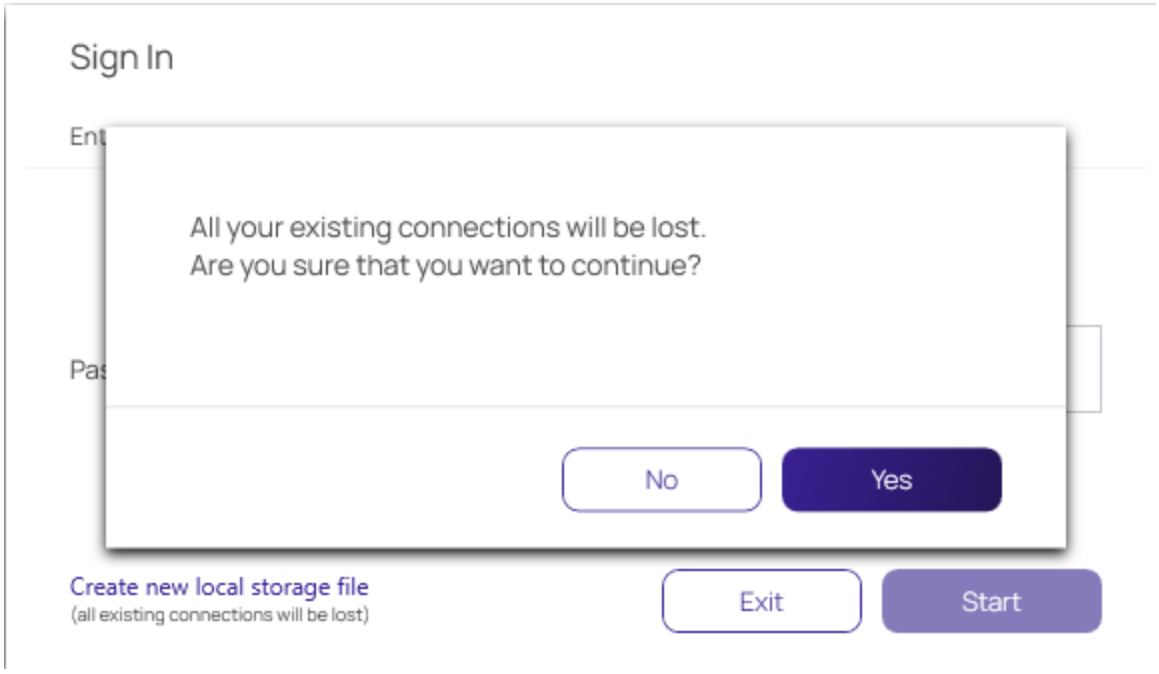
Signing into Connection Manager

When opening Connection Manager locally on your system, you are presented with a Sign-in modal.



1. Enter the password you previously created.
2. Click **Start**.

You can choose to **Create new local storage file**, however that will remove all existing connections for your system.



User Interface Components

Users of Secret Server's modern interface will find Connection Manager's interface and functionality to be similar in look and feel. The interface takes advantage of some client-side functionality such as right-click menus, double-click menus, and others.

Display Themes

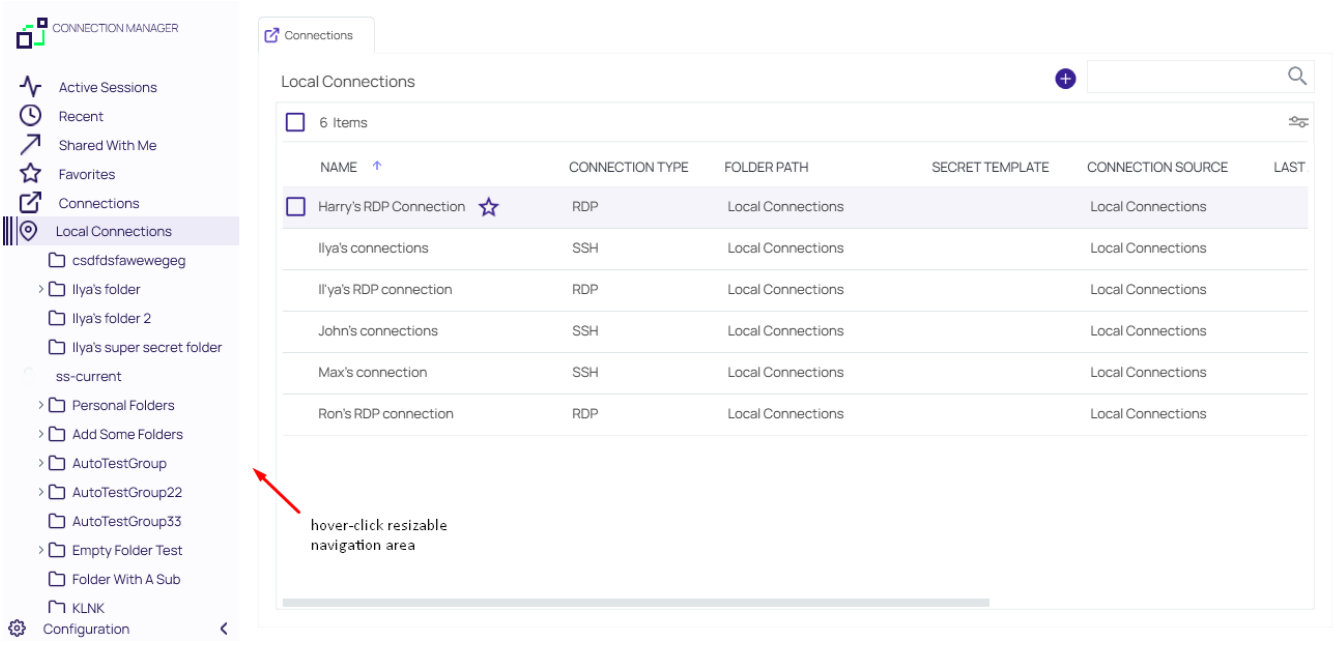
Connection Manager supports both light and dark mode. The application automatically follows your system appearance settings, so to switch themes, simply adjust the display or appearance settings on your MacOS or Windows device.

Main Screen

The main screen consists of two components:

- the navigation tree (which may be minimized) on the left and
- the tabbed work area to the right.

The two sections work in concert with each other.



The navigation area is hover-click resizable.

Menus

There are several menu types available within the user interface:

Stack Menu

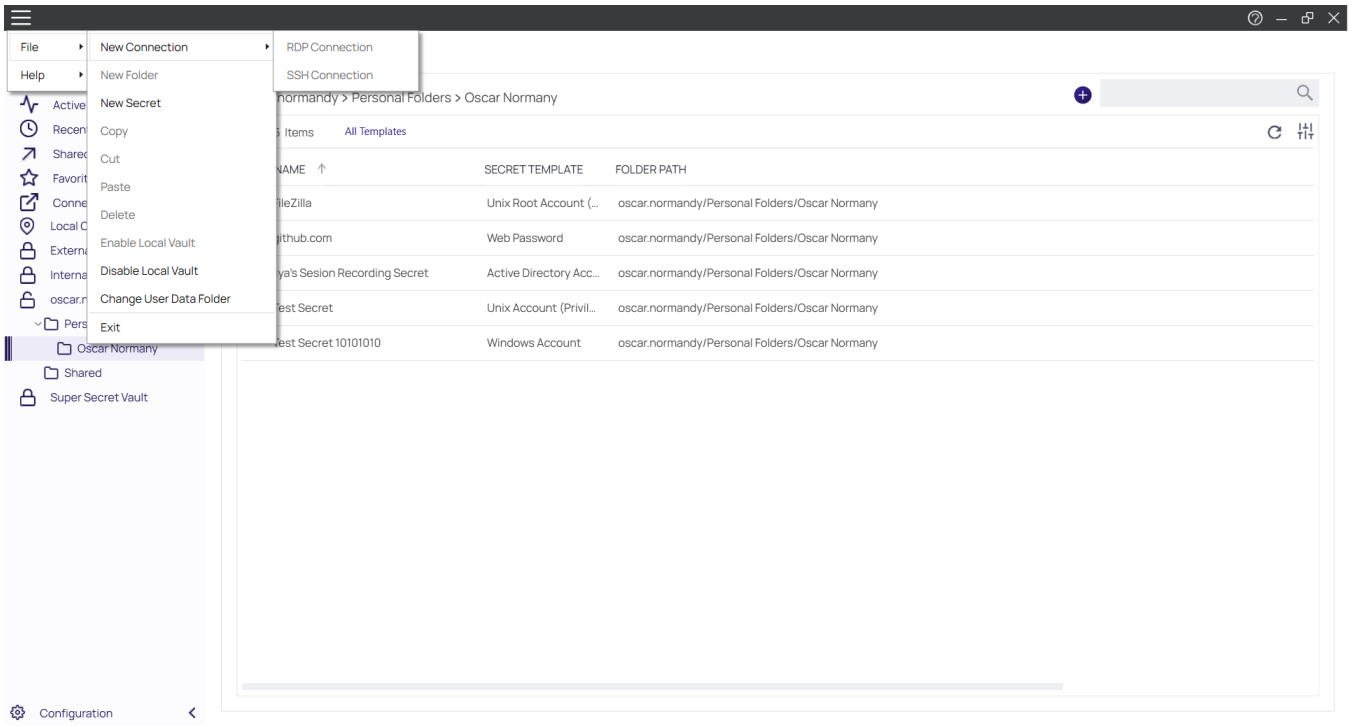
The menu at the top left of the application allows you to select File and Help.



File

Under File you can do the following:

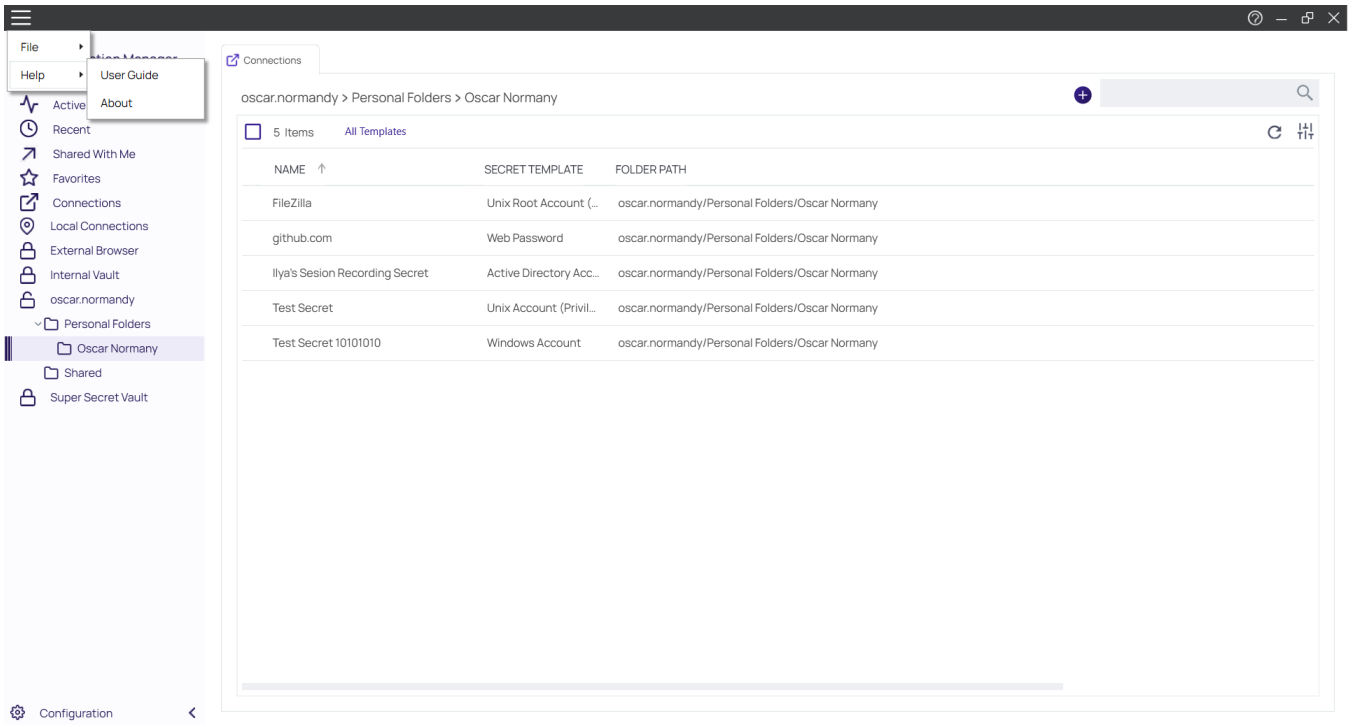
- Create new connections (RDP or SSH)
- Create new folders
- Delete folders/connections
- Exit the application



Note: The Stack menu is context sensitive so the available, displayed options depend on what is currently selected in the navigation tree or the main work area.

Help

Under Help you can select User Guide and About:



Right Click Navigation Menu

Right clicking a folder allows you to:

- Create new folders
- Create new connections
- Delete folders
- Export and Import connections
- Collapse and Expand Secret Server connections and Local connections

Work Area Menu

Right clicking the work area allows you to:

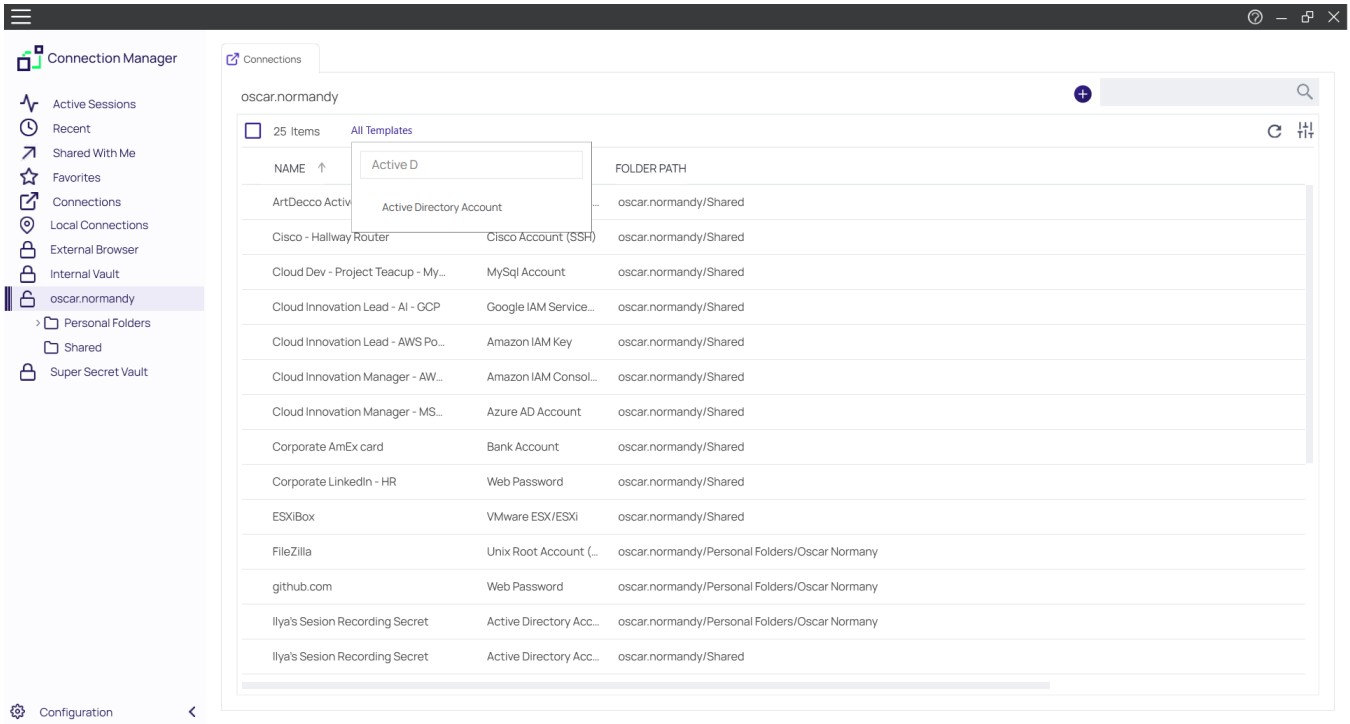
- Create new folders
- Create new connections (RDP or SSH)

Search

In the upper right corner of Connections, Local Connections, and Secret Server Connections windows there is a search box. A normal search action will only look within the currently selected folder. This search bar will act as a global search in some cases.

Template Search

The Template Search functionality allows you to search for secrets by secret template. You can select a template from the list or type in the name of the template.



Global Search

The global search option is only available at the top-level node for a Secret Server connection, or if the Local Connections node is selected in the navigation bar. Global search is available in the top right corner of the work area and will perform a search through the entire selected connection.

For example, if a user selects the top level of a Secret Server connection and then performs a search, the search will look through the entire Secret Server connection for the value, but it will not look through the Local Connections or any other Secret Server connections. If a user instead selects their personal folder or a sub-folder within the connection, the search will be limited to only the selected folder.

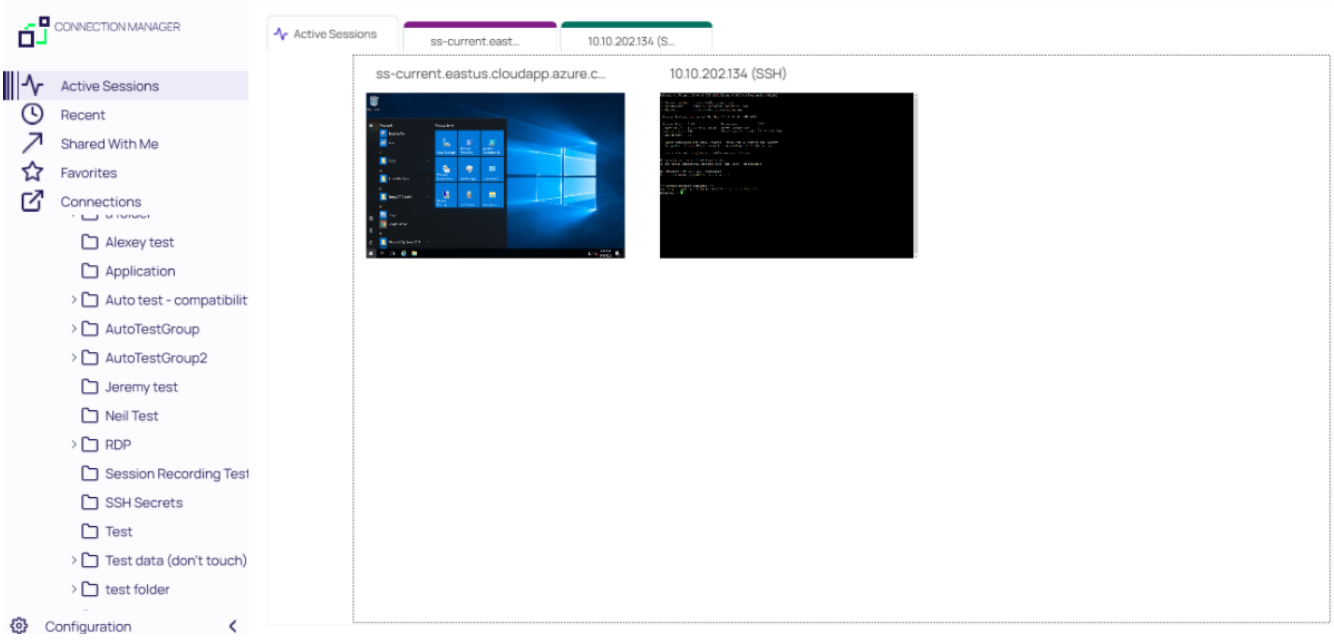
Configuration

Located at the bottom left of the application screen, the Configuration button allows users to set up and control various aspects of the application.

Navigation Tree

Active Sessions

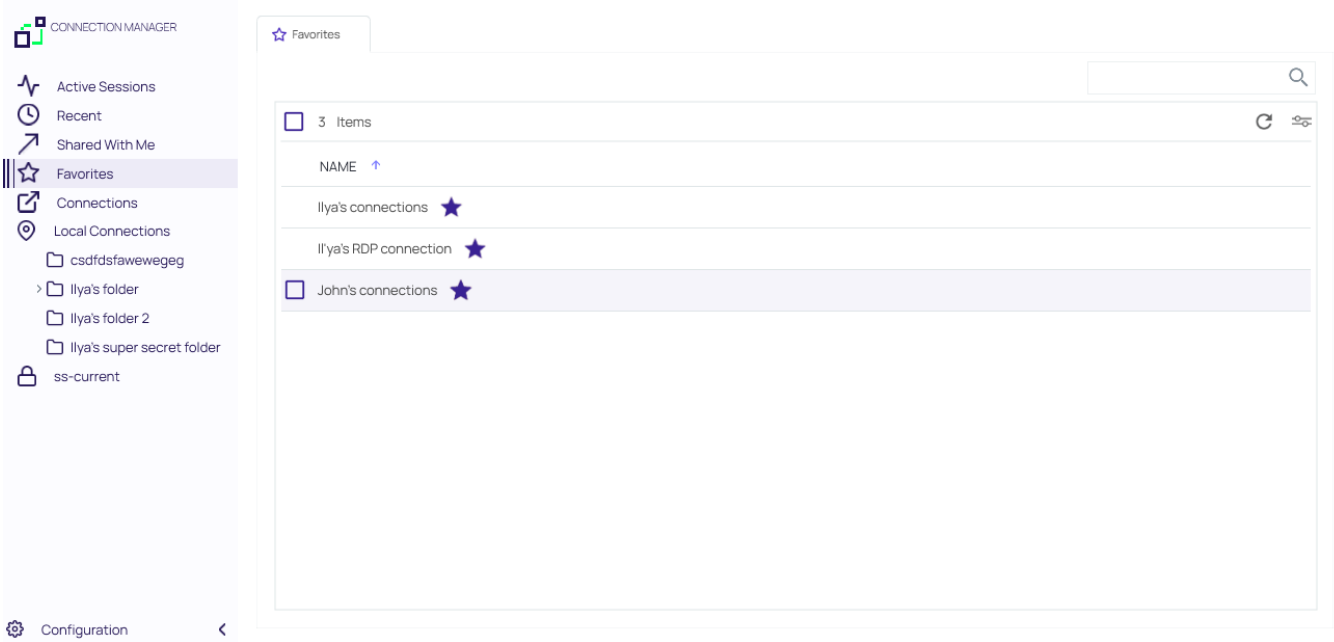
Select to view all active sessions.



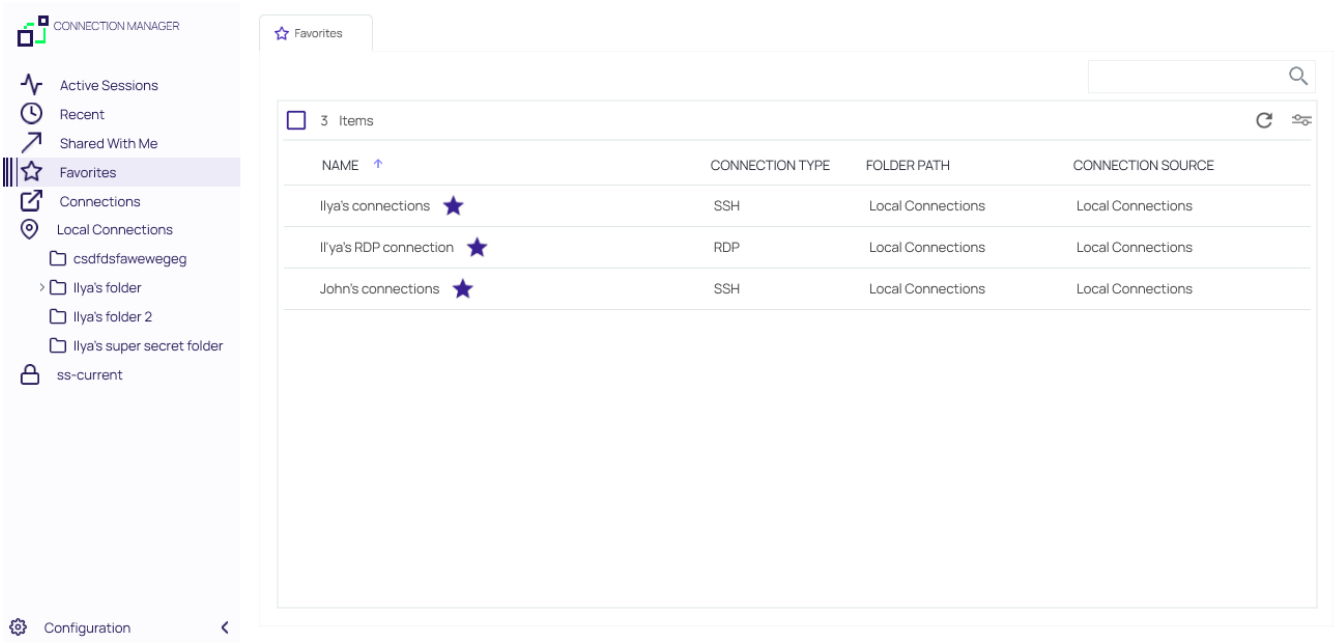
Favorites

You can add favorite connections by hovering over an existing connection and selecting the star. Favorites that are specified in Connection Manager will also be listed as favorites in Secret Server and vice versa.

Favorites page showing only local connection favorites:

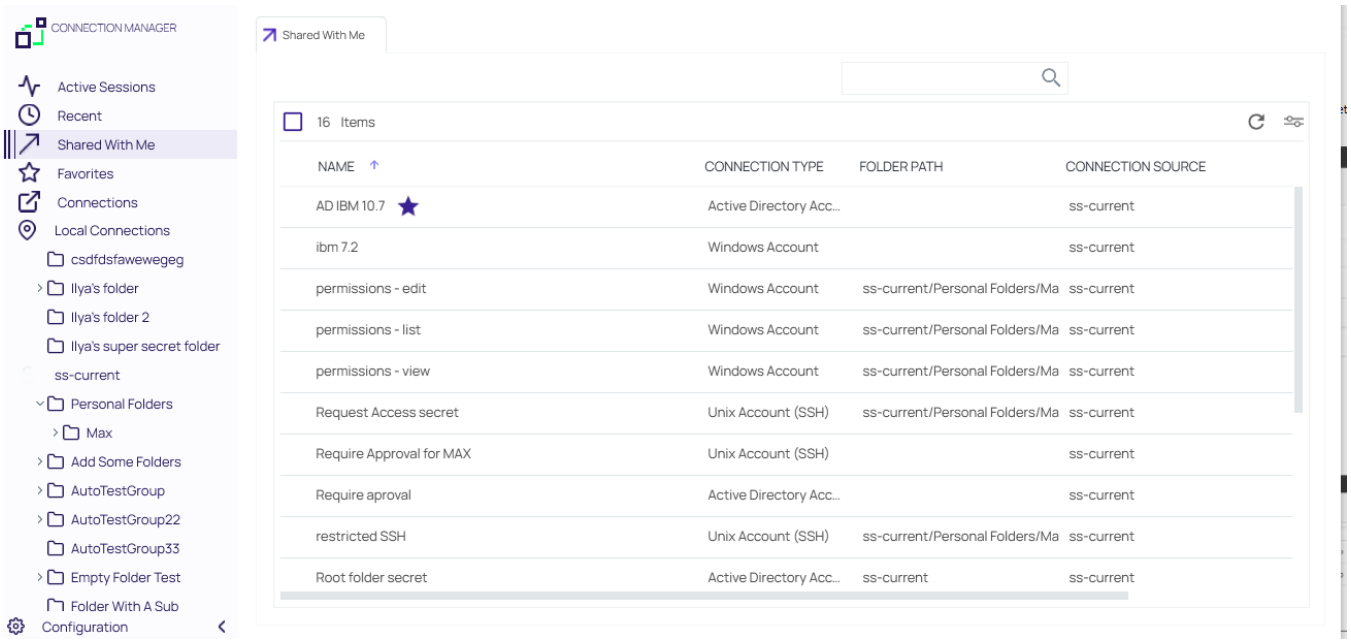


Favorites page showing local and Secret Server connection favorites:



Shared With Me

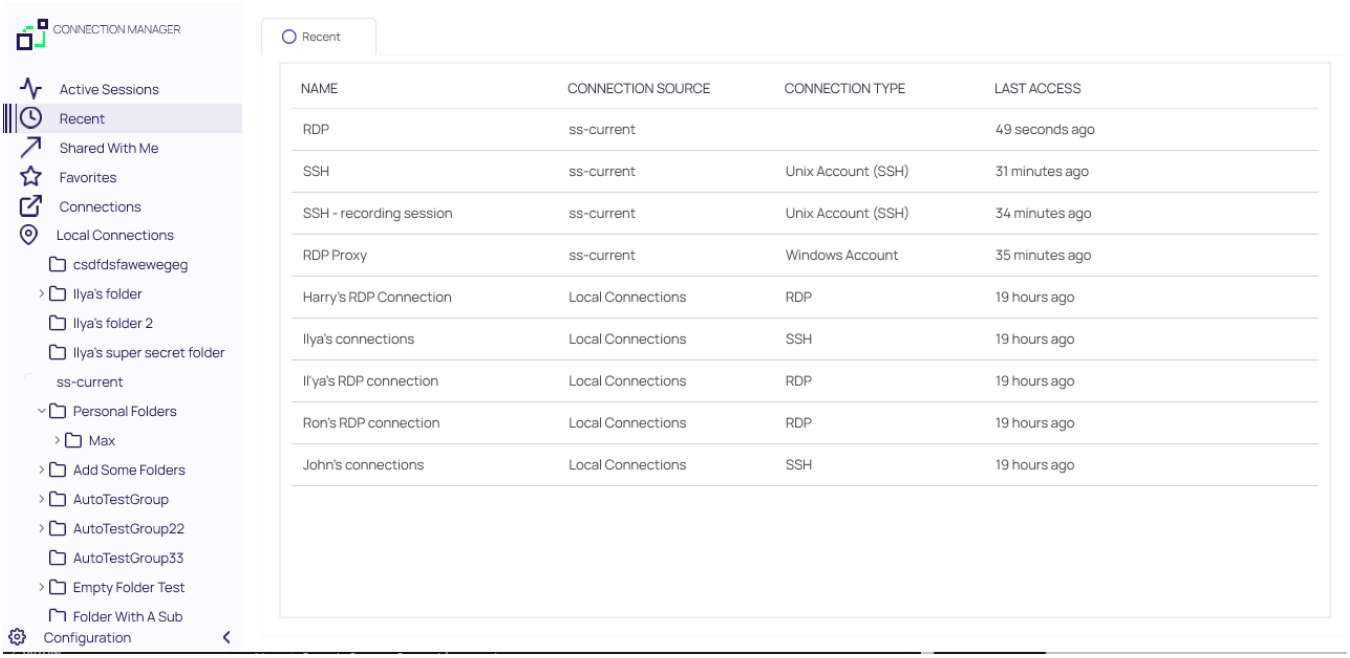
Select to view or launch all secrets and sessions shared with you from all currently connected secret servers.



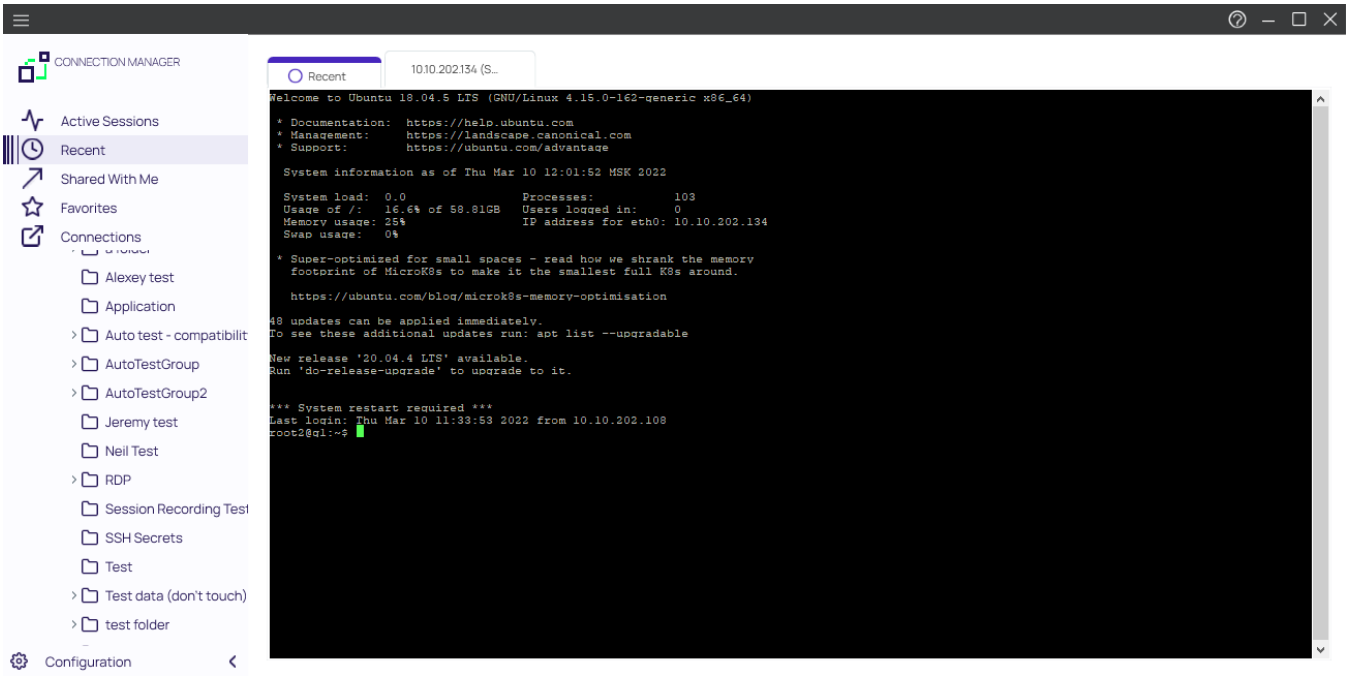
Double clicking on these Secrets will launch sessions.

Recent

Select to view or launch recently active sessions or to create a new Secret Server connection.

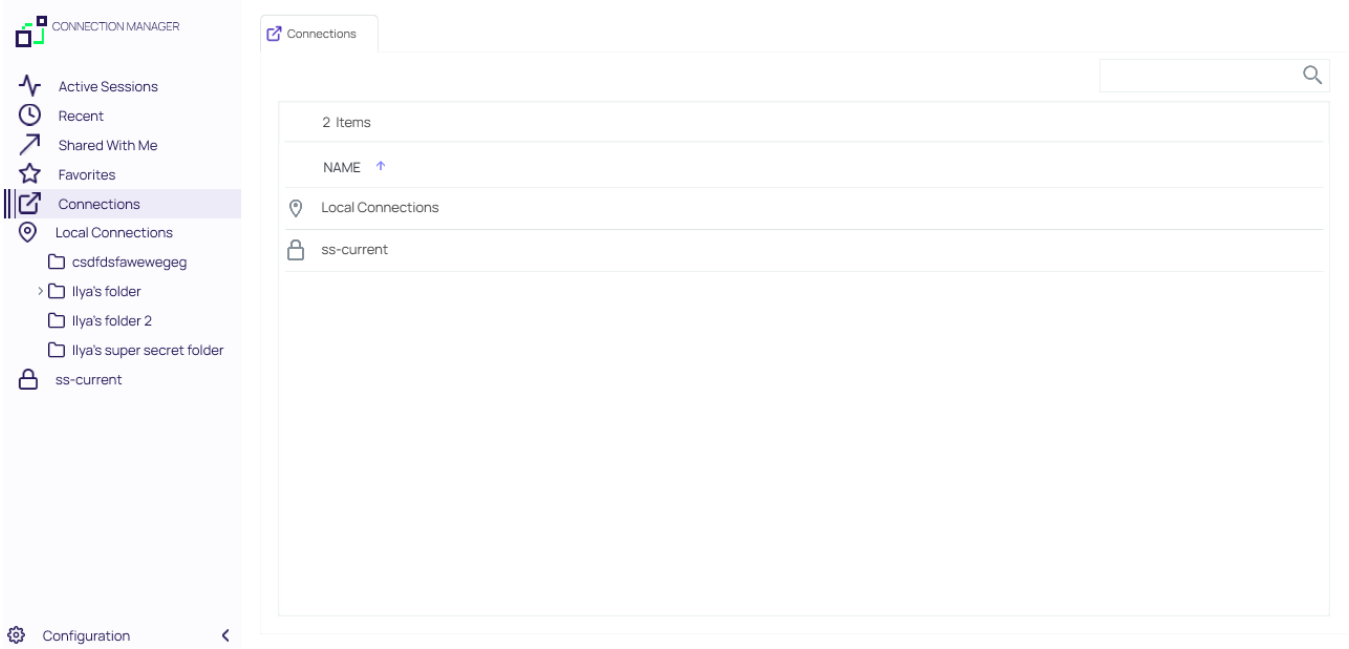


Existing entries also display connection type. These can be viewed via tab.

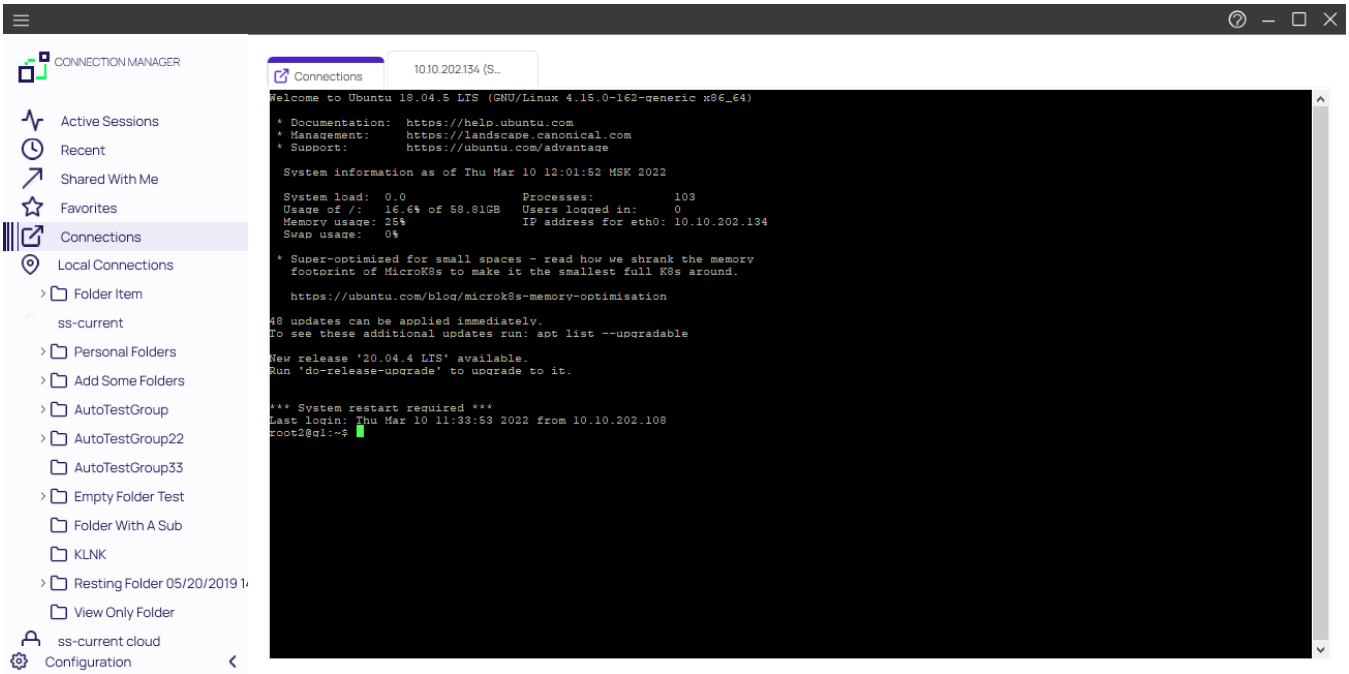


Connections

Select to display the folder tree for Local and Secret Server connections.



Navigate using the tree, or drill-down through folders to display in the work area window. Existing connections can be viewed via tab.



Local Connections

Select to view all local connections. In this view, you can drag and drop folders to organize them logically.

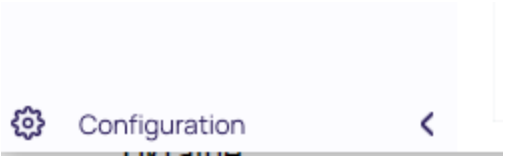
Shared with me

Select to view all secrets/sessions shared with you from a Secret Server connection. You can double-click these Secrets to launch sessions for them.

Configuration

Clicking within this area brings up a sub-menu with options such as

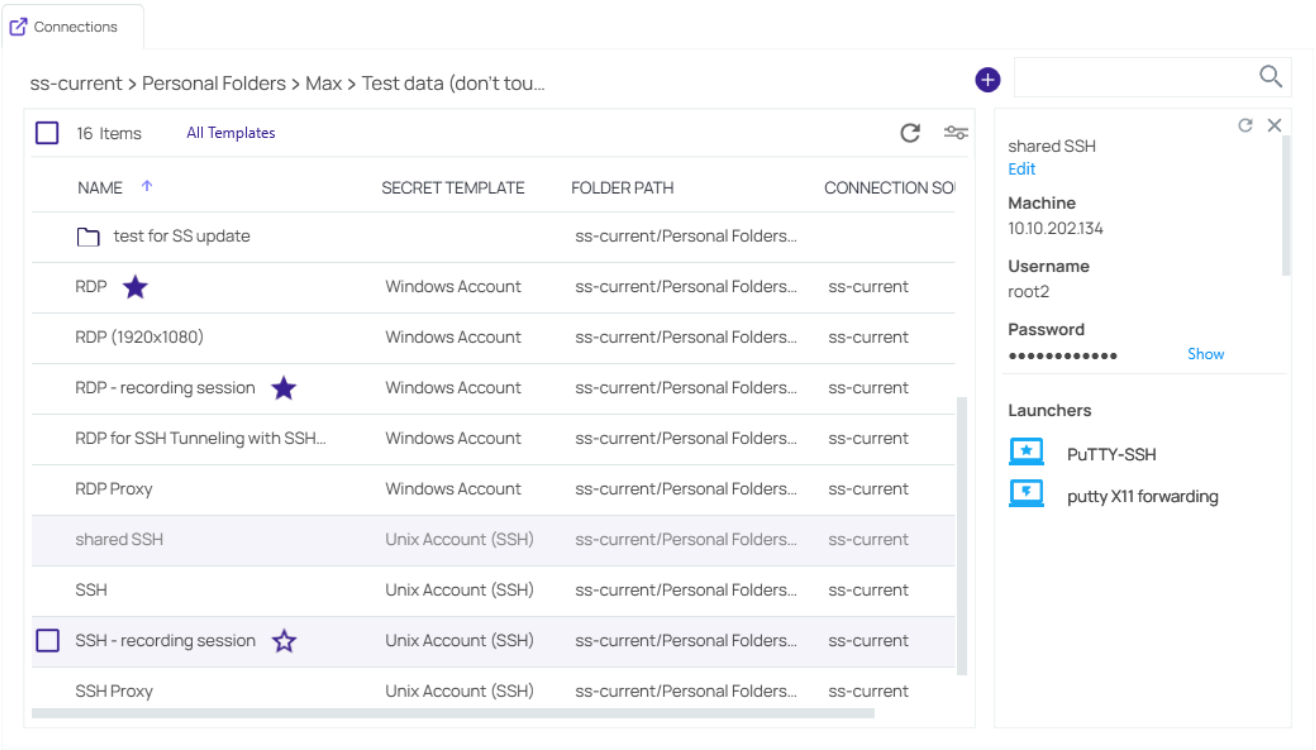
- Secret Server Connections and
- Global Configurations.



The **<** can be used to collapse and **>** expand the Navigation menu.

Properties Area

All Local connections, Secret Server connections, and folders have a Properties section. This section allows a user to view some of the details of the connection and folder and allows users to perform functions on the selected object, such as launching a connection, editing properties, or viewing passwords.



Note: The Properties section for a Secret Server Secret will never display, or have an option to display, the password for that Secret.

Work Area

The work area consists mostly of tabs representing open connections. The first tab corresponds to one of the selected options in the navigation tree which includes

- Active Sessions,
- Recent Connections, or
- a folder-view of Local Connections/connected Secret Server. For the latter, you may navigate through folders directly inside either connection tabs.

Authenticating to a Vault

This section contains information about:

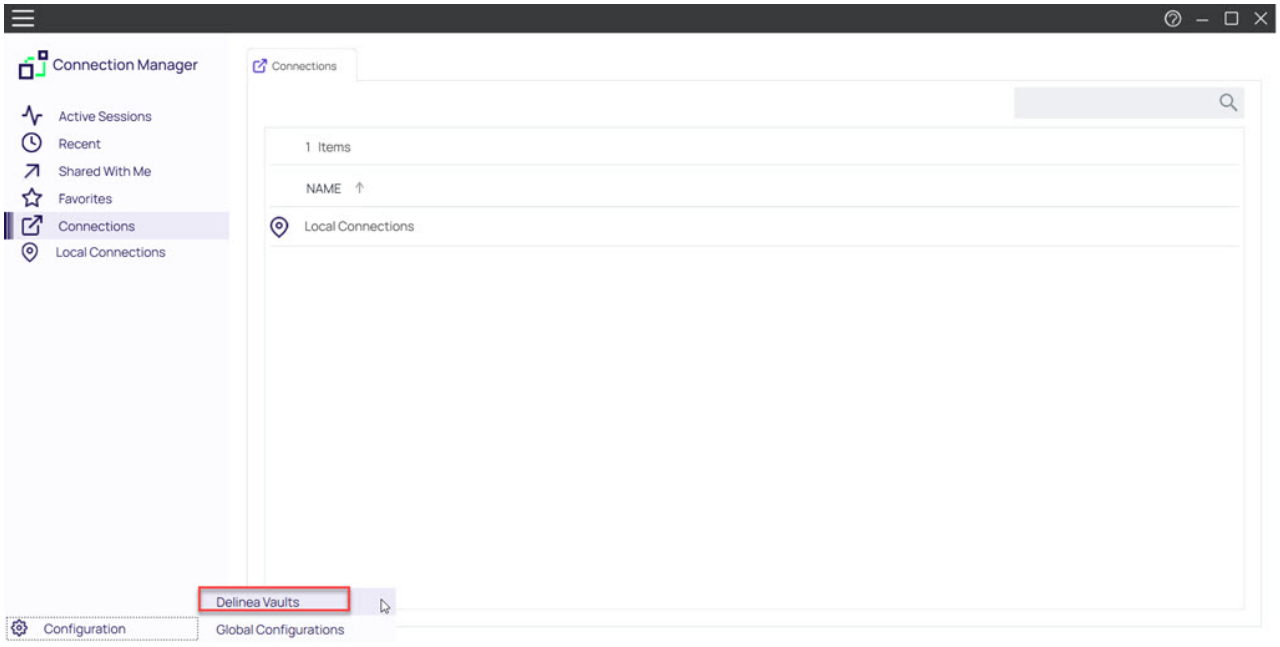
- "Authenticating to a Delinea Platform Vault" below
- "Authenticating to Secret Server " on page 55
- "Authenticating to Secret Server via Local Username" on page 66
- "Re-authenticating to a Vault" on page 76
- "Modifying a Vault" on page 78
- "Removing a Vault" on page 81

Authenticating to a Delinea Platform Vault

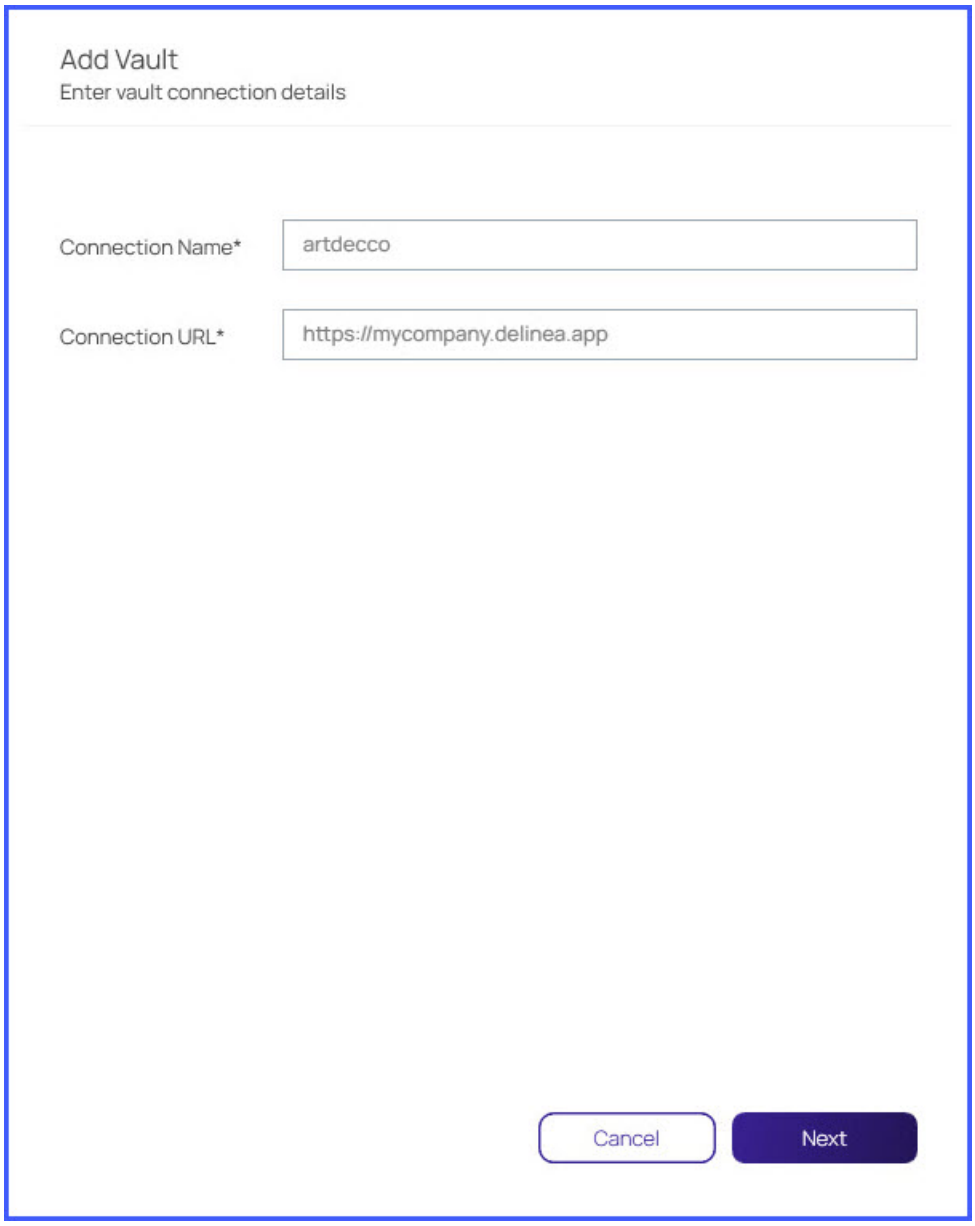
Users can connect to the Delinea Platform via external and internal browser. External browser login is conducted through the user's default web browser, whereas internal login is conducted through an embedded Connection Manager browser.

Authenticating to the Delinea Platform via External Browser

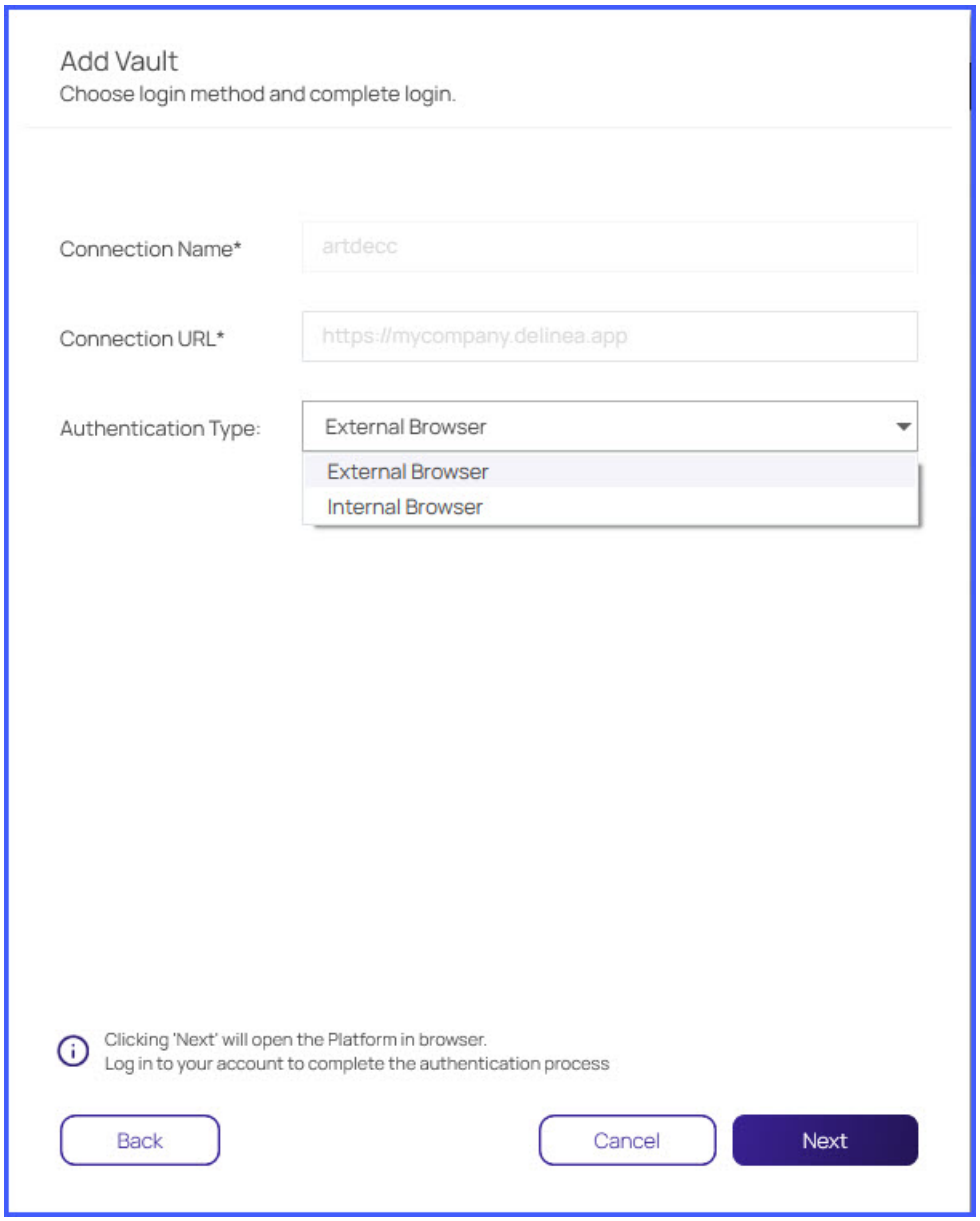
1. In the *Configuration* menu, select **Delinea Vaults**



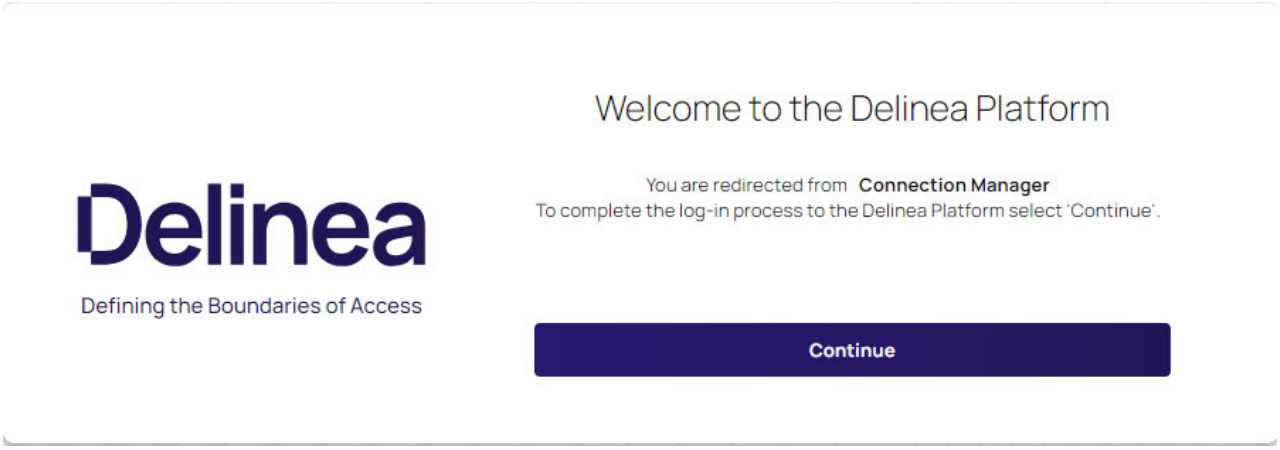
2. Enter your *Connection Name* and *Connection URL* and click **Next**



3. In the *Authentication Type* dropdown menu, select **External Browser** and click **Next.**

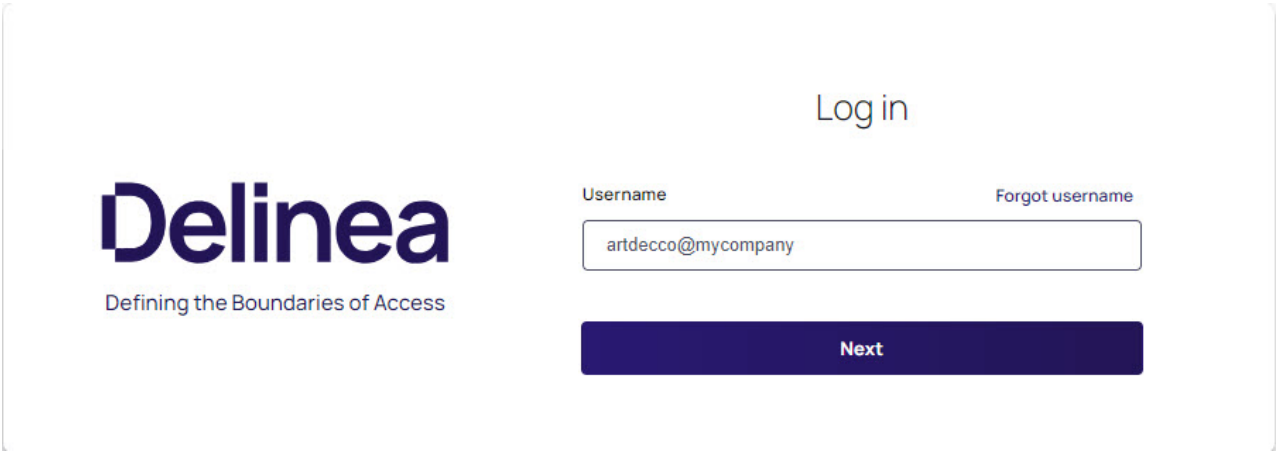


4. A browser window will open to redirect you to the Delinea Platform's login page. Click **Continue** to proceed.



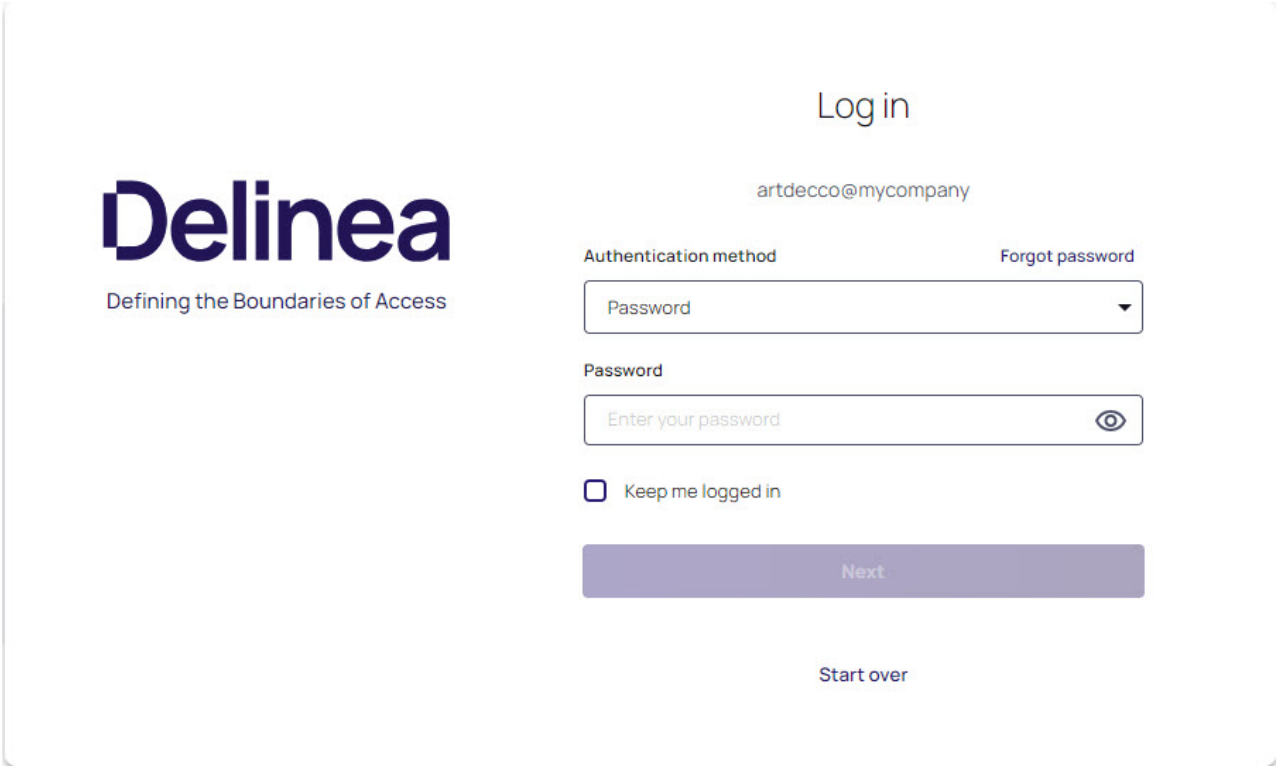
5. Enter your *Username* and click **Next.**

   Note: The username must be in the following format: username@domain. For example, artdecco@mycompany

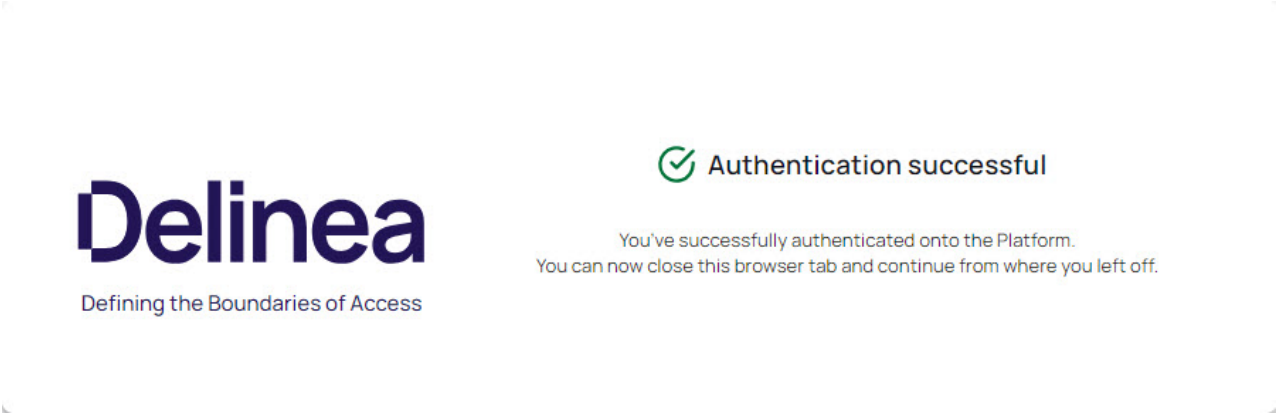


6. If required, select your authentication method and enter your credentials. Click **Next**

   Note: You may be challenged with other secondary prompts like MFA, Security Question, etc. depending on your login profile.



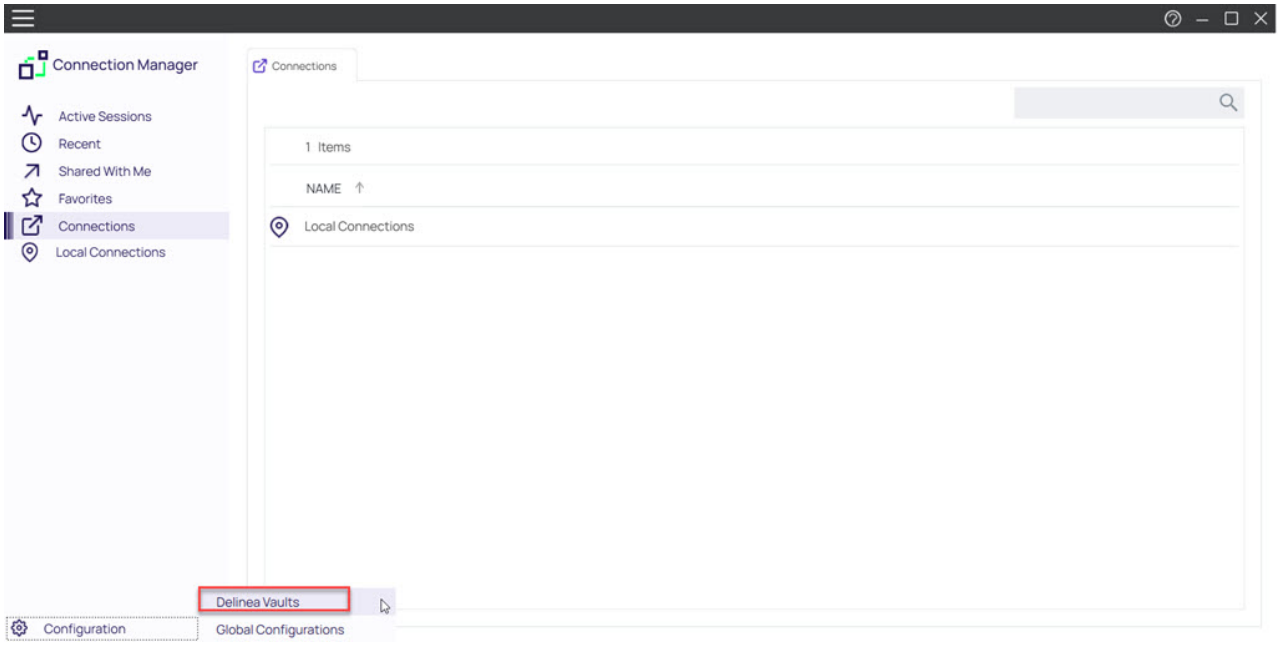
7. You have successfully logged in to the Delinea Platform.



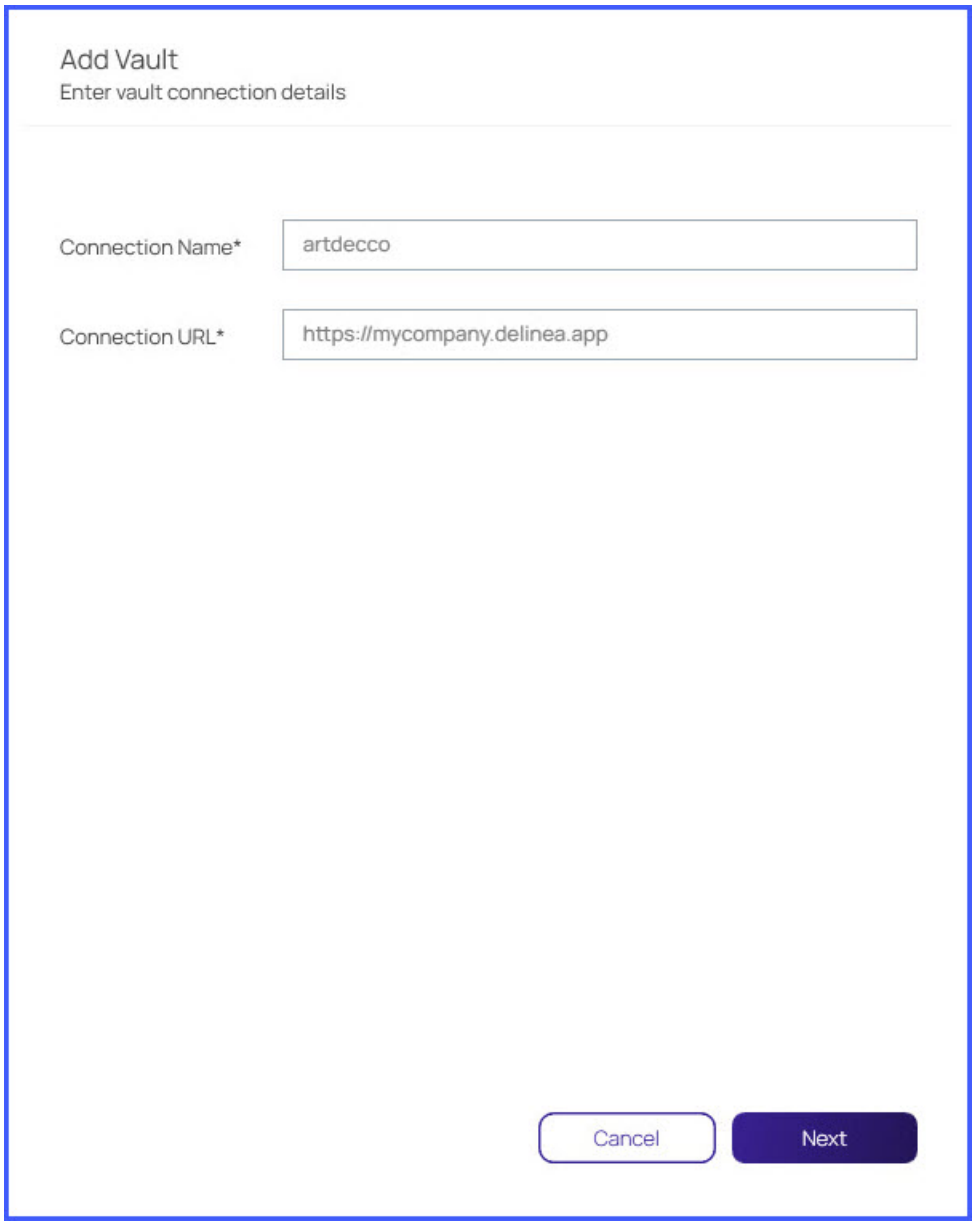
Authenticating to the Delinea Platform via Internal Browser

Internal browser authentication is deprecated as of the 2.8 release. The information on this page applies to versions 2.7.1 and earlier.

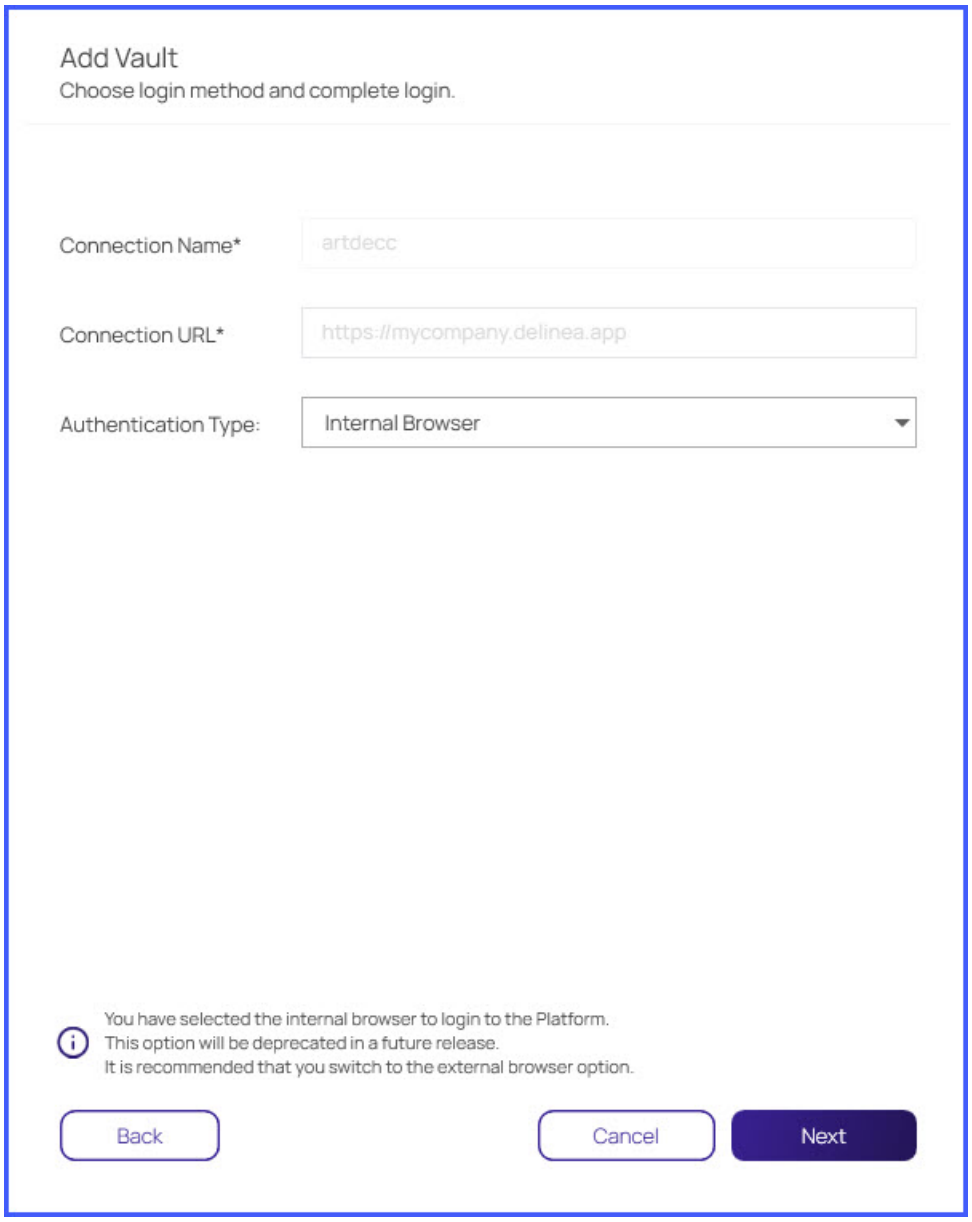
1. In the *Configuration* menu, select **Delinea Vaults**



2. Enter your *Connection Name* and *Connection URL* and click **Next**.

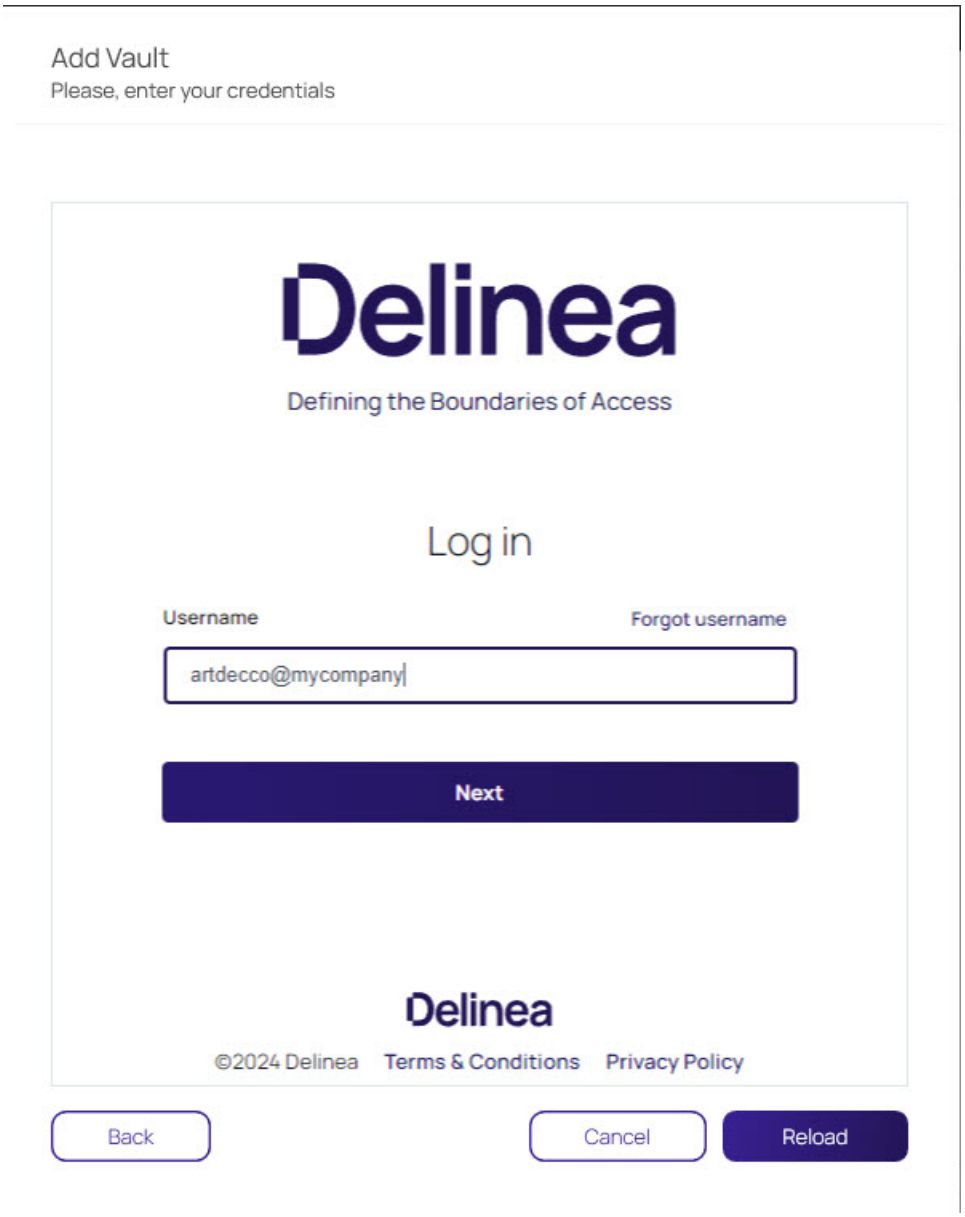


3. In the *Authentication Type* dropdown menu, select **Internal Browser** and click **Next.**



4. Enter your *Username* and click **Next**

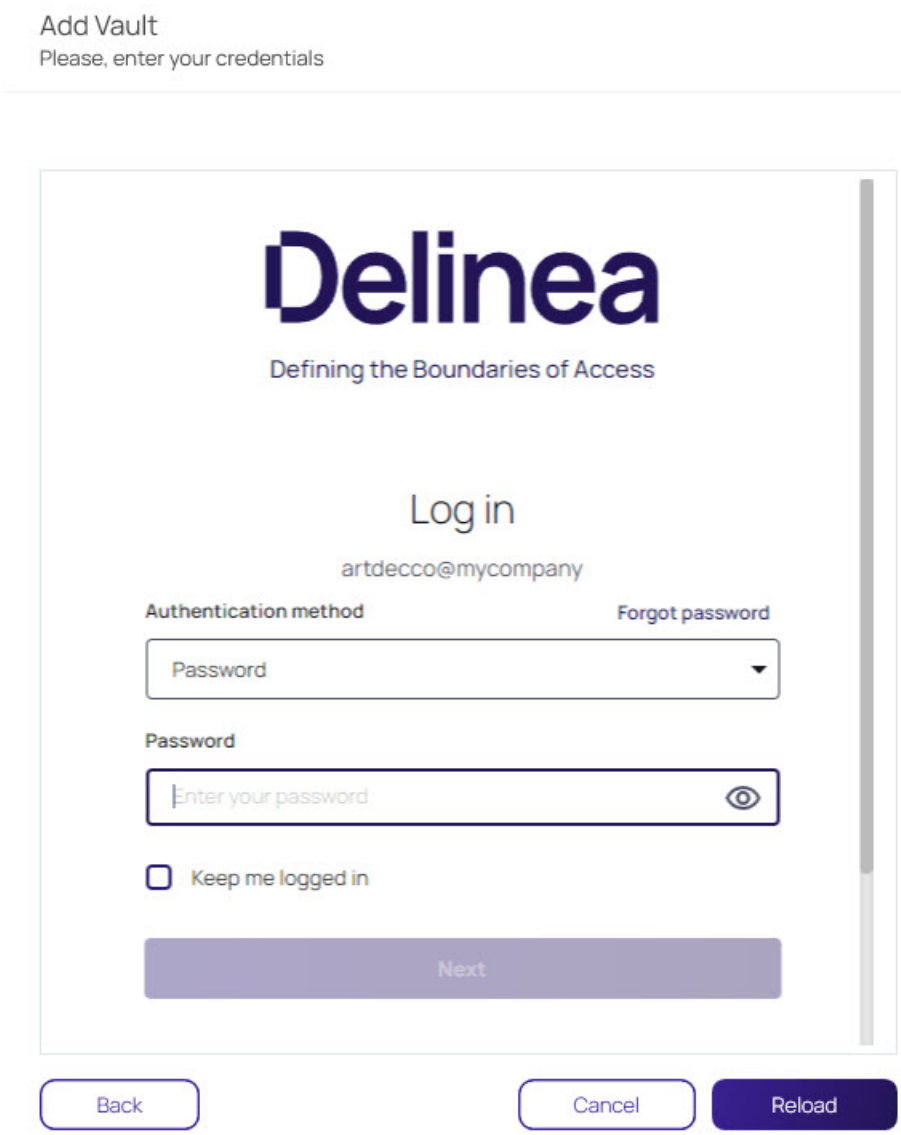
   Note: The username must be in the following format: username@domain. For example, artdecco@mycompany



.

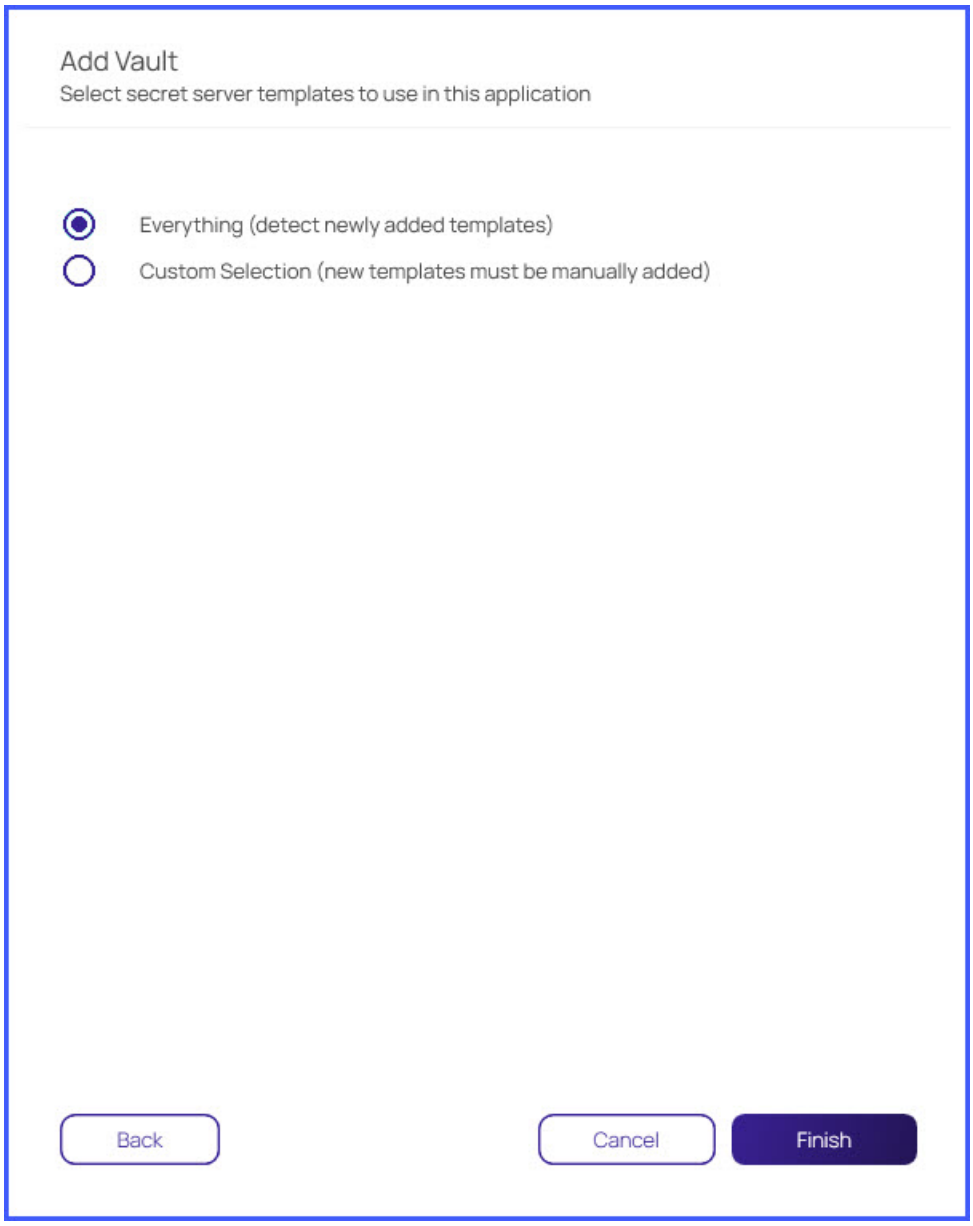
5. If required, select your authentication method and enter your credentials. Click **Next**

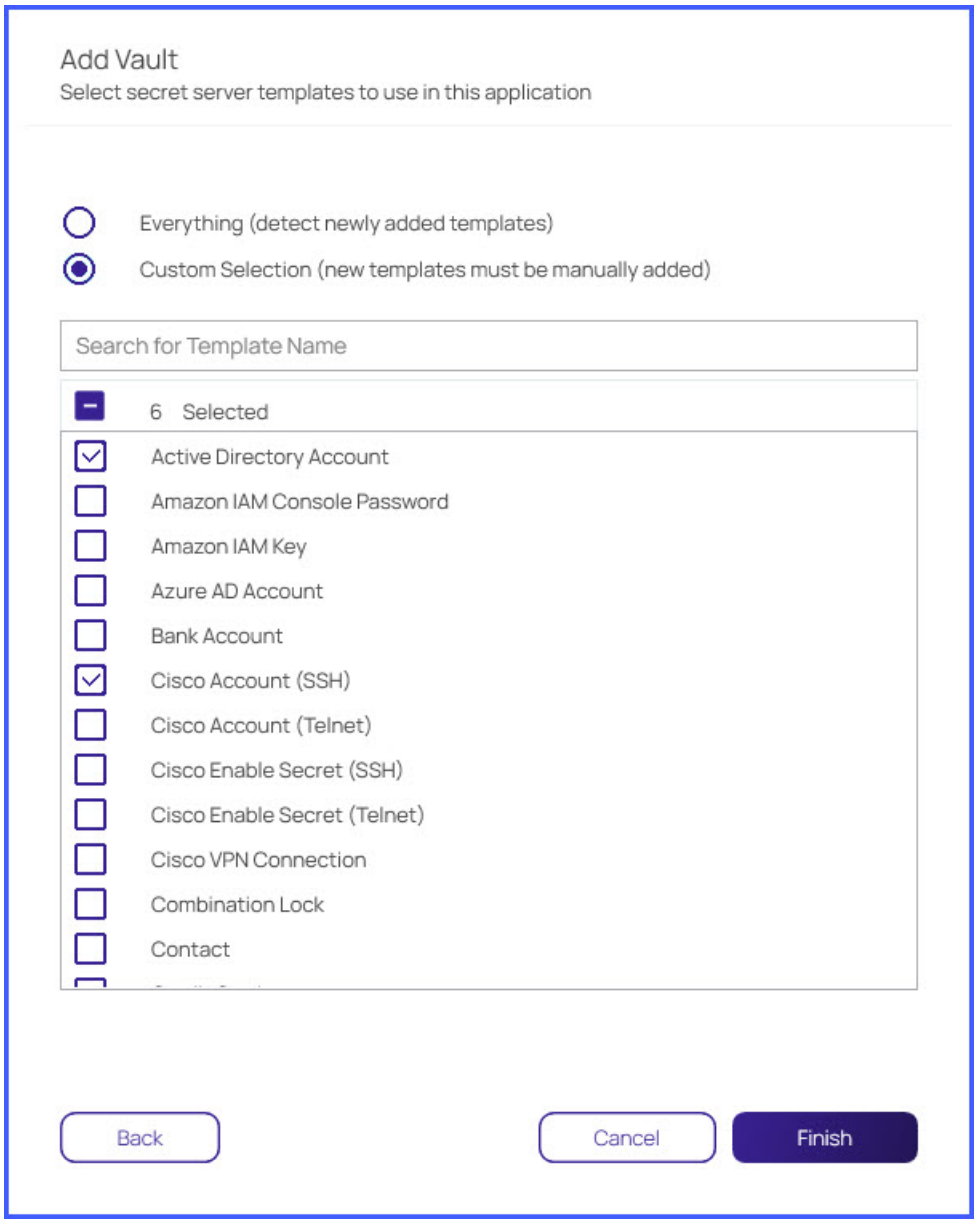
   Note: You may be challenged with other secondary prompts like MFA, Security Question, etc. depending on your login profile.



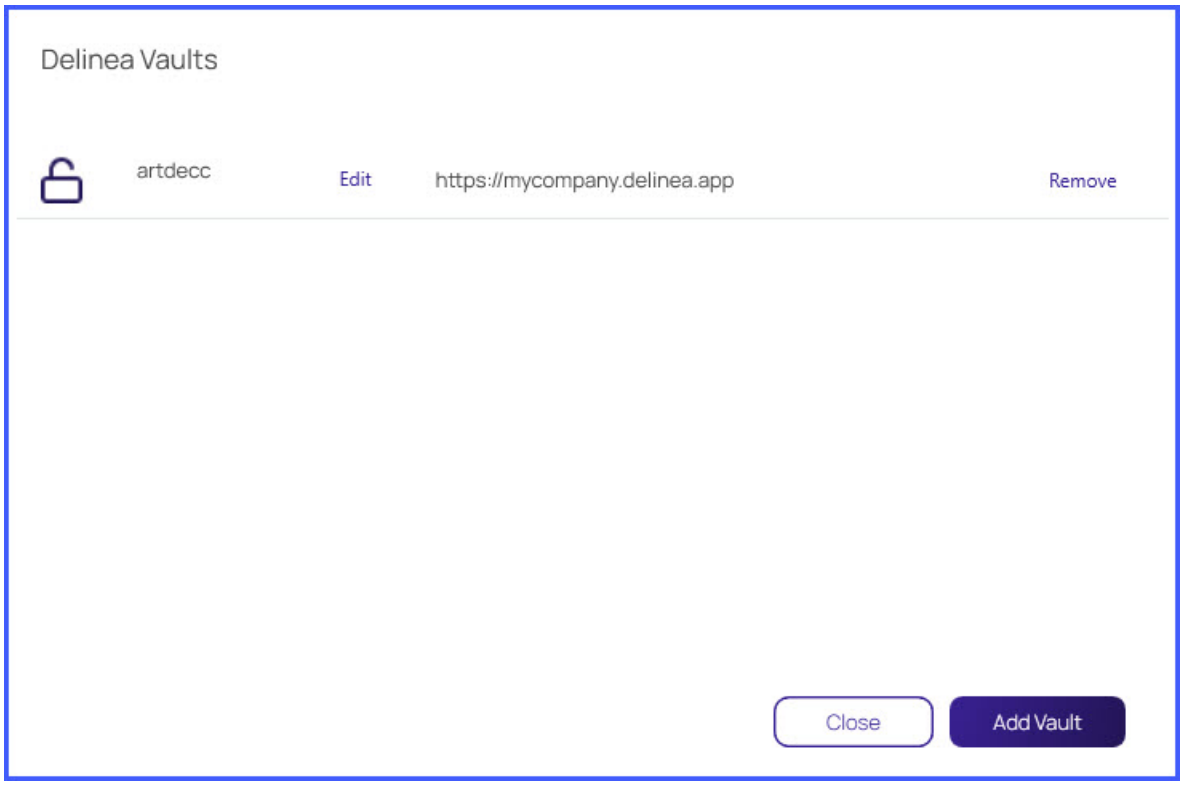
.

6. Select the Secret Server templates you would like to use with this application. You can choose to use all templates or custom selected ones. Click **Finish.**


Add Vault
Select secret server templates to use in this application
Everything (detect newly added templates)
Custom Selection (new templates must be manually added)
Back
Cancel
Finish



7. Your external vault has been created.

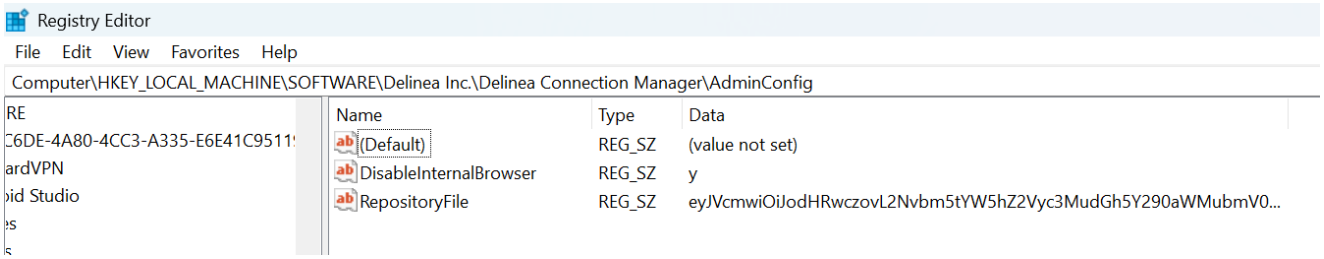


Enabling Internal Browser Authentication

Administrators can enable internal browser authentication by following the steps below:

On Windows:

In the Registry Editor, change the value next to the *DisableInternalBrowser* parameter from `y` to `n`



On MacOS:

Change the value next to the `env.DisableInternalBrowser` parameter in the root `p.list` file from `y` to `n`.

`/Library/Preferences/com.Delinea.ConnectionManager.plist env.DisableInternalBrowser y`

Authenticating to Secret Server

This section contains information about:

- "Secret Server Requirements " below
- " Authenticating to Secret Server via External Browser " below
- "Authenticating to Secret Server via Internal Browser " on page 61
- "Authenticating to Secret Server via Local Username" on page 66

Secret Server Requirements

The following are the hard requirements for connecting to Secret Server:

- Must have Secret Server 10.7:
  - Requires RESTAPIs
- Must have the "IsConnectionManager" flag set on Secret Server license
- When we connect, we try to check what version of Secret Server is being used:
  - If below 10.7 we will not connect
  - If we cannot detect the Secret Server version, we return the message we receive from Secret Server and it usually means the Secret Server version # is hidden, and we receive an "Access Denied" message
- A Secret Server Username

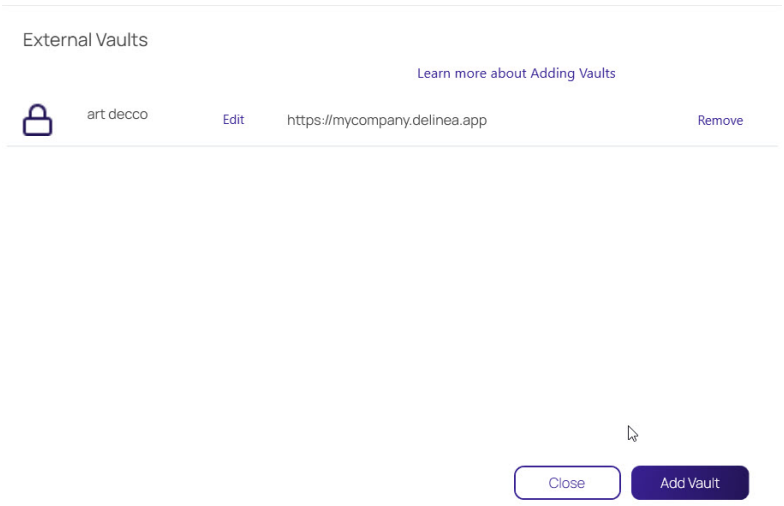
Note: If you are using a TLS certificate to authenticate to Secret Server, only TLS certificates versions 1.2 and newer are supported.

Authenticating to Secret Server via External Browser

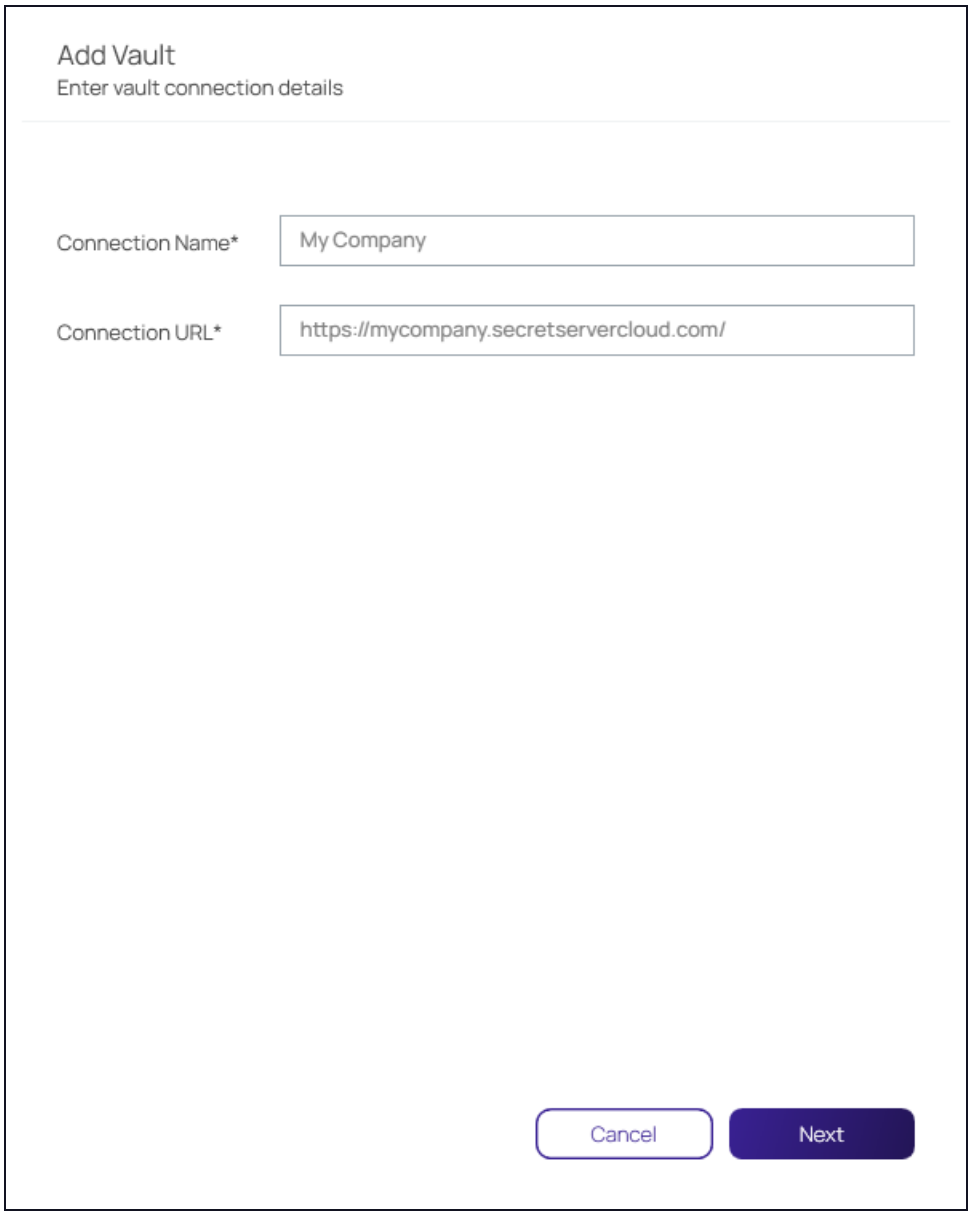
Connection Manager will only authenticate to Secret Server version 10.7 or later and requires a valid Secret Server license.

Note: For Secret Server implementations using Windows authentication, also refer to details in this article Setting Up Integrated Windows Authentication in Secret Server. Use the RestAPI as the authentication method instead of Windows authentication.

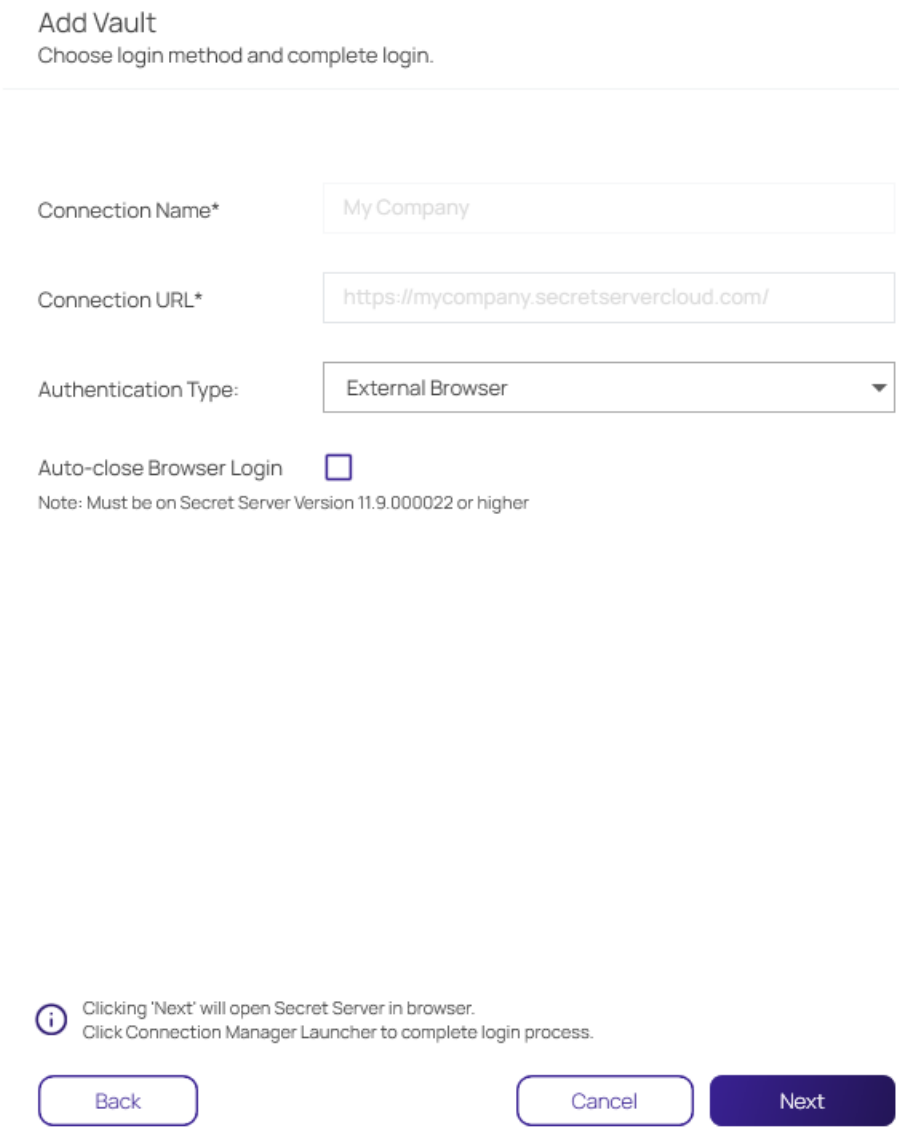
1. In the *Configuration* menu, select **Delinea Vaults**.
2. Click **Add Vault**.



3. Enter your Secret Server *Connection Name* and *Connection URL* and click **Next**.

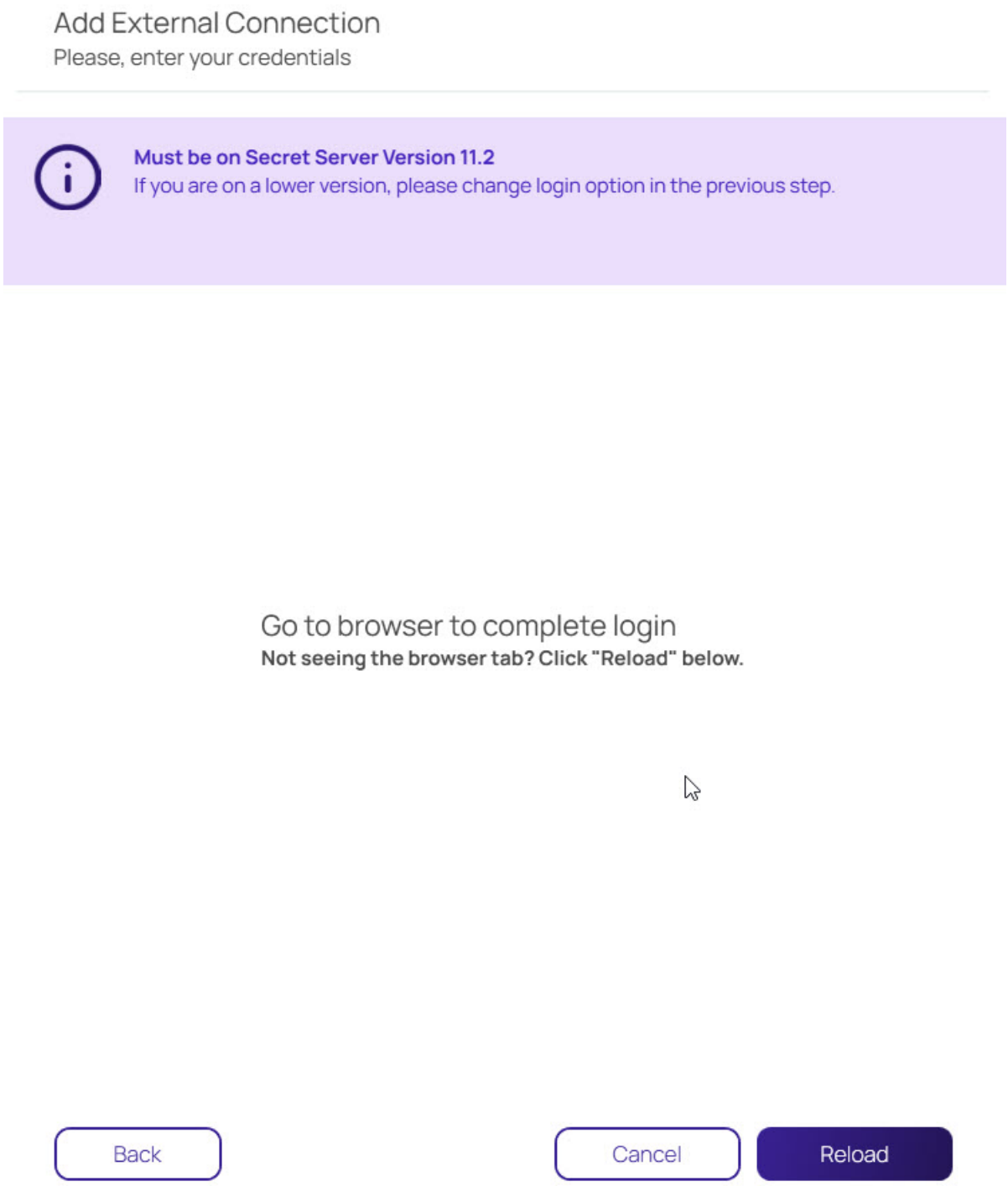


4. Select **External Browser** from the *Authentication Type* dropdown menu. If you would like your browser to auto-close upon successful login, check the *Auto-close Browser Login* box.

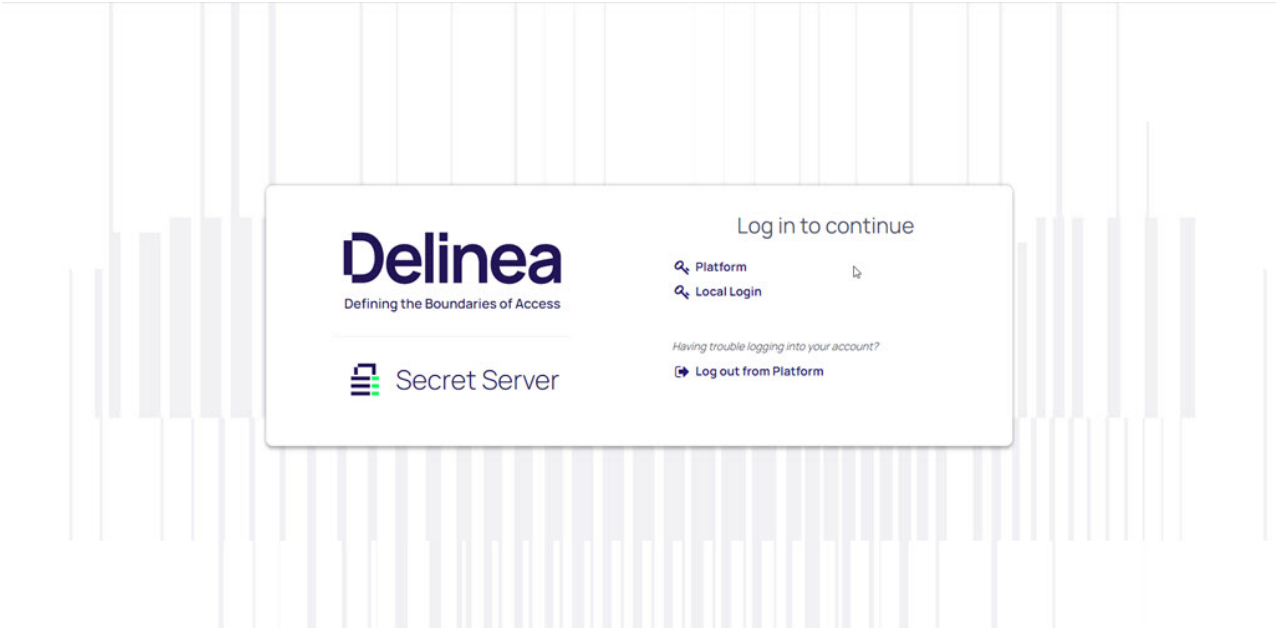


Note: The auto-close browser login feature requires Secret Server version 11.9.000022 or newer.

5. A Connection Manager banner will appear requesting that you go to your browser to complete the connection.



6. Login with your Delinea Platform or Local Login credentials.



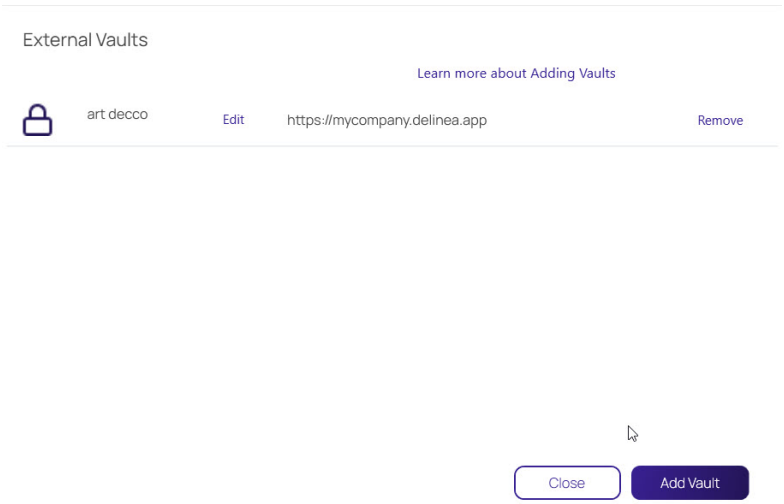
Note: When completing the login process in a browser tab opened by Connection Manager, this tab may not automatically close after a successful login.

Note: The external browser window will not close automatically after your first successful login attempt, but it will close after a second successful login and after.

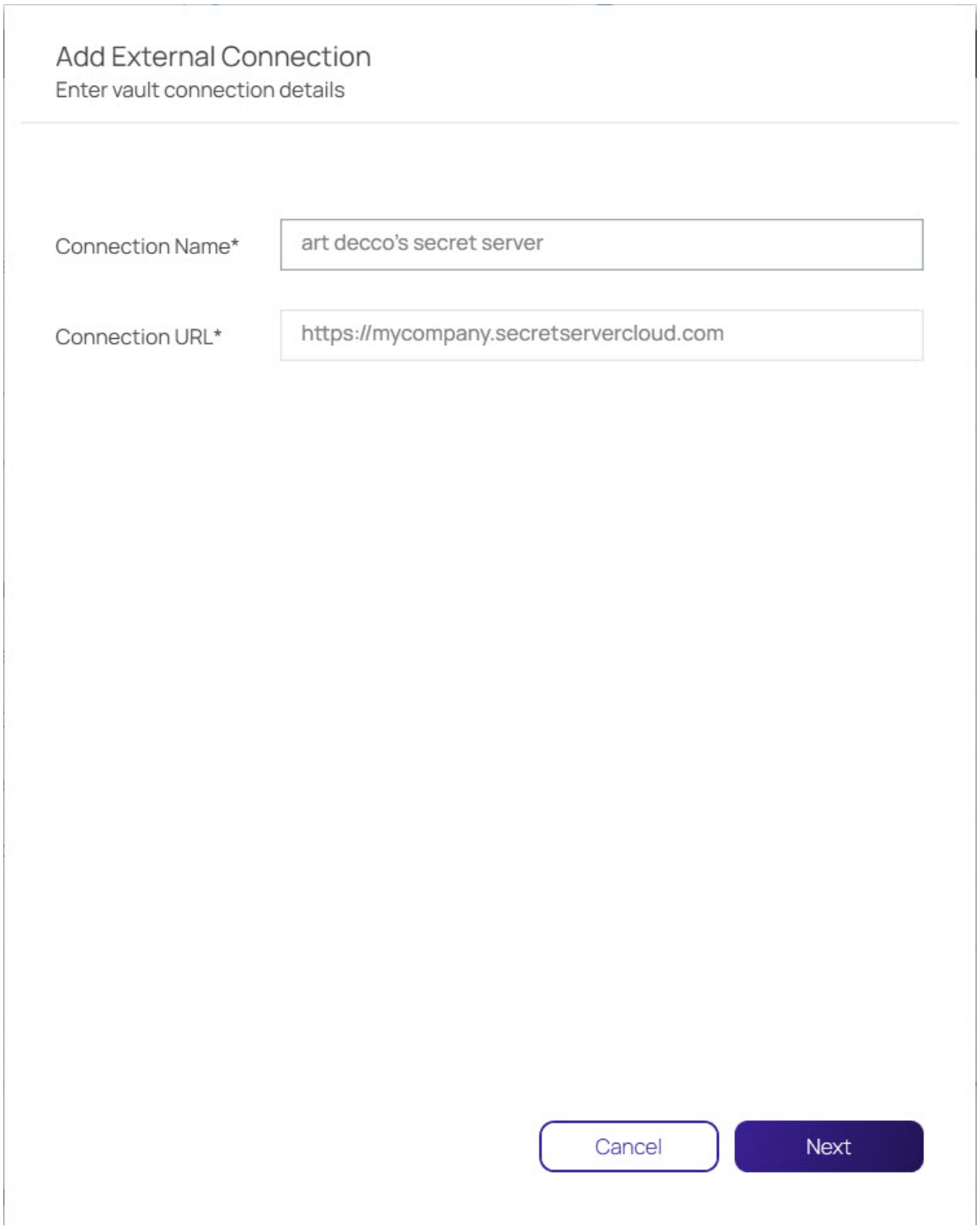
Authenticating to Secret Server via Internal Browser

Internal browser authentication is deprecated as of the 2.8 release. The information on this page applies to versions 2.7.1 and earlier.

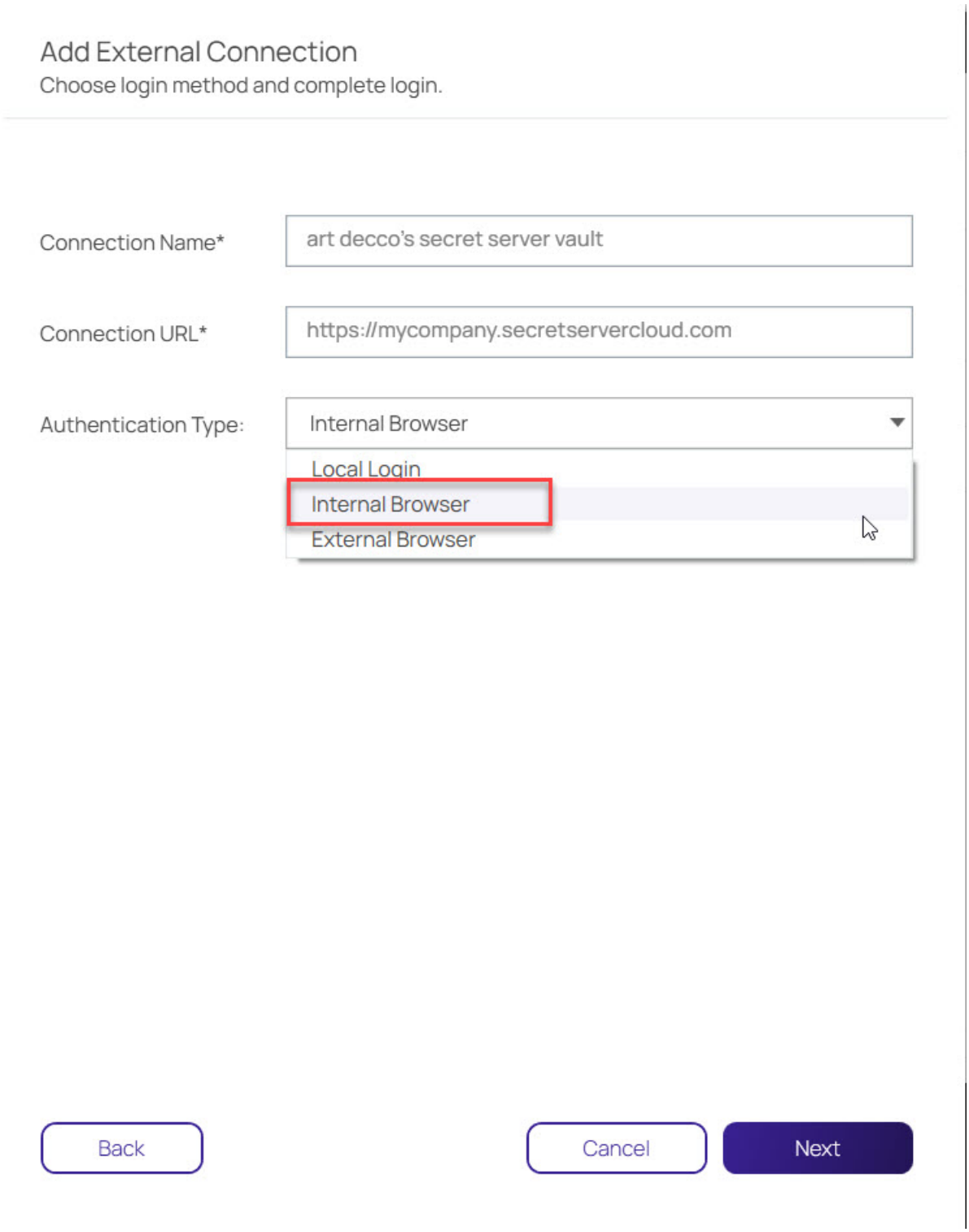
1. In the *Configuration* menu, select **Delinea Vaults**.
2. Click **Add Vault**.



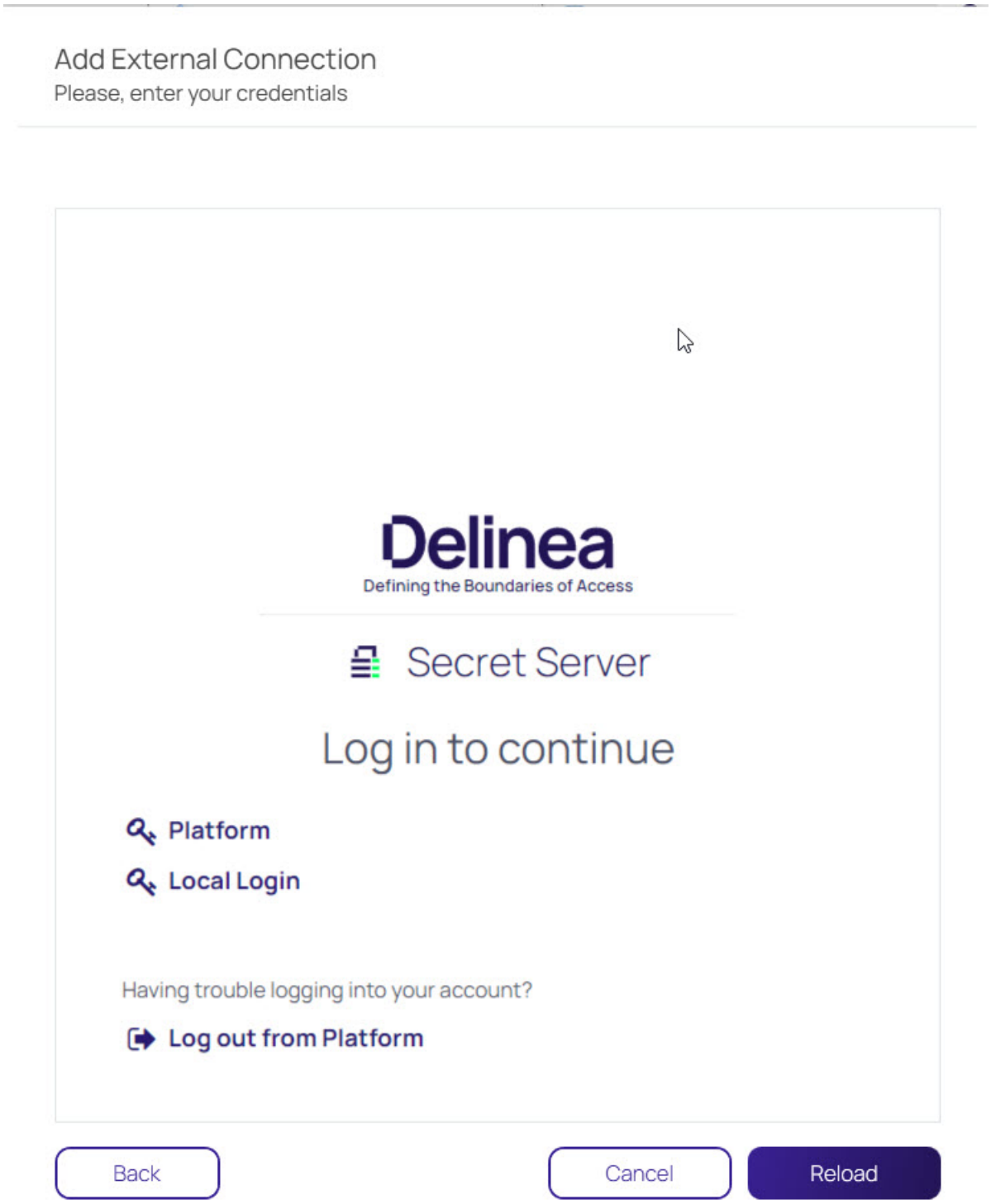
3. Enter your Secret Server *Connection Name* and *Connection URL* and click **Next**.



4. Select **Internal Browser** from the *Authentication Type* dropdown menu.



5. Log in with your Delinea Platform or Local Login credentials.

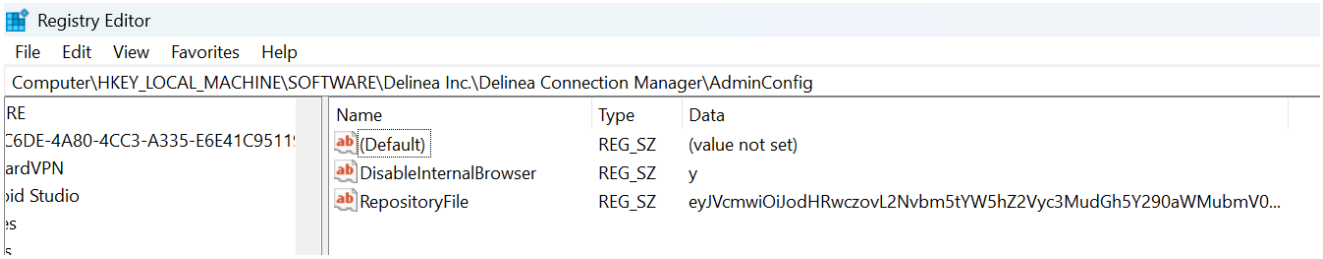


Enabling Internal Browser Authentication

Administrators can enable internal browser authentication by following the steps below:

On Windows:

In the Registry Editor, change the value next to the *DisableInternalBrowser* parameter from `y` to `n`



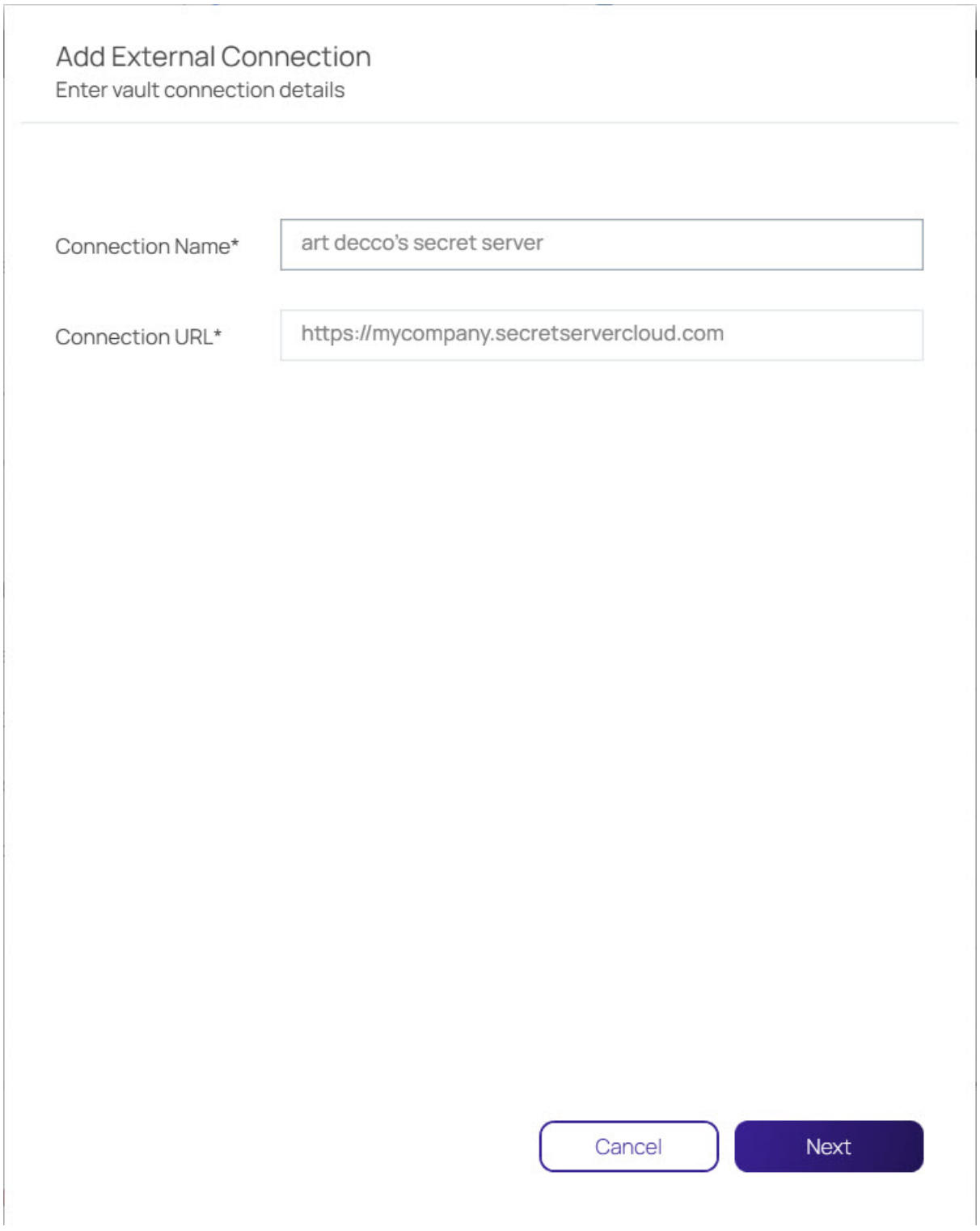
On MacOS:

Change the value next to the `env.DisableInternalBrowser` parameter in the root `p.list` file from `y` to `n`.

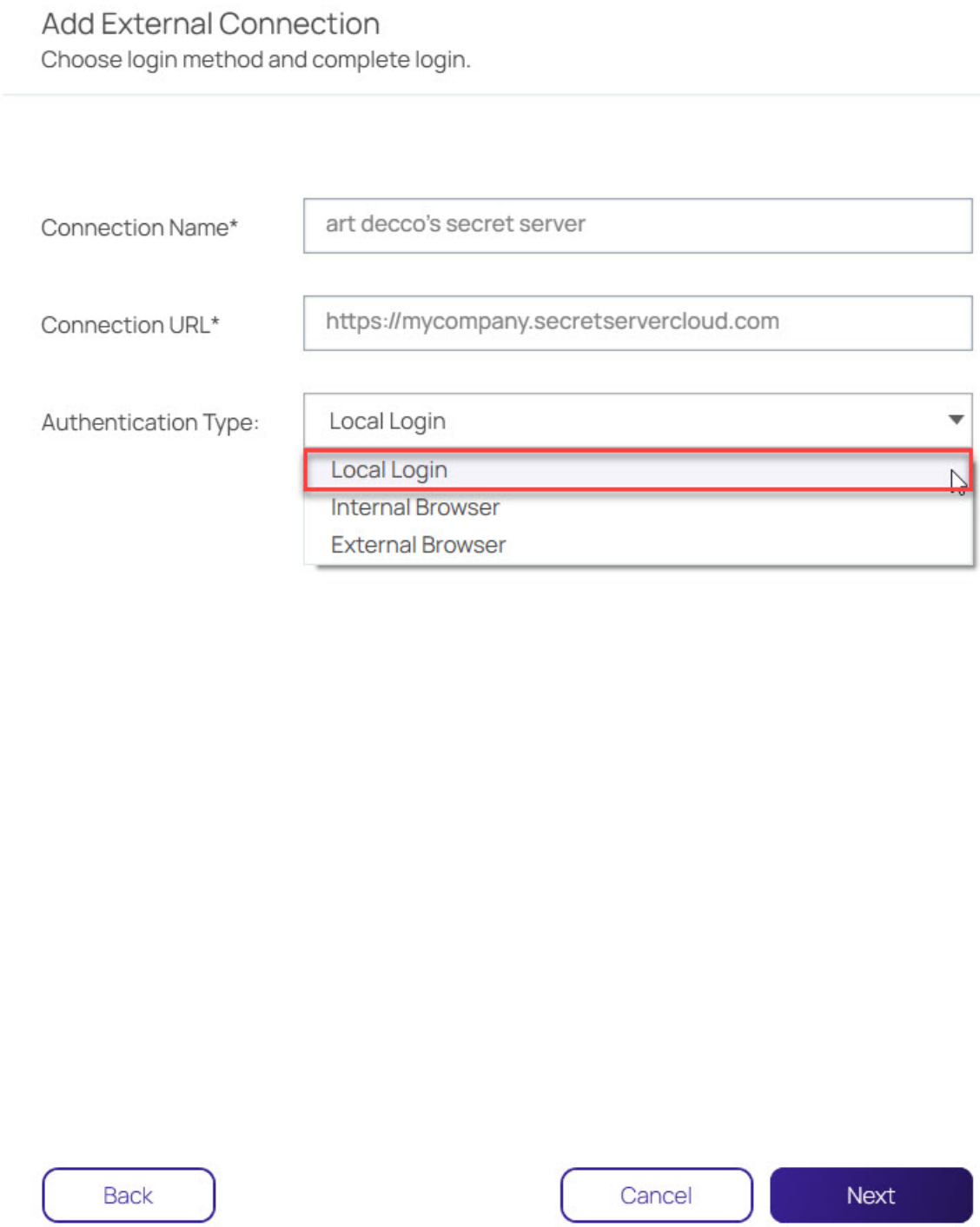
```
/Library/Preferences/com.Delinea.ConnectionManager.plist env.DisableInternalBrowser y
```

Authenticating to Secret Server via Local Username

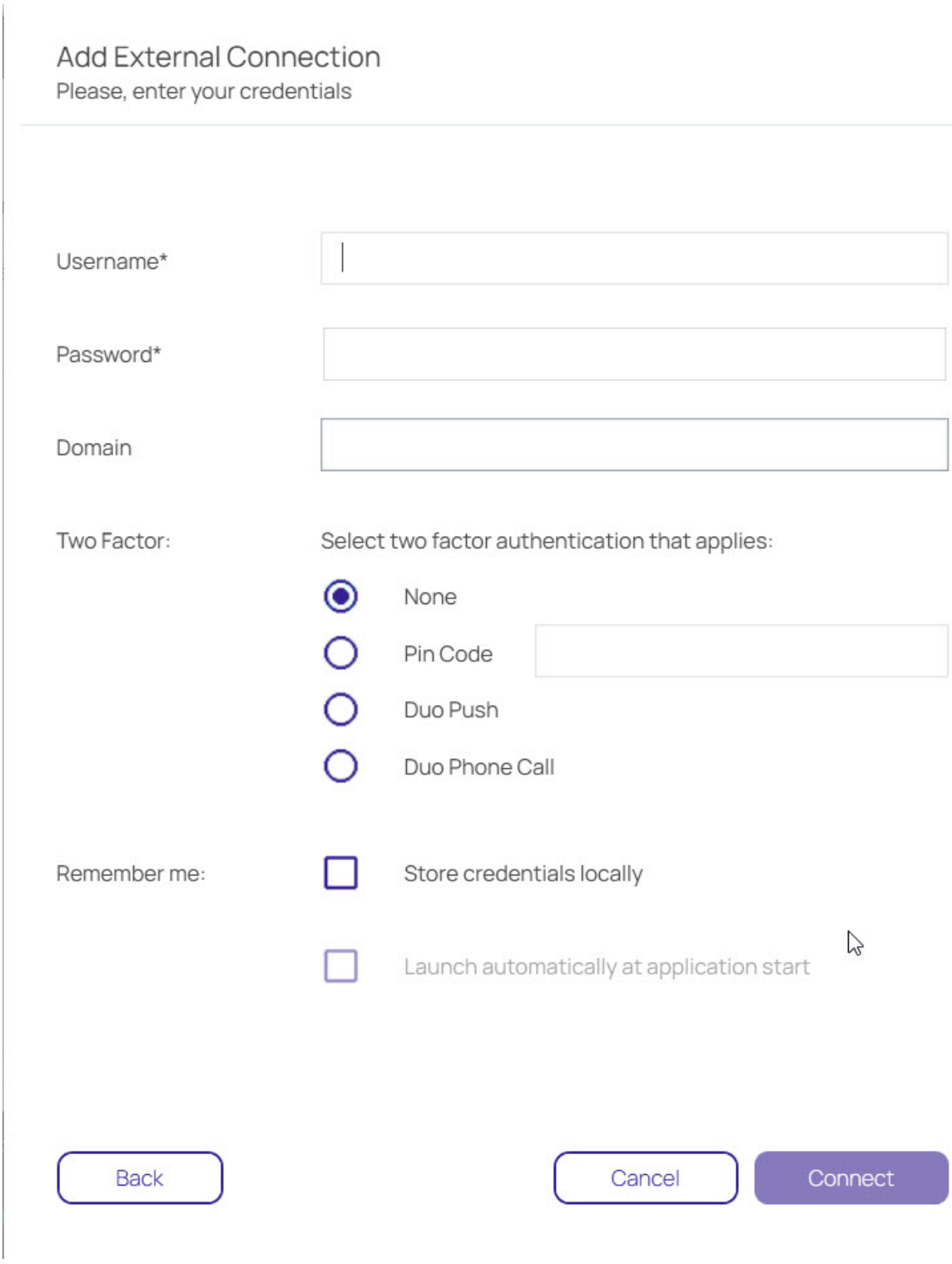
1. In the *Configuration* menu, select **Delinea Vaults**
2. Click **Add Vault**
3. Enter your Secret Server *Connection Name* and *Connection URL* and click **Next**



4. Select **Local Login** from the *Authentication Type* dropdown menu and click **Next**



5. Complete all of the required fields

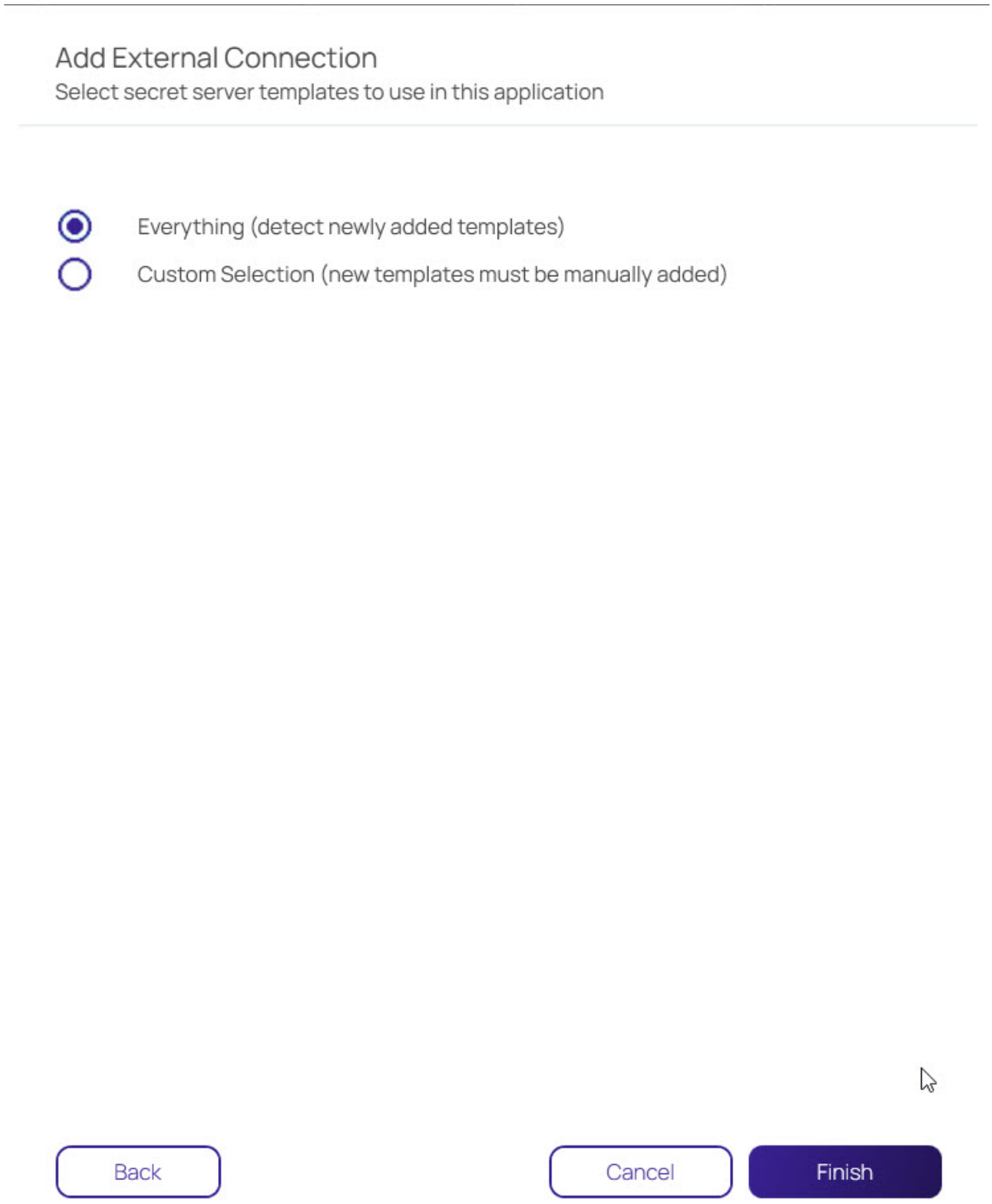

Add External Connection
Please, enter your credentials
Username*
Password*
Domain
Two Factor:
Select two factor authentication that applies:
None
Pin Code
Duo Push
Duo Phone Call
Remember me:
Store credentials locally
Launch automatically at application start
Back
Cancel
Connect

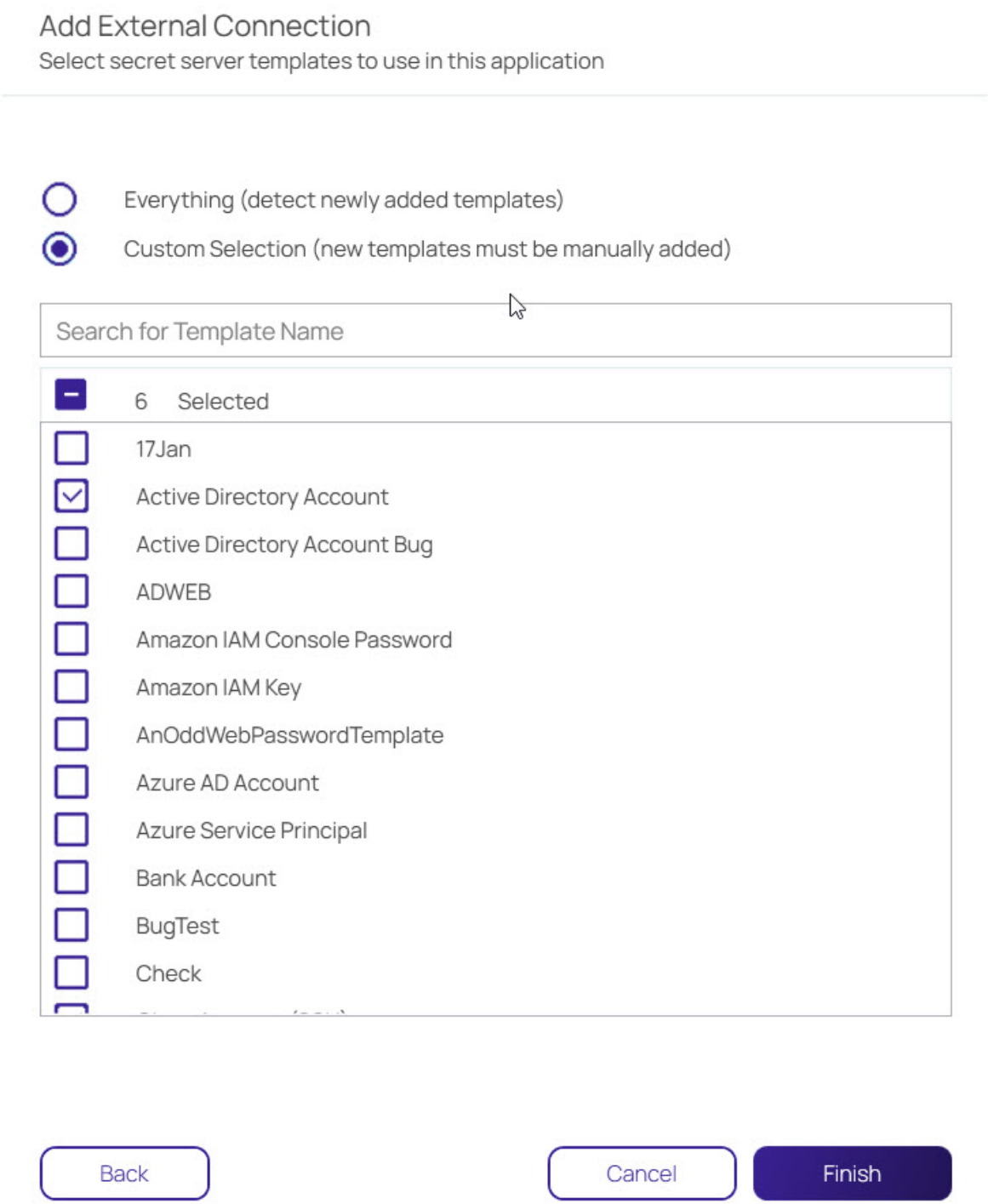
- **Username**: The username for the Secret Server instance to which you want to login. (This is NOT the "username@company.com" format.) * **Password**: The password for the account.* **Domain**: The Secret Server environment. If this environment has been given a specific Domain value for login, enter the same value here. * **Two Factor**: Select the appropriate two-factor authentication option for your environment.

  Note: Connection Manager only supports the Secret Server TOTP Authenticator multifactor authentication option. Email is not supported. * **Remember me**: Select this check box if you want Connection Manager to remember the credentials you entered. This option stores the credentials in local storage and encrypts them using your application password.

  Note: Even if the *Remember me* option is selected, a user will still need to authenticate back to Secret Server when the application launches or times out.

6. Click **Connect**
7. Select the Secret Server templates to use with this vault. You can choose to use all templates or custom selected ones.


Add External Connection
Select secret server templates to use in this application
Everything (detect newly added templates)
Custom Selection (new templates must be manually added)
Back
Cancel
Finish



8. Click **Finish**

Authenticating to a Local Vault

A local vault is an encrypted and password-protected data file saved on the user's machine that stores local connection credentials and passwords.

Local Vault Enabled

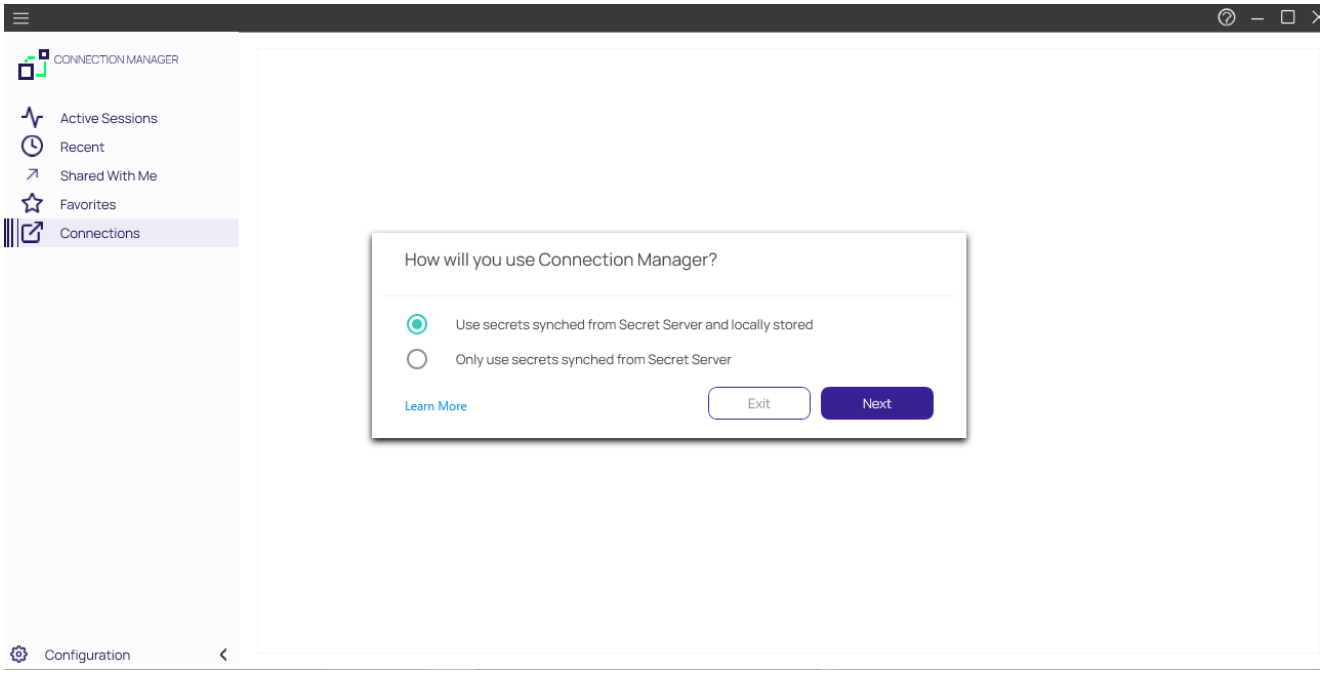
With the local vault enabled, the user can create local RDP and SSH connections, and save the connections and credentials locally. The user must protect this local data by logging into Connection Manager with their password each time they open the application. As soon as the user logs into Connection Manager, they are automatically connected to Secret Server.

Local Vault Disabled

For added security, administrators and users can disable storage of connection credentials and passwords in a local vault. When use of the local vault is disabled, the user cannot create local RDP or SSH connections. When the local vault is already enabled and the user disables it, any existing local connections will be permanently deleted and the user will be able to access only secrets that are synched from Secret Server. The user will not need to log into Connection Manager each time they open the application, but they will need to log into Secret Server when they open Connection Manager.

Enable or Disable Local Vault on Installation or Upgrade

When Connection Manager is installed on a machine for the first time, or when upgrading to version 1.6.0 or higher, the application asks, "How will you use Connection Manager?"



The first choice, **Use secrets synched from Secret Server and locally stored**, enables use of the local vault.

The second choice, **Only use secrets synched from Secret Server** disables use of the local vault.

You can also disable use of the local vault using the command line argument `-disablelocalvault` on installation only (not on upgrade), as follows:

Windows

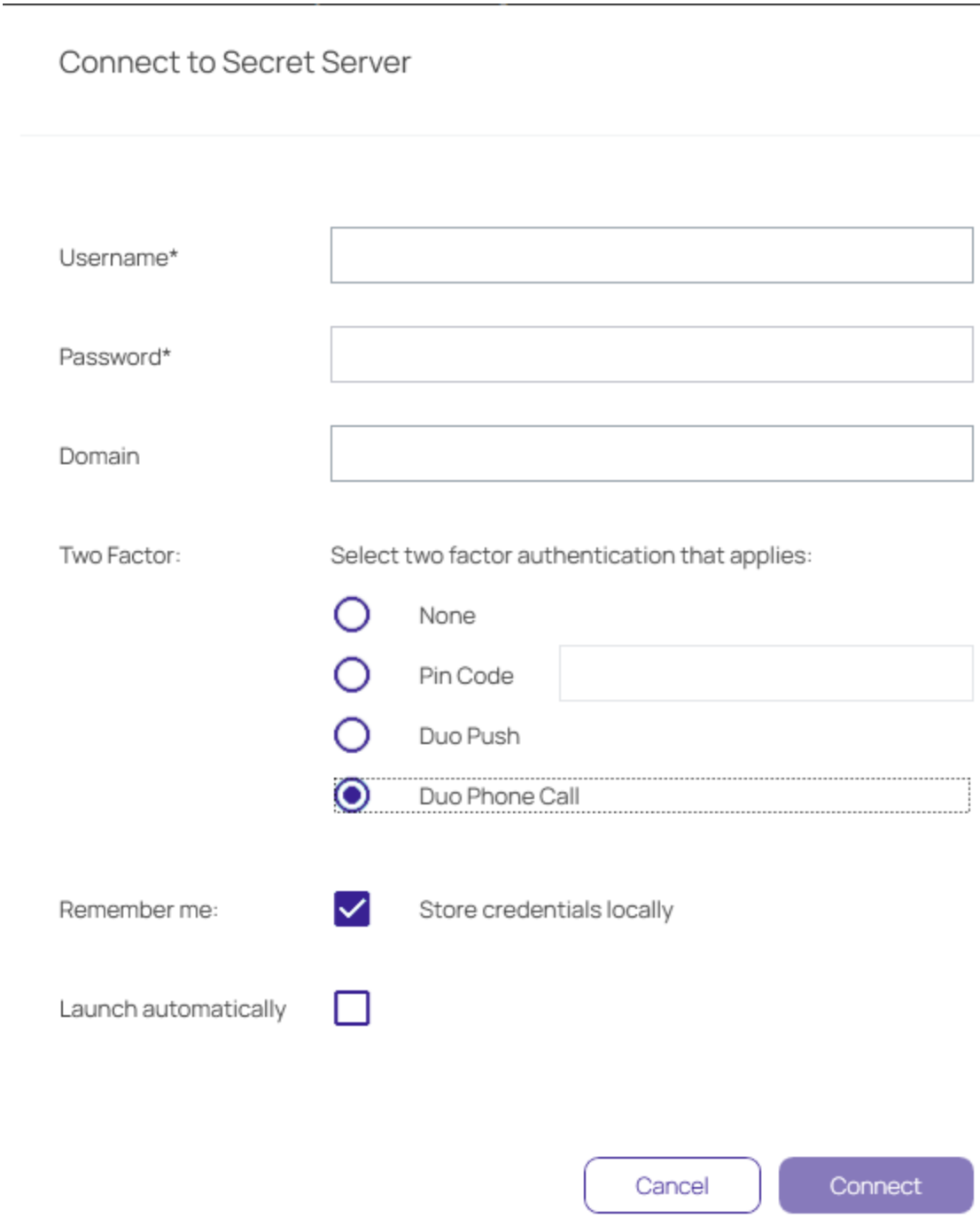
```
Delinea.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS=-disablelocalvault
```

Mac

```
sudo installer -pkg ~/Downloads/Delinea.ConnectionManager.<your version>.pkg -target / &&
open /Applications/Delinea/Delinea.ConnectionManager.app --args -disablelocalvault
```

Enable or Disable Local Vault When Authenticating to Secret Server

In the workflow for connecting to Secret Server, the user can check the box next to **Remember me** to store their credentials to a local vault. To disable the local vault, ensure that the **Remember me** box is unchecked.



Enable or Disable Local Vault at Any Time

To enable or disable the local vault at any time, do the following:

1. From the main Connection Manager screen, click the hamburger icon in the top left corner
2. Click **File**.

3. Click either **Enable Local Vault** or **Disable Local Vault**.

Default Local Vault Location

The default local vault location, on Windows is *C:\Users\User Name\AppData\Roaming\Delinea\Connection Manager*

The default local vault location, on MacOS is */Users/User name/Library/Application Support/Delinea/Connection Manager*

Changing Local Vault Location

Windows

The Delinea.ConnectionManager.exe.config - AppDataFolder user setting can be modified at any time. The changes will be applied after restarting Connection Manager.

Use the `-lspath` argument during installation:

Example command line:

```
"Delinea.ConnectionManager.2.6.0.WindowsInstaller.msi KEYS="-lspath C:/myFolder""
```

Example PowerShell:

```
.\Delinea.ConnectionManager.exe /quiet RUNCM=runCM KEYS='"-lspath C:/myFolder""
```

MacOS

Update the `Env.DataLocation` variable to set local vault location.

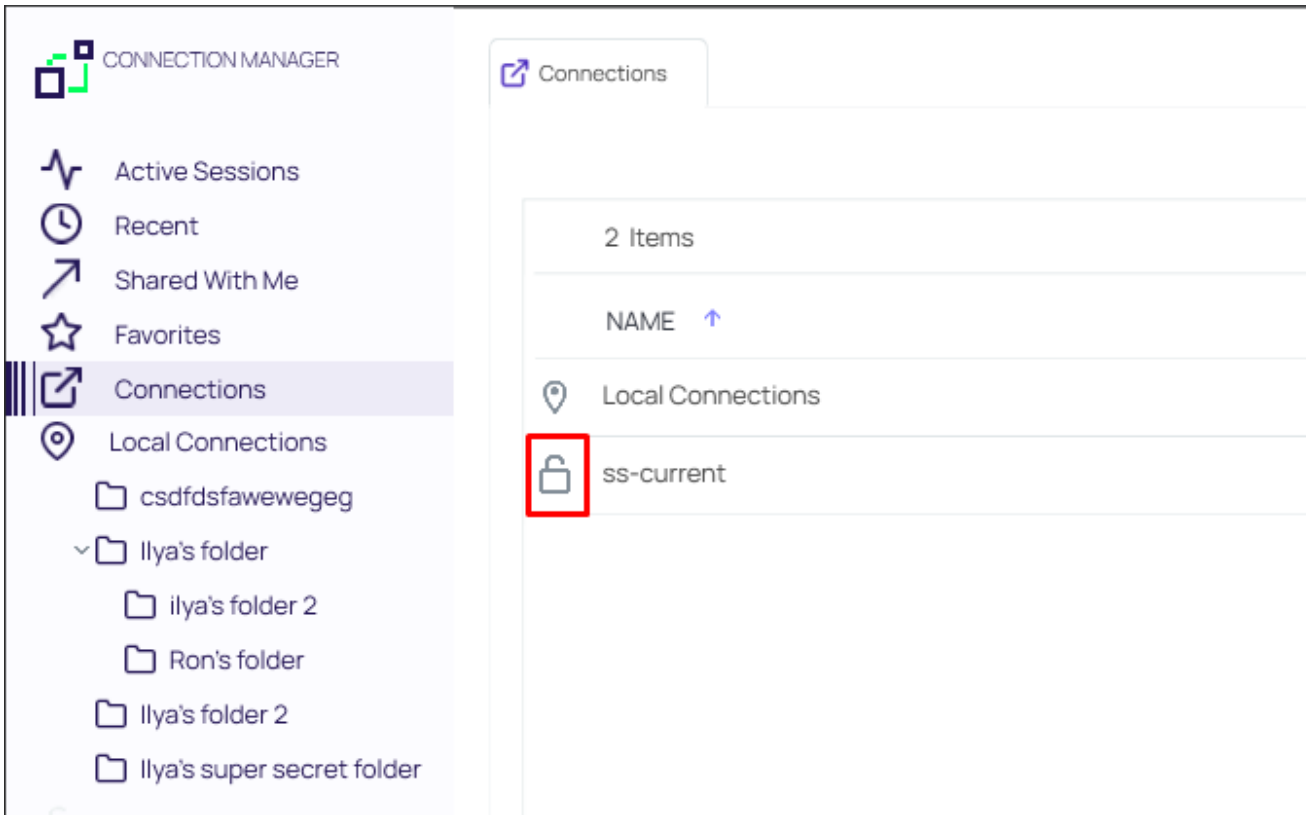
Note: If you decide to change the location of the local vault, you will also need to copy the *ConnectionManager.dat* file to your new local storage location in order to keep your original vault configuration.

Re-authenticating to a Vault

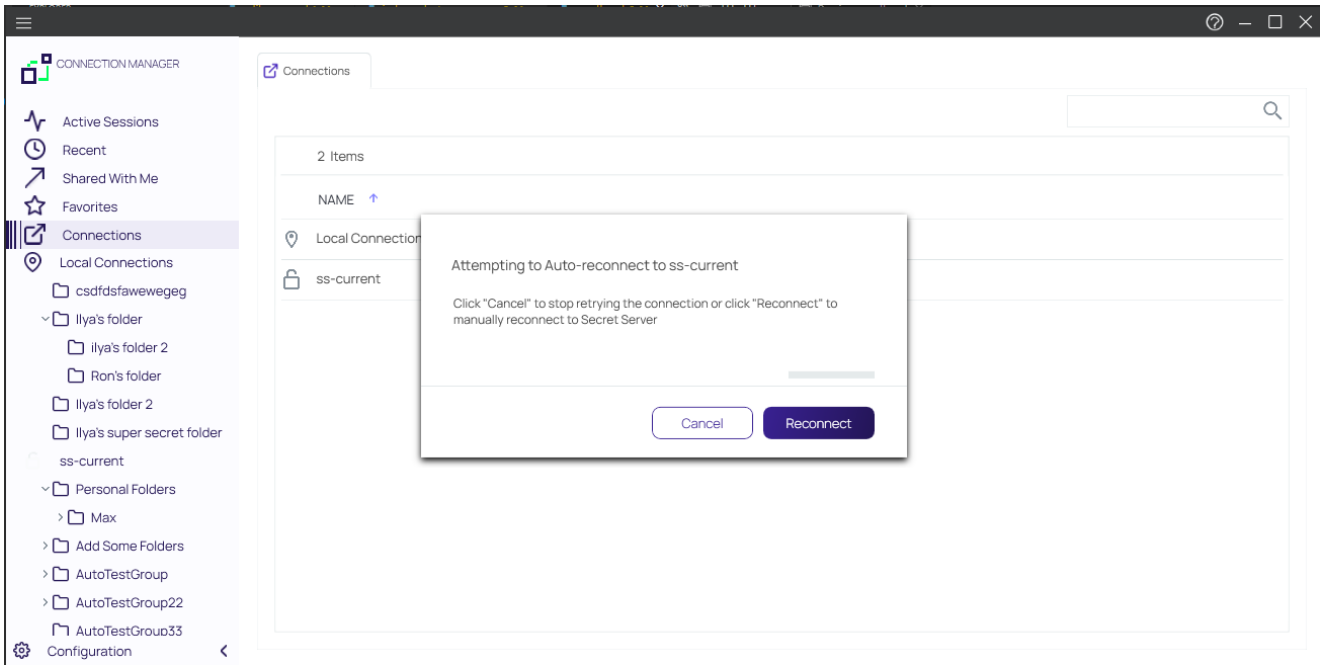
Note: When Connection Manager starts, the configured Secret Server connection are displayed under the Connections tab, but they are **not** connected.

To reauthenticate an existing Secret Server connection, either:

- Double-click the **closed-lock icon** in the navigation menu, or
- On the Connections page, in the list right-click the connection you wish to open and select **Connect**.



If you lose your internet connection to Secret Server, Connection Manager makes multiple attempts to automatically reauthenticate to Secret Server in the background. After 30 seconds, Connection Manager displays the dialog, **Attempting to Auto-Reauthenticate to [Secret Server name]** for three more minutes and continues to attempt to reauthenticate. The dialog displays a **Cancel** button for users who wish to drop the connection, and a **Reauthenticate** button for users who wish to attempt to manually attempt to reauthenticate. If at any time during this period the Secret Server connection is regained, Connection Manager automatically reauthenticates. If the period passes without reauthenticating to Secret Server, the dialog closes, the Connect dialog opens, and the user must reauthenticate through Connection Manager when reauthenticating to Secret Server.

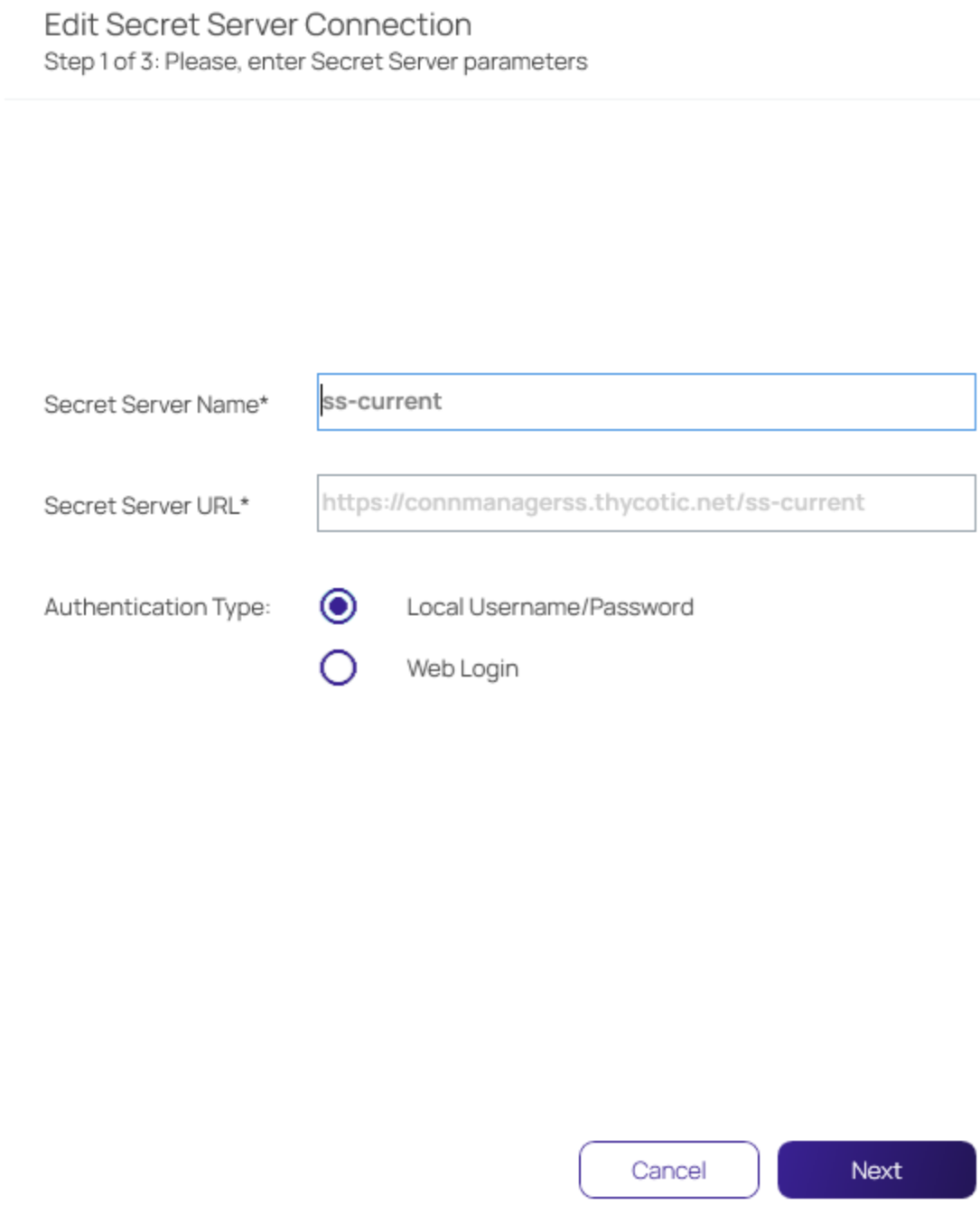


Important: Reauthentication will not work if the session was launched via protocol handler from the browser. Connection Manager was designed to handle sessions that were launched in browsers, such as "Launch" and "Forget". In this case, Connection Manager does not have access to any Secret Server parameters, proxies or credentials not stored and not accessible after running sessions. This was done as a security measure. For Connection Manager to reauthenticate, it needs to have access to the secret, which is why it is recommended that users run sessions under Connection Manager.

Modifying a Vault

Existing connections to Secret Server can be modified. Most fields can be modified except for the Secret Server URL field:

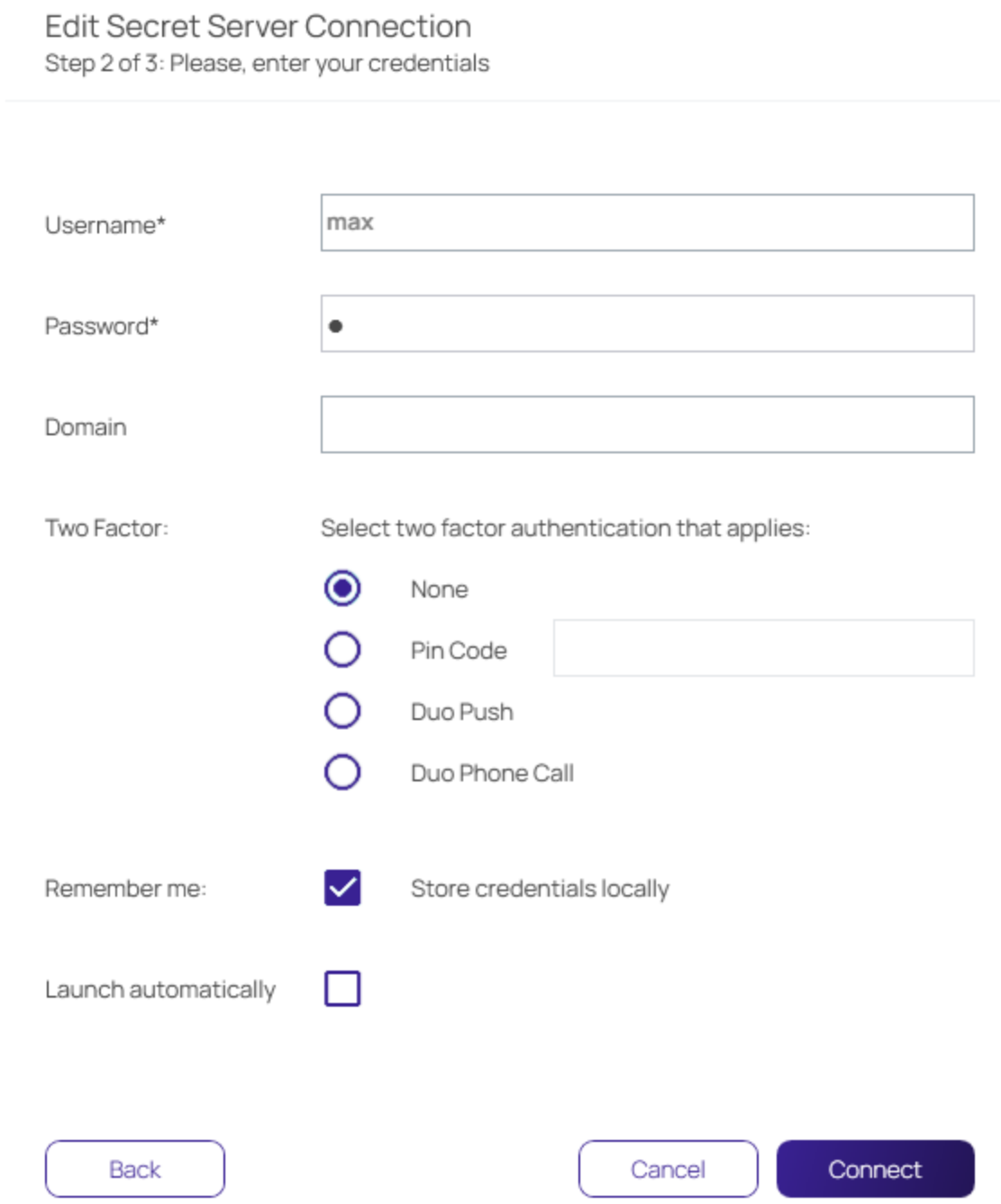
1. On the Configuration menu, select **Secret Server Connections**. The Secret Server Connections window opens.
2. Click **Edit** next to the Secret Server connection to be modified. The Edit text is between the Connection name and the URL value. The Connection dialog box opens.



Note: Users can make modifications to any of the fields here except for the Secret Server URL. If the *Remember me:* option was selected previously, the user will not be able to change the Username value either.

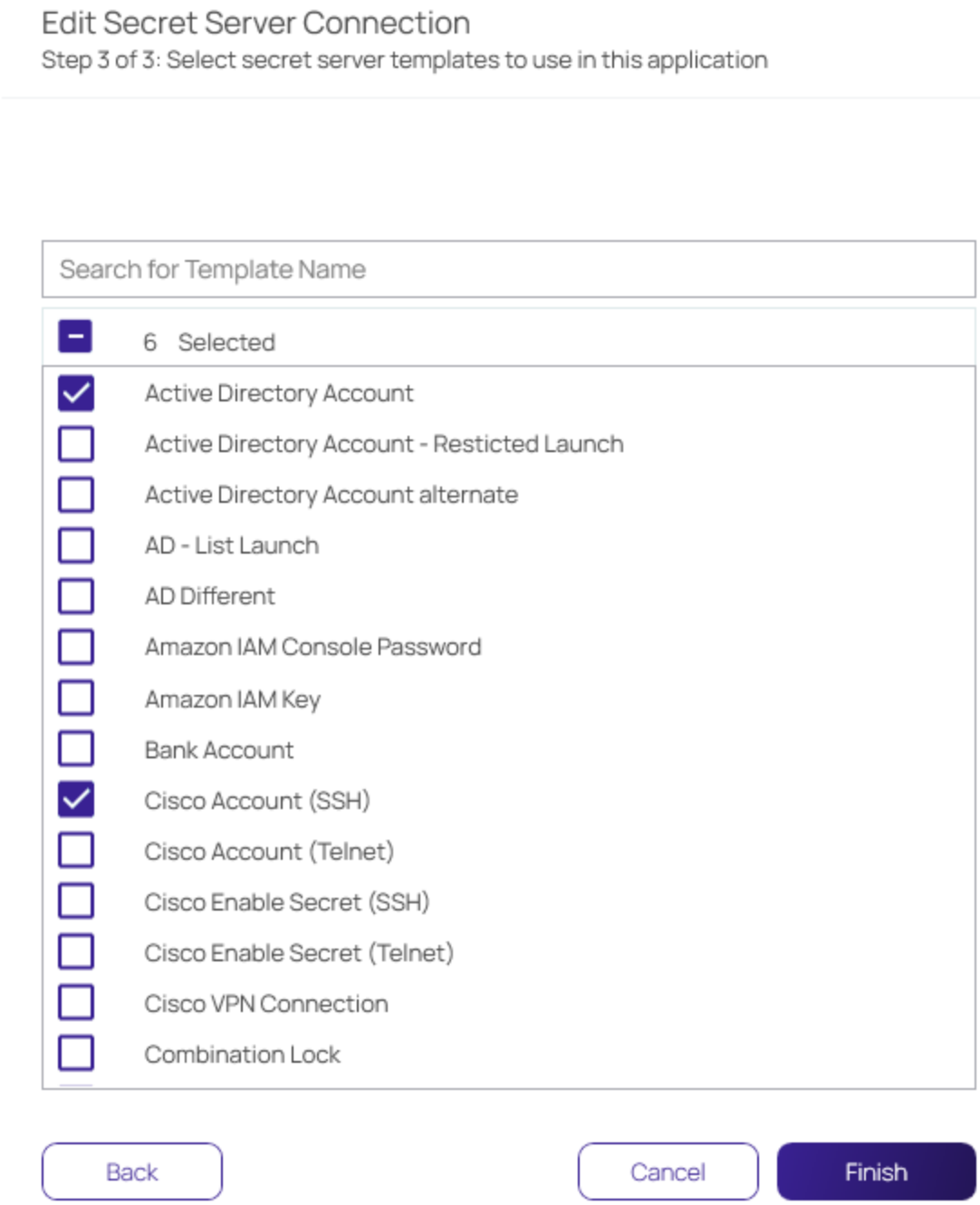
Input the Secret Server Name, URL and Authentication Type and click **Next**.

3. The system will prompt you to input your Username and Password credentials. Click **Connect** when finished.



4. Make any desired changes in Step 3 and click **Finish**.

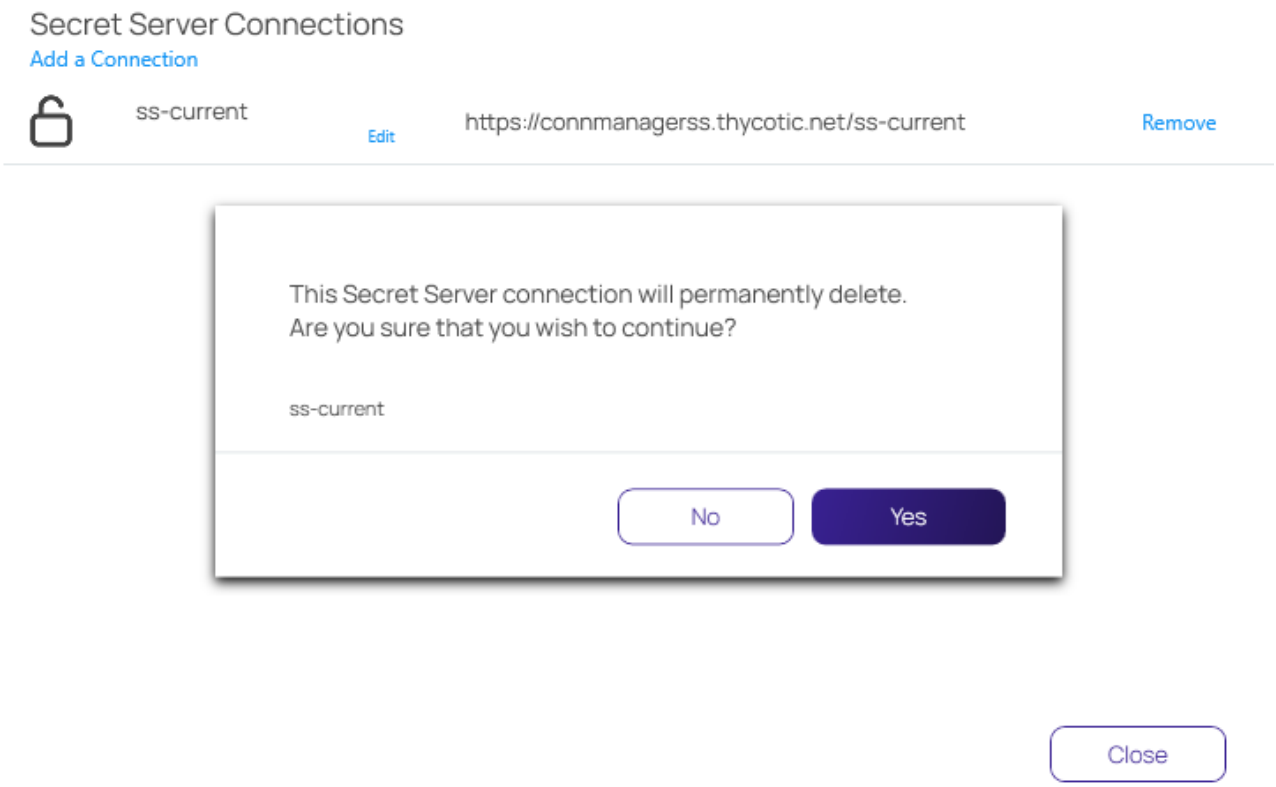
> **Note:** A user may modify template selections at any time by selecting **Edit** next to the Secret Server connection as shown below.



Removing a Vault

To remove a vault:

1. On the Configuration menu, select **Secret Server Connections**. The Secret Server Connections window opens.
2. Click the **Remove** text to the far right of the Secret Server connection to be removed. A warning prompt will ask you to confirm.



3. Click **Yes** to confirm.

Session Connections

This section contains information about:

- "Remote Systems " below
- "Integrated Connections" on page 91
- "Importing and Exporting Connections" on page 95

Remote Systems

This section contains information about:

- "Creating Connections" on the next page
- "Opening Connections" on page 84

- "Editing Local Connections " on page 86
- "Deleting Connections " on page 90
- "Duplicating Connections" on page 91

Creating Connections

Connection Manager allows users to create new connections to remote systems and store them locally. Secret Server secrets may only be viewed and initiated within Connection Manager.

All required fields and the appropriate optional fields must be filled out. If you choose not to enter a username and password, you will be prompted to enter this information when connecting. Many of the fields will have default values pre-entered. You may keep these values or modify them as appropriate.

1. From the Local connections section of the navigation tree, navigate to the folder where the new connection will be created.
2. Right-click the **folder name** and select **New Connection** followed by the **connection type** (RDP or SSH).

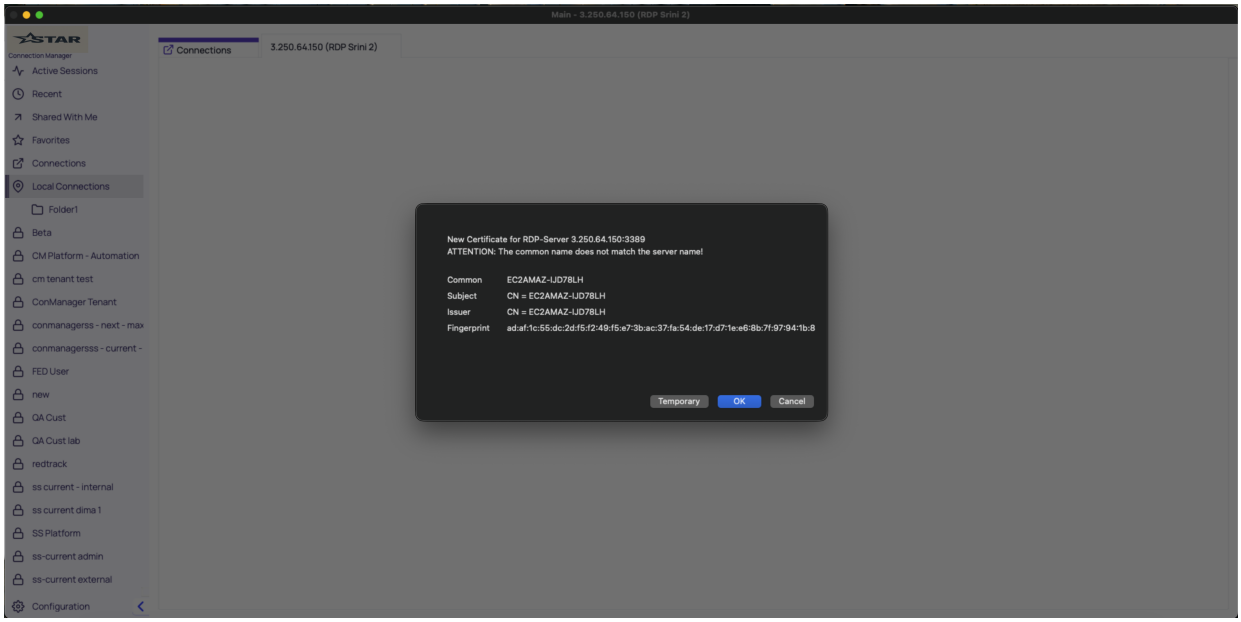
   Depending upon the connection type (RDP or SSH), a dialog box will open. The options will vary based on the type of connection selected. View "Integrated Connections" on page 91 for additional information on credentials.

   RDP Connection

   - **Connection Name**: Enter a friendly name for the new connection.
   - **Computer Name**: Enter the unique identifier for the computer name or IP address.
   - **Port**: Enter the port number for the connection or leave default.
   - **Credentials**: Select the appropriate credential for the new connection.

     When connecting to the RDP server for the first time, you can view the RDP server's certificate details and

approve the certificate:



SSH Connection

- **Connection Name**: Enter a friendly name for the new connection.
- **Computer Name**: Enter the unique identifier for the computer name or IP address.
- **Port**: Enter the port number for the connection or leave default.
- **Credentials**: Select the appropriate credential for the new connection.

Note: The default value settings may be modified under the Configuration option.

3. Once all appropriate information is added, click **Create** to add the connection.

Important: Connection Manager does not support reauthentication for secrets enabled with proxies, checkout or session recording. If the connection to the server is lost, Connection Manager will terminate the session.

Opening Connections

The process of connecting to a Local connection or to a Secret from Secret Server is essentially the same.

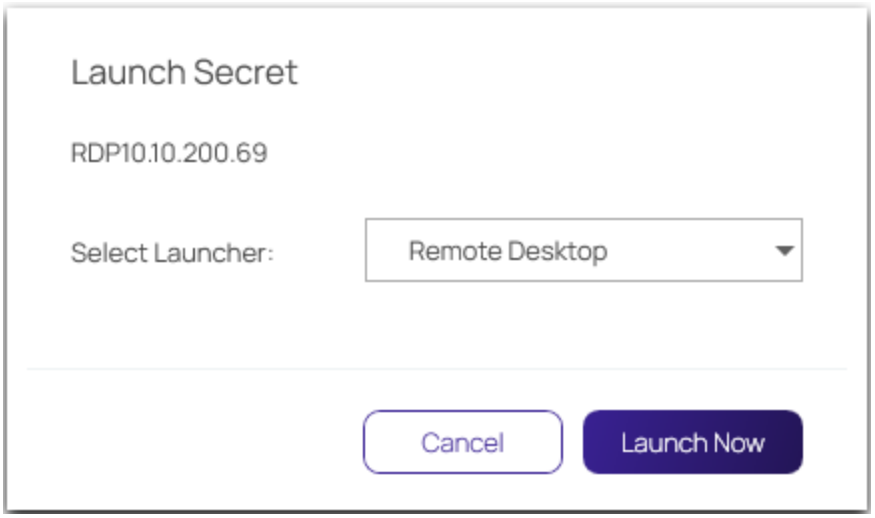
1. Navigate to the remote connection. The remote session can be opened two ways:
   - In the main window, double-click the connection name. A new connection tab will open, or
   - Select the connection to open the Properties tab. In the bottom half of the Properties window there is a section that lists available Launchers for use. Click the desired launcher and the session will open.

     Sessions launched from a Secret Server Secret may have workflows associated with the launching or closing of a session. If the connection requires no special workflow, the remote connection will be

established as a new tab in the work area. If user entry is required for a workflow action, a window(s) will open prior to connecting so users can enter the appropriate or required data.

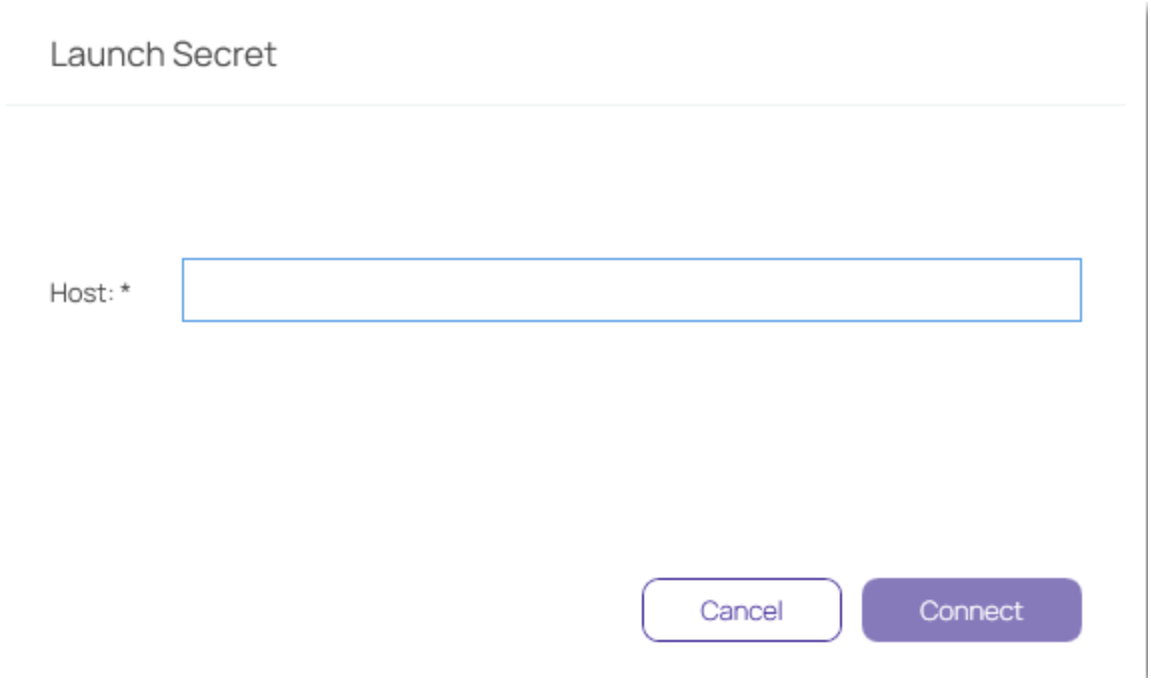
Note: When connecting to a Secret with an Allowed List, users will be prompted to enter a text value if the list is empty.

2. Select a launcher. For Secrets where multiple launchers are available, you are prompted to select one.



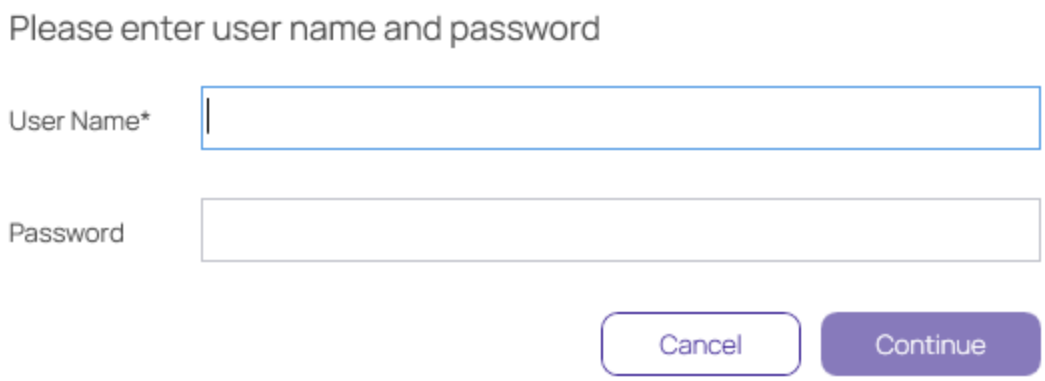
Click **Launch Now**.

3. Select a **Host** or **Machine ID**. For Secrets where a host is not specified, you are prompted to enter a host machine name into a search box. As soon as enough characters are typed to generate at least a partial match, Connection Manager returns matching machines.



Click **Connect**.

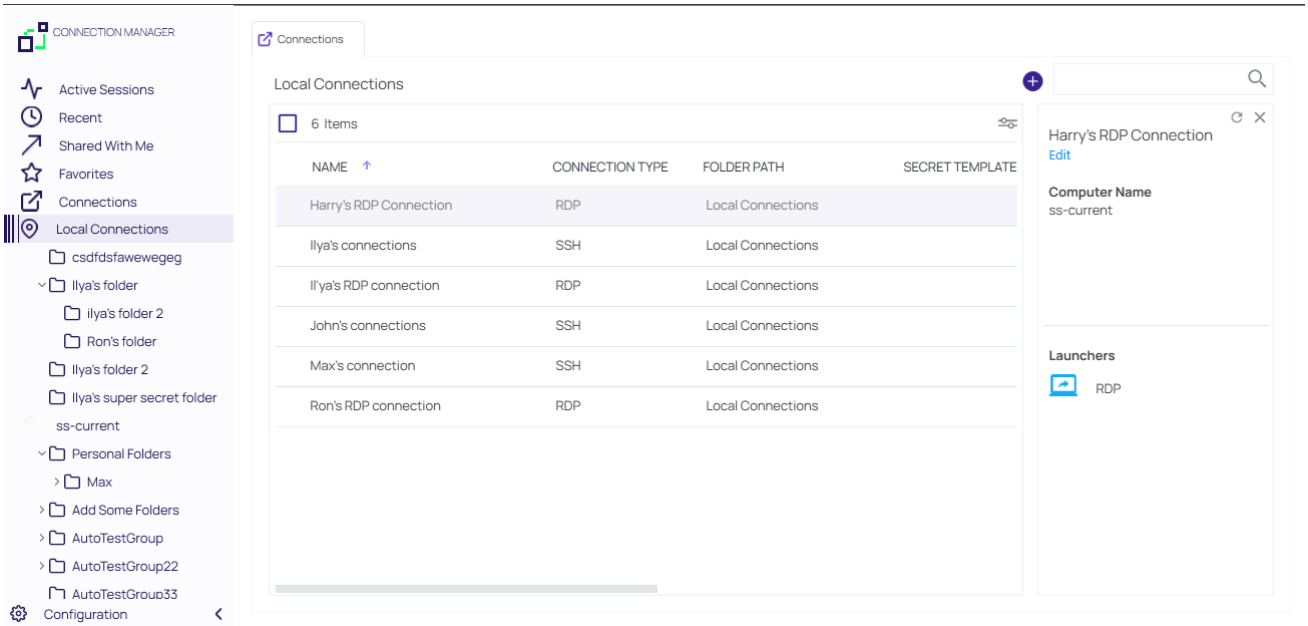
4. Enter user credentials. For Connections or Secrets without an embedded username and/or password, a modal opens (based on launcher type) to enter credentials.



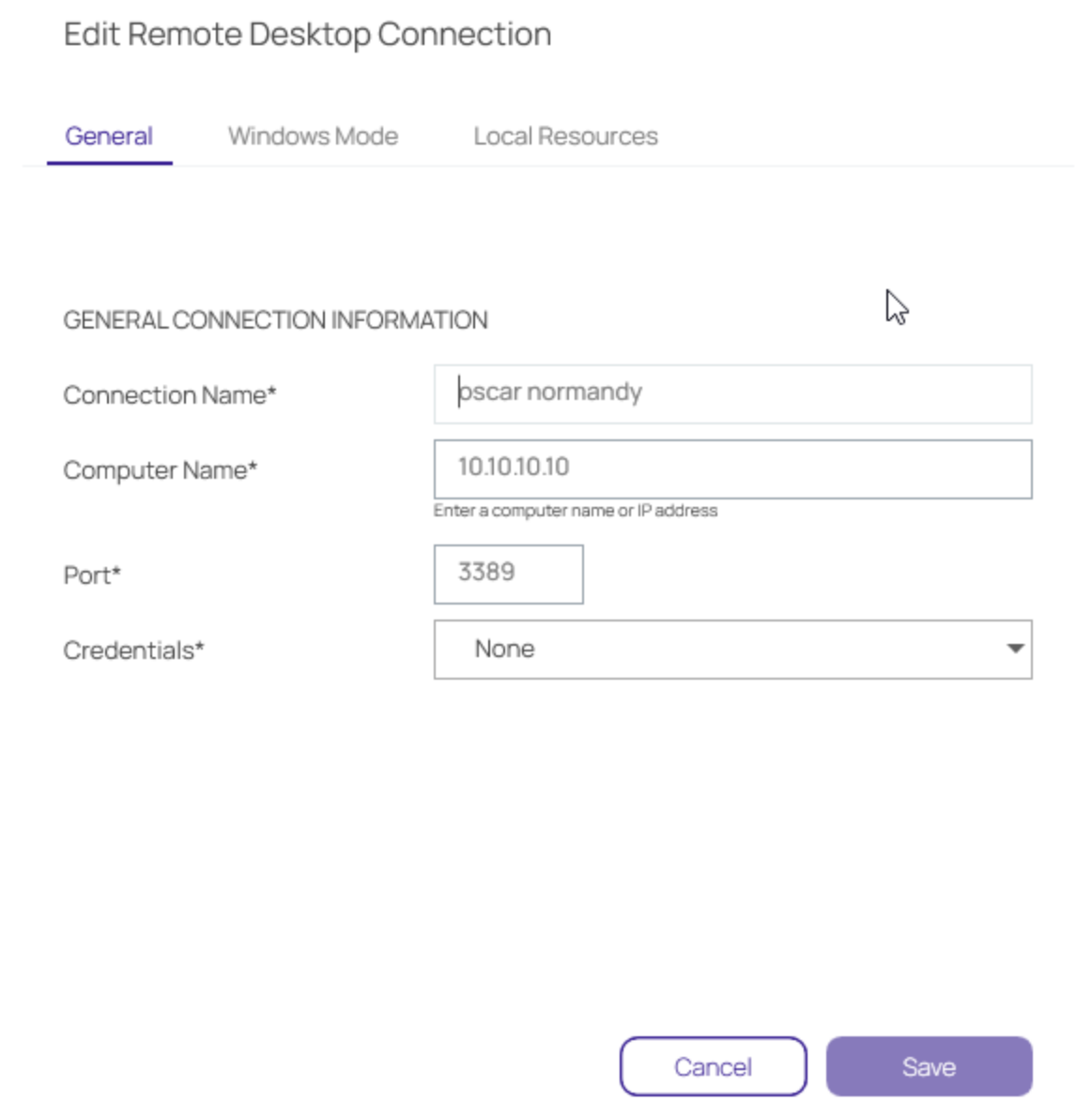
Click **Continue**.

Editing Local Connections

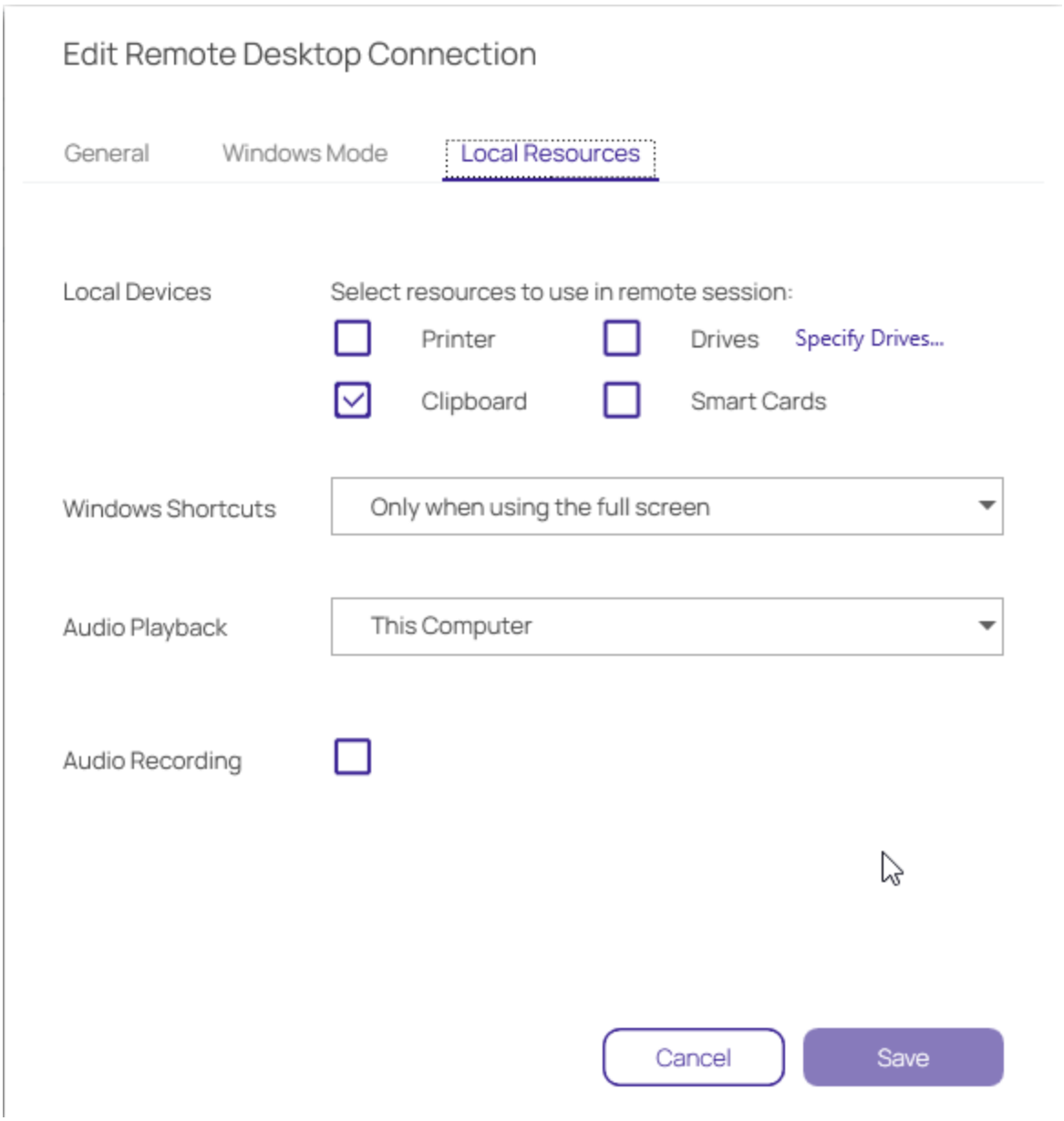
1. Navigate to the connection to be edited and click the connection name.



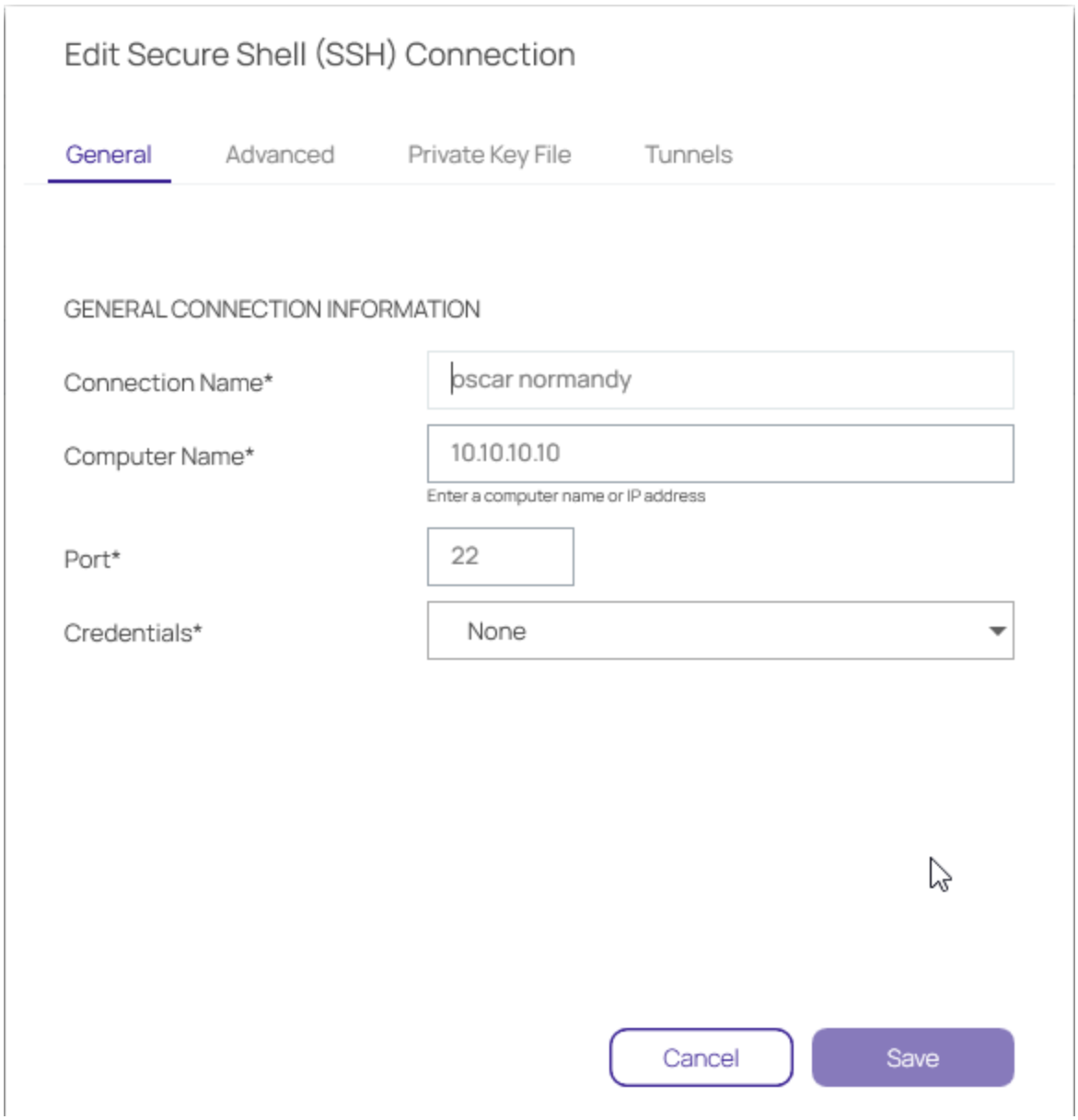
2. In the Connection properties area under the connection name, click **Edit**. An Edit dialog will open depending on the connection type.



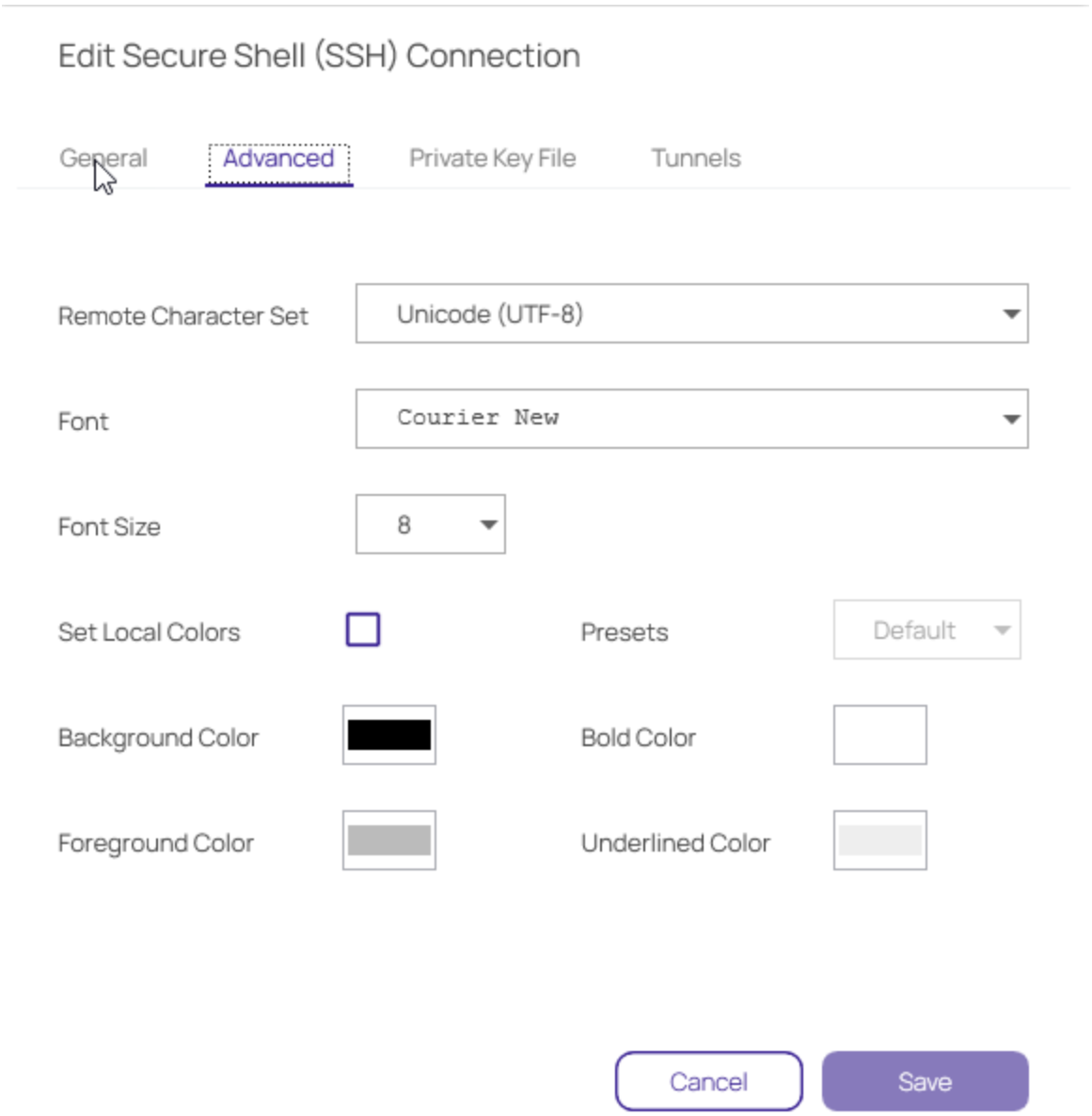
In the Local Resources tab, you can edit the resources for RDP connections:



For SSH connections, you will see the following window:



In the Advanced tab, you can edit the color schema and font size:



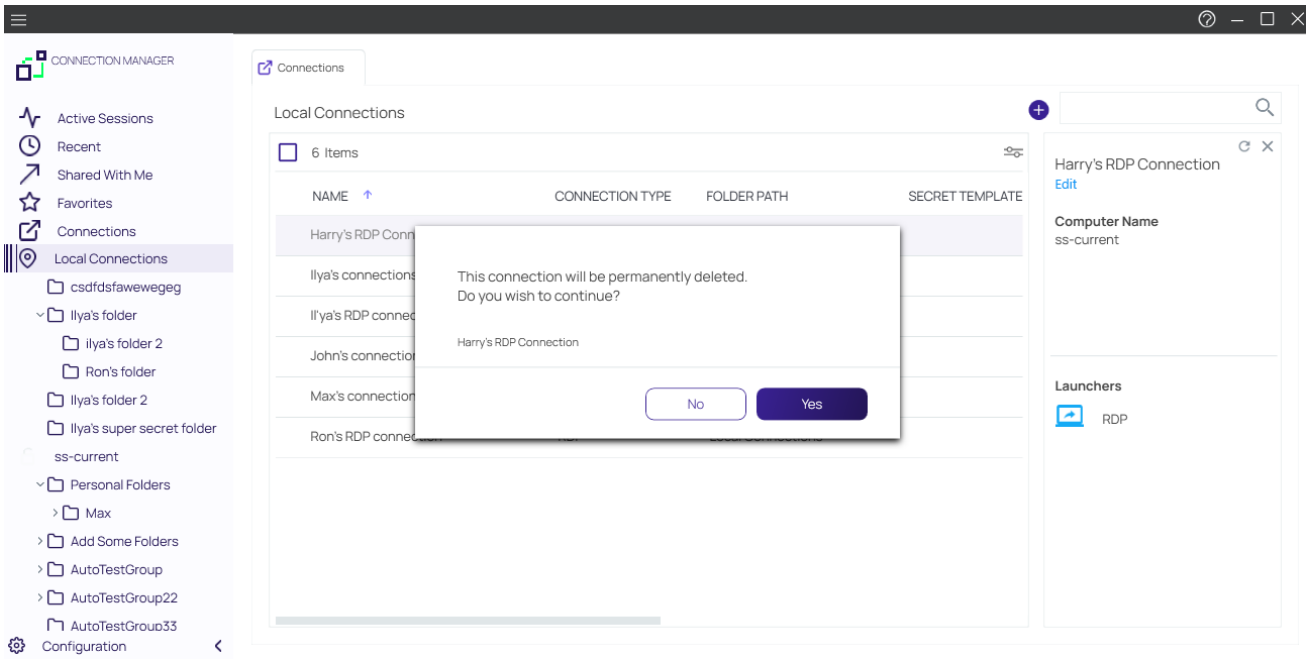
3. Modify the fields as desired. (Most values in a local connection may be edited, except the required fields and the username field.)
4. Click **Save** when finished.

Deleting Connections

A Local connection may be deleted from Connection Manager

Important: This action is **NOT** reversible. Once a connection is deleted it cannot be recovered.

1. Navigate to the connection to be removed.
2. Right-click the connection and select **Delete**. A confirmation modal opens.



3. Click **Yes** to confirm.

Duplicating Connections

1. Navigate to the connection you wish to duplicate and right-click the connection.
2. From the right-click context menu, click **Copy**. The connection is copied to your clipboard.
3. Right-click the Connection Manager screen and from the context menu, click **Paste**. The duplicate connection is added to the connections on the Connection Manager screen.
4. Edit the Connection name and other parameters as desired.

Integrated Connections

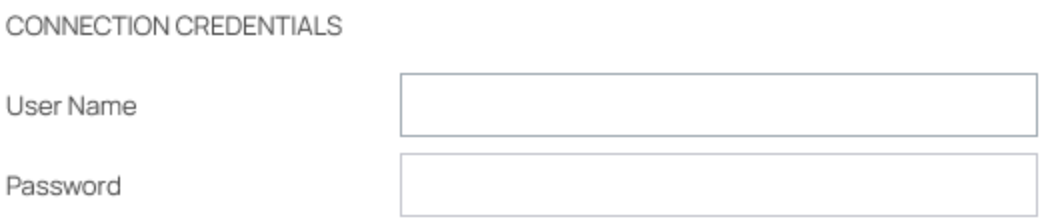
When logging into Connection Manager, if there are no existing Secret Server connections, a user will be directed to the Create a Secret Server Connection dialog box as shown in the Authenticate to Secret Server section.

Credentials

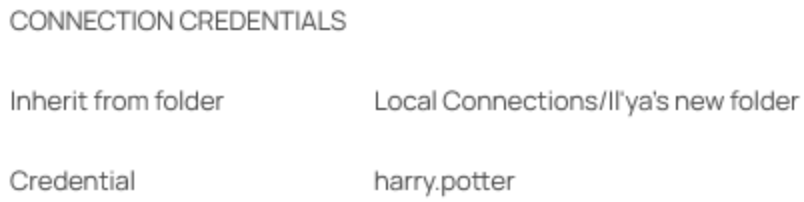
Users can apply credentials directly to new folders and connections and at the same time, ensure all sub-folders inherit the same credentials.

- **None**: Allows a user to create new folders and connections without any credentials – i.e. no username and password values. This can be changed later.

- **Local Credentials**: Allows a user to apply username and password credentials to the new folder or local connection.



- **Inherit from Folder**: Allows a user to apply credentials or a secret to a folder or connection to imitate the folder in which it will reside, or any sub-folders or connections created within it. While making the connection, if a connection already exists, it will be displayed.



- **Map Secret**: Allows a user to apply secrets to the new folder or connection.



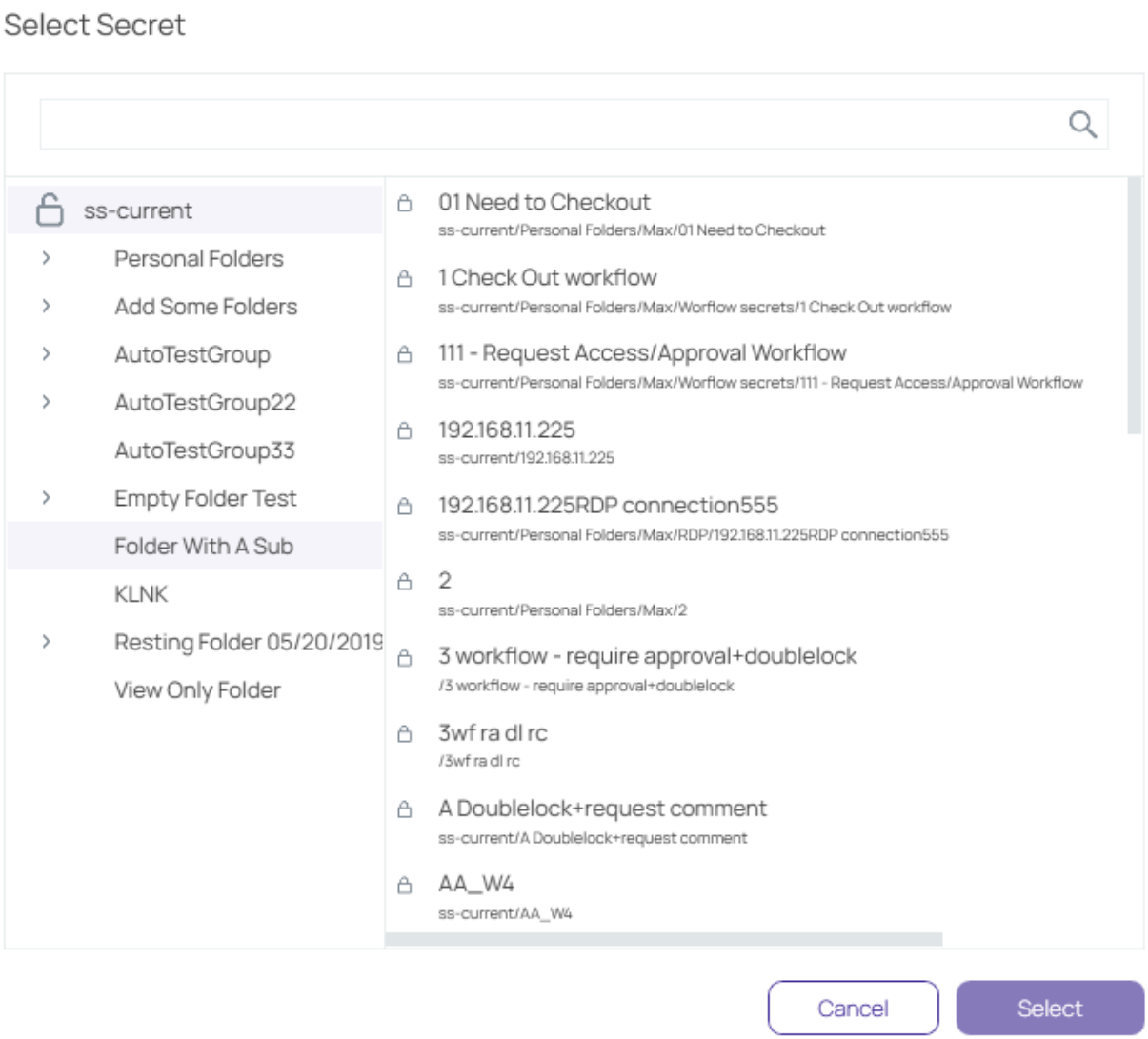
Map a Vault Secret to a Folder

Connection Manager gives a user the ability to map secrets directly to folders.

Note: The process is the same whether the connection is RDP or SSH.

Important: For mapped secrets with a proxy enabled, Connection Manager selects the target host from the local secret. In previous versions, the target hosts were selected from the secret on the server.

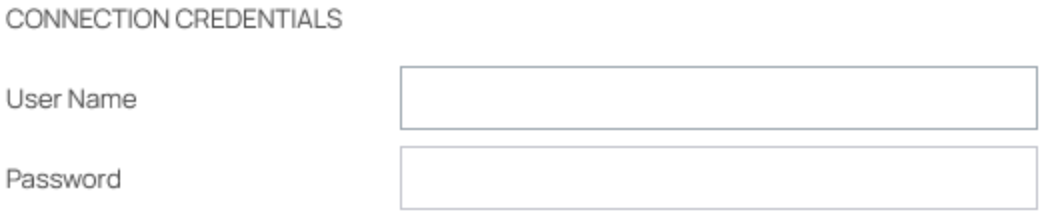
1. From within Connection Manager, create a new folder or edit an existing folder. The Create a Remote Desktop Connection dialog box opens.
2. Enter the **connection name**, **computer name**, **port**, and from Credentials, select **Map Secret**. The Select Secret dialog box opens.



The Select Secret dialog box shows the currently existing connections. Those that are authenticated and accessible, are shown with an open lock next to the name. A closed lock indicated authentication is required, generally a username and password. Users can drill-down the navigation tree to access more folders.

Users may also search for a secret by name using the search bar at the top of the Select Secret window. Clicking on a connection and then typing in the search box will search only the folders within that connection.

3. Click the **Secret** to which you would like to map and click **Select**. The name of the secret will now appear within the Create a Remote Desktop Connection dialog box under Connection Credentials.



4. Once all required information is entered, click **Create**.

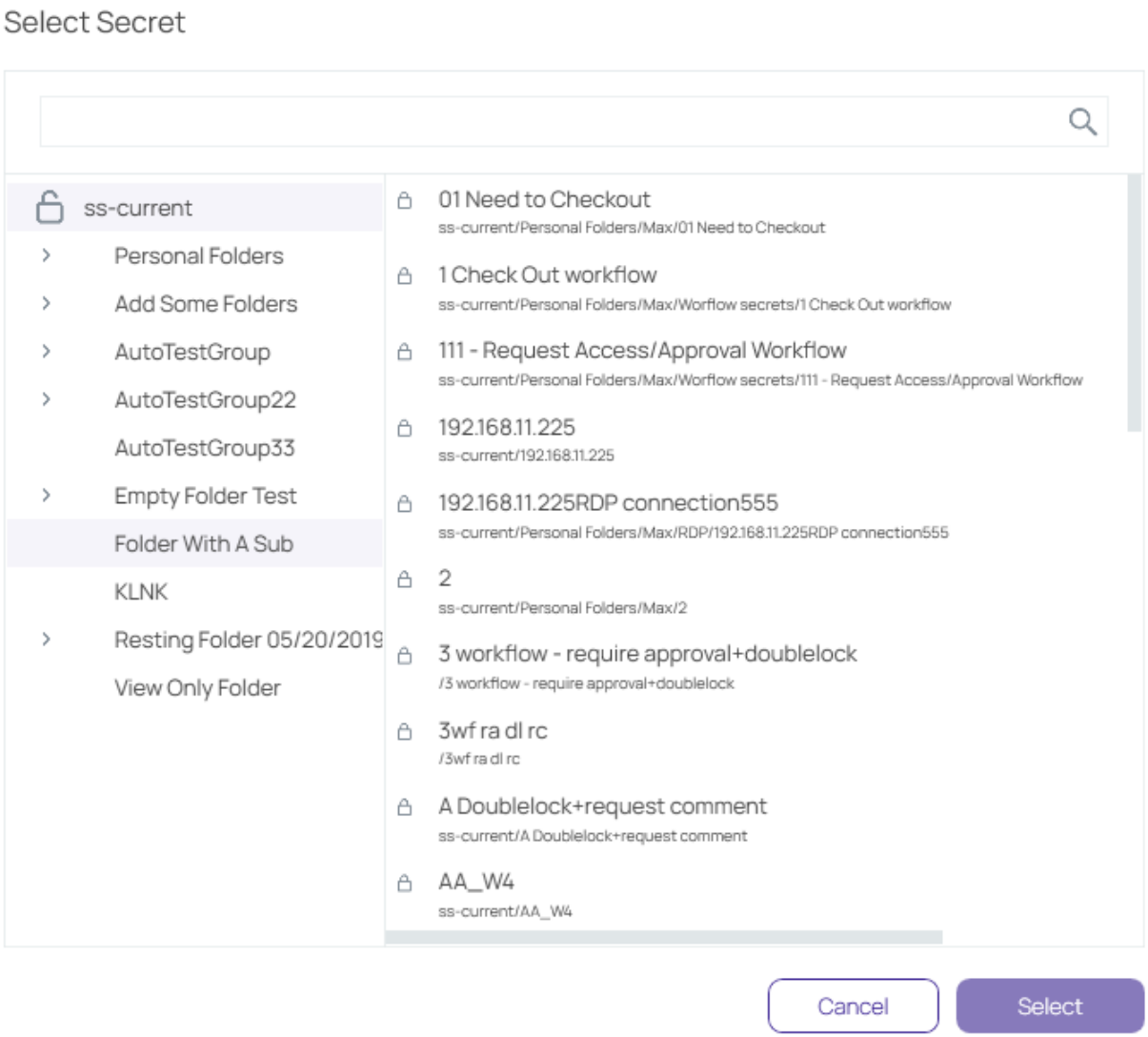
Map a Vault Secret to a Connection

Connection Manager gives a user the ability to map secrets directly to connections.

Note: The process is the same whether the connection is RDP or SSH.

Important: For mapped secrets with a proxy enabled, Connection Manager selects the target host from the local secret. In previous versions, the target hosts were selected from the secret on the server.

1. From within Connection Manager, go to "Creating Connections" on page 83 or "Editing Local Connections " on page 86. The Create a Remote Desktop Connection dialog box opens.
2. Enter the **connection name**, **computer name**, **port**, and from Credentials, select **Map Secret**. The Select Secret dialog box opens.



The Select Secret dialog box shows the currently existing connections. Those that are authenticated and accessible, are shown with an open lock next to the name. A closed lock indicates authentication is required, generally a username and password. Users can drill-down the navigation tree to access more folders.

Users may also search for a secret by name using the search bar at the top of the Select Secret window. Clicking on a vault and then typing in the search box will search only the folders within that vault.

3. Click the **Secret** to which you would like to map and click **Select**.
4. Click **Save.**
5. Your secret is now mapped to a connection.

Importing and Exporting Connections

This section contains information about:

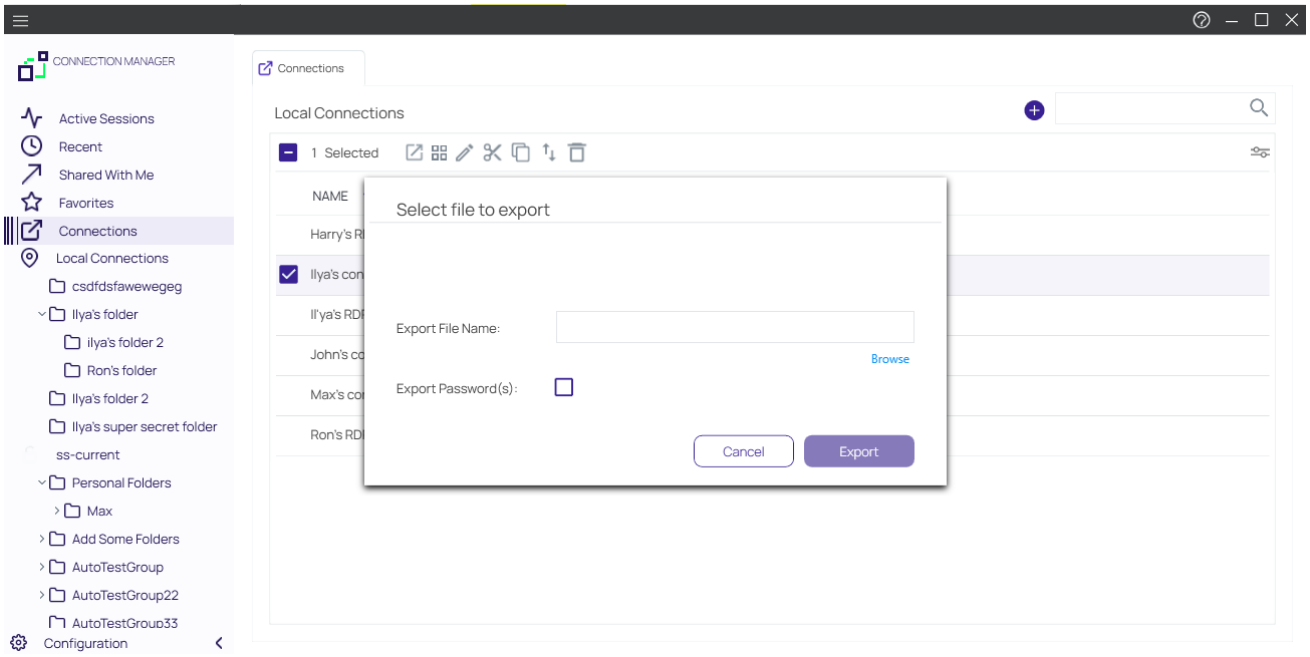
- "Exporting Connections" below
- "Importing JSON Files" below
- "Importing Devolution Files" on page 98
- "Importing RDG Files" on page 100
- "Importing RDP Files" on page 101
- "Importing CSV Files" on page 105

Exporting Connections

Export allows users to export all local connections. When a folder is selected, the contents of that folder, along with any subfolders (and their contents), are included in the export file.

To initiate an export, follow these steps:

1. On the Navigation menu, click the **desired folder or connection** under the Local connection section. Alternatively, the Local Connection or folder may be selected in the main window.
2. Right-click and select **Export**. The **Select file to export** window opens.



3. Click **Browse** and enter **the location and file name** for export.

   Note: If Export Password(s) is selected, passwords for the connections are exported in **clear text**.
4. Click **Export** to complete the action.

Importing JSON Files

The Import option is only available for Local connections and can only be accessed from the Navigation tree.

To initiate an import, perform the following:

1. On the Connection Manager navigation tree, select the **Local Connection folder** to which the contents should be imported.
2. Right-click and select **Import**. A file browser window opens.
3. Navigate to the location of the .JSON file containing the content for import.
4. Select the .JSON file and click **Open**. The Connections are imported.

JSON Example

The contents of any Export or Import file is in JSON format. The following is an example of the formatting:

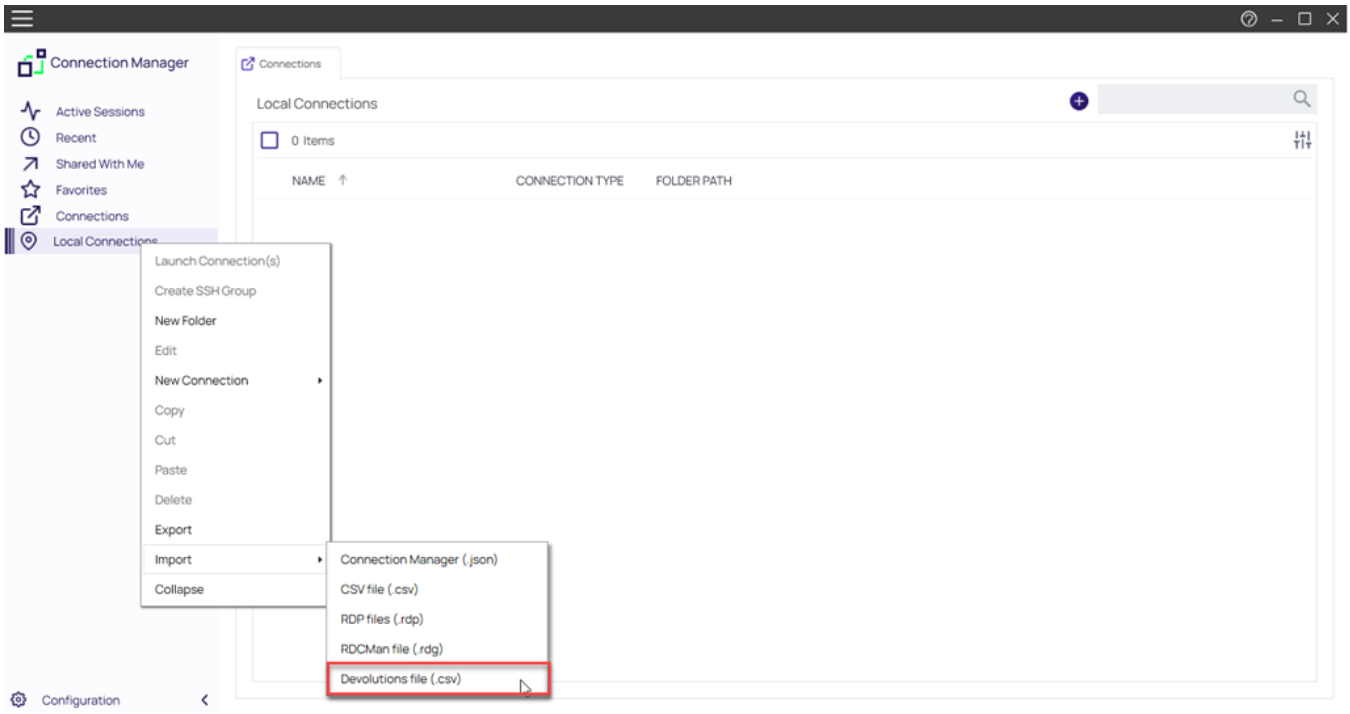

```
{
"SchemaVersion": "1.0",
"Folders": [
 {
  "Id": "abcde123-456f-7890-12g3-456h78ij9kl0",
  "Name": "Folder1"
 },
 {
  "Id": "bgh9fkf5-771s-6218-6v8-z2ph441w0rr2",
  "ParentFolderId": " abcde123-456f-7890-12g3-456h78ij9kl0",
  "Name": "SubFolderA"
 },
   }
],
"Secrets": [
 {
  "Name": "Connection1",
  "Type": "Rdp",
  "ParentFolderId": " bgh9fkf5-771s-6218-6v8-z2ph441w0rr2",
  "ComputerName": "MachineName",
  "Port": "3389",
   "UserName": "UserA"
  "Password": "PasswordInClearText"
 },
]
}
```

Note: The red text for the password field indicates that this part of the JSON file will only be included if the Export Password(s) option is used.

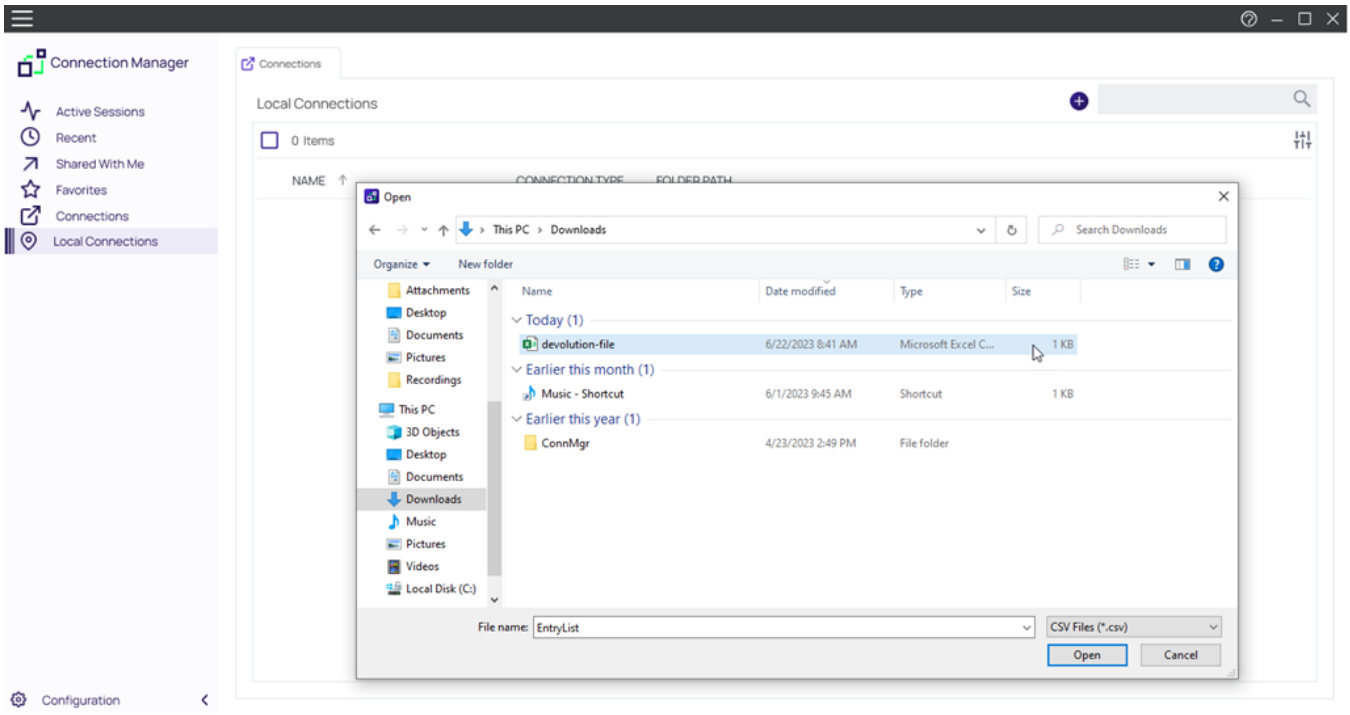
Importing Devolution Files

Connection Manager supports the import of Devolution files. To import a Devolution file:

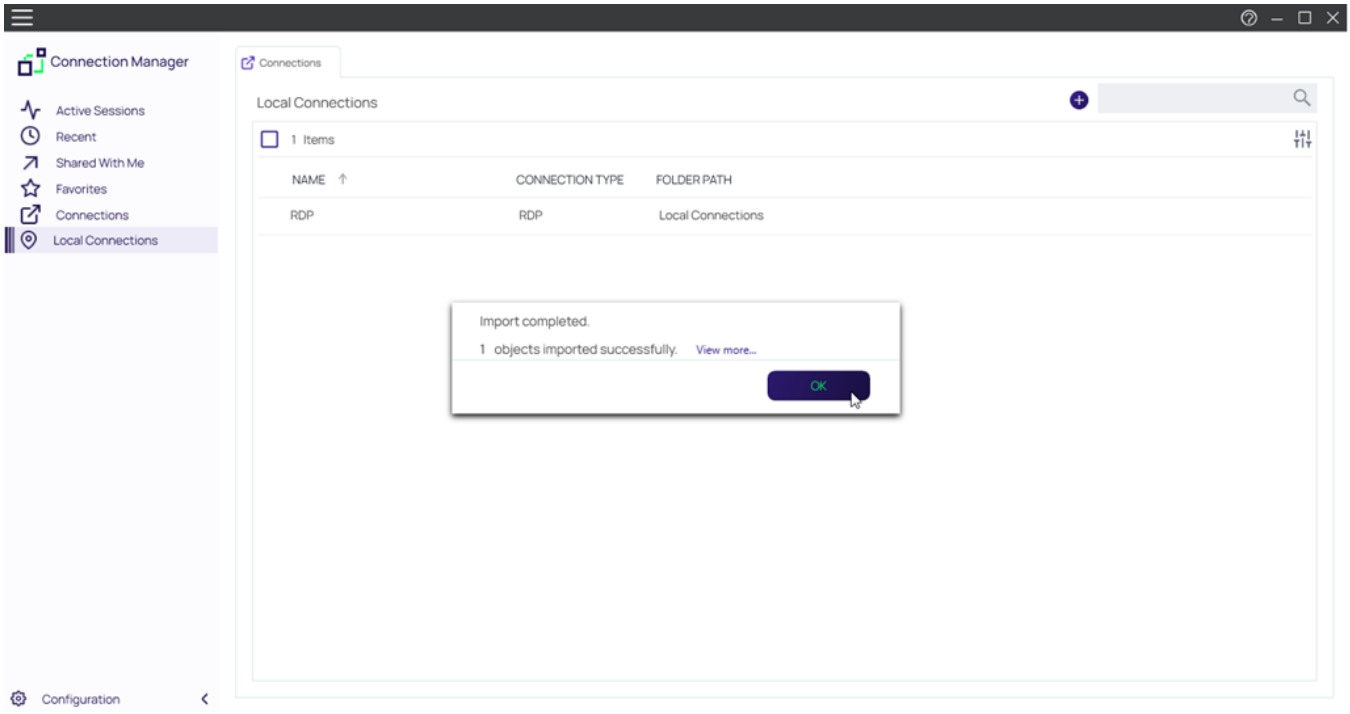
1. Right click on **Local Connections**
2. Hover over **Import** and select **Devolutions file**



3. A dialog window will appear. Select the files you would like to import.

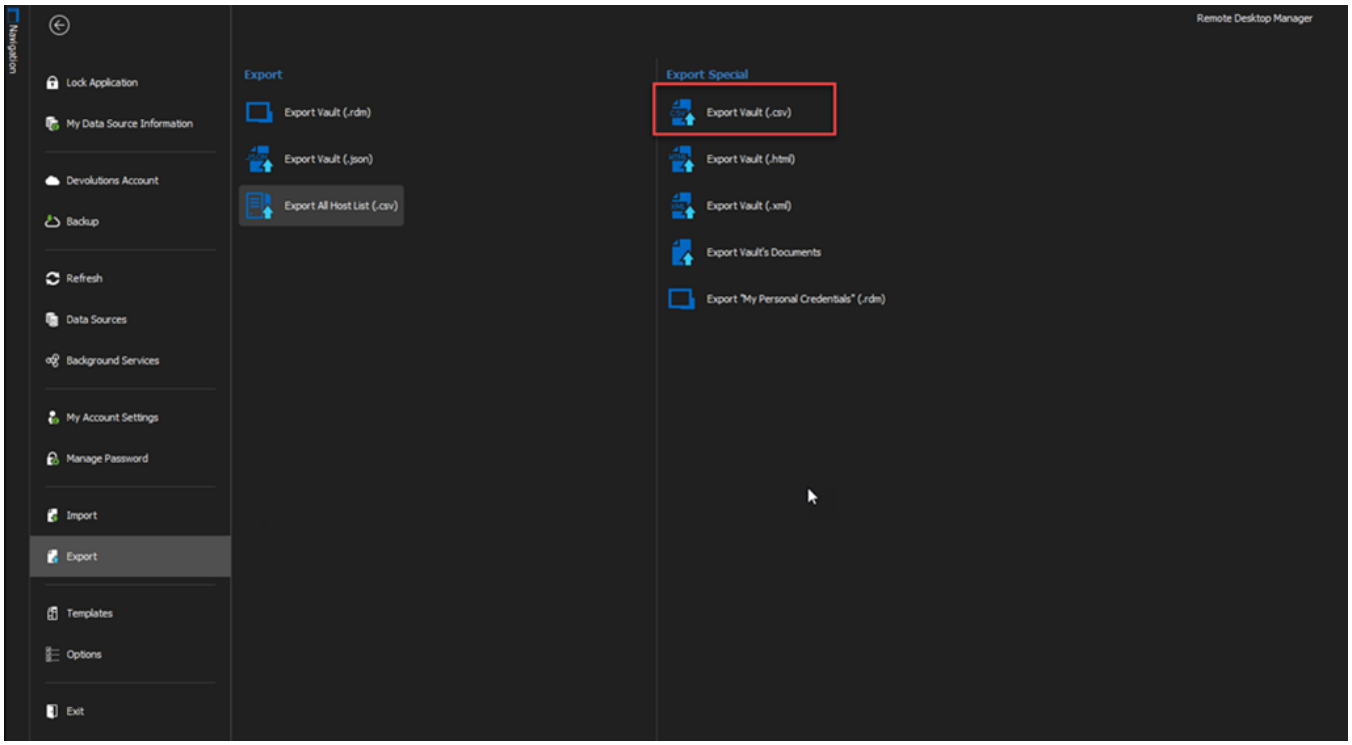


4. After the import is complete, a confirmation window will appear that the import was successful.



5. Click **OK** to return back to your Local Connections.

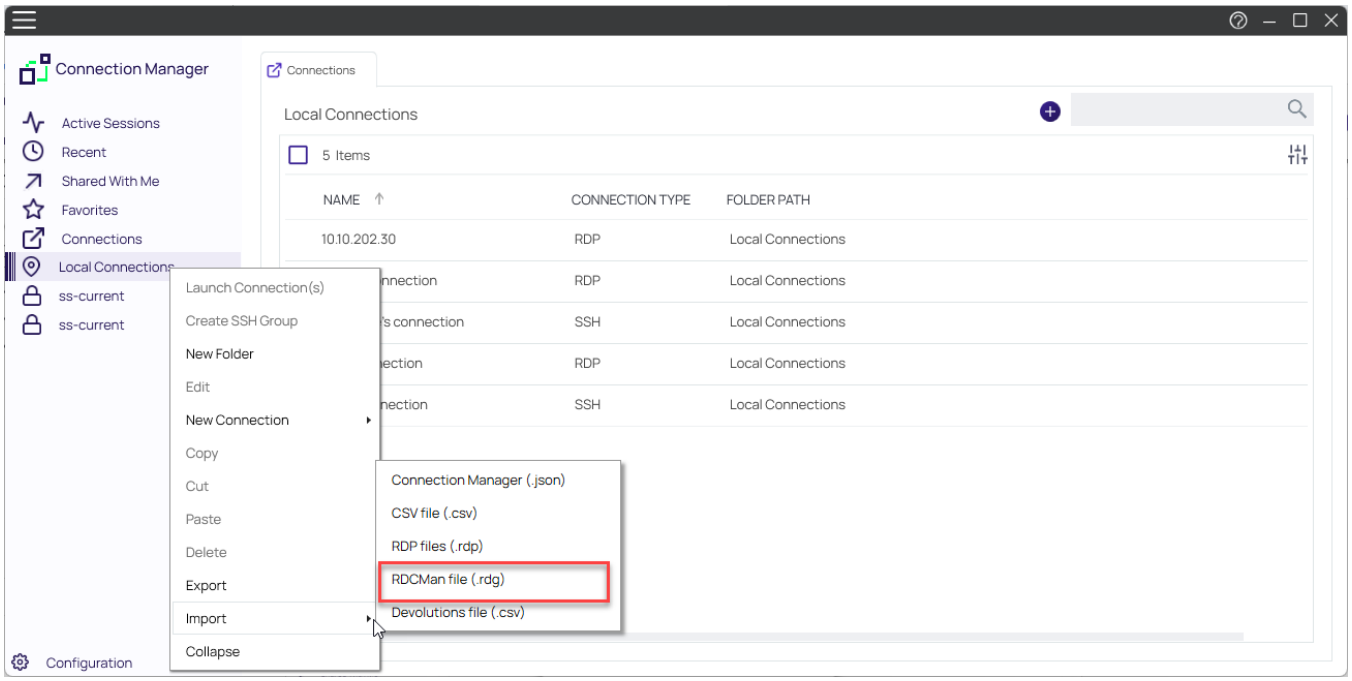
Note: When exporting connections from Devolutions, do not click **Export All Host Lists**. Instead, click **Export Vault** from the *Export Special* list.



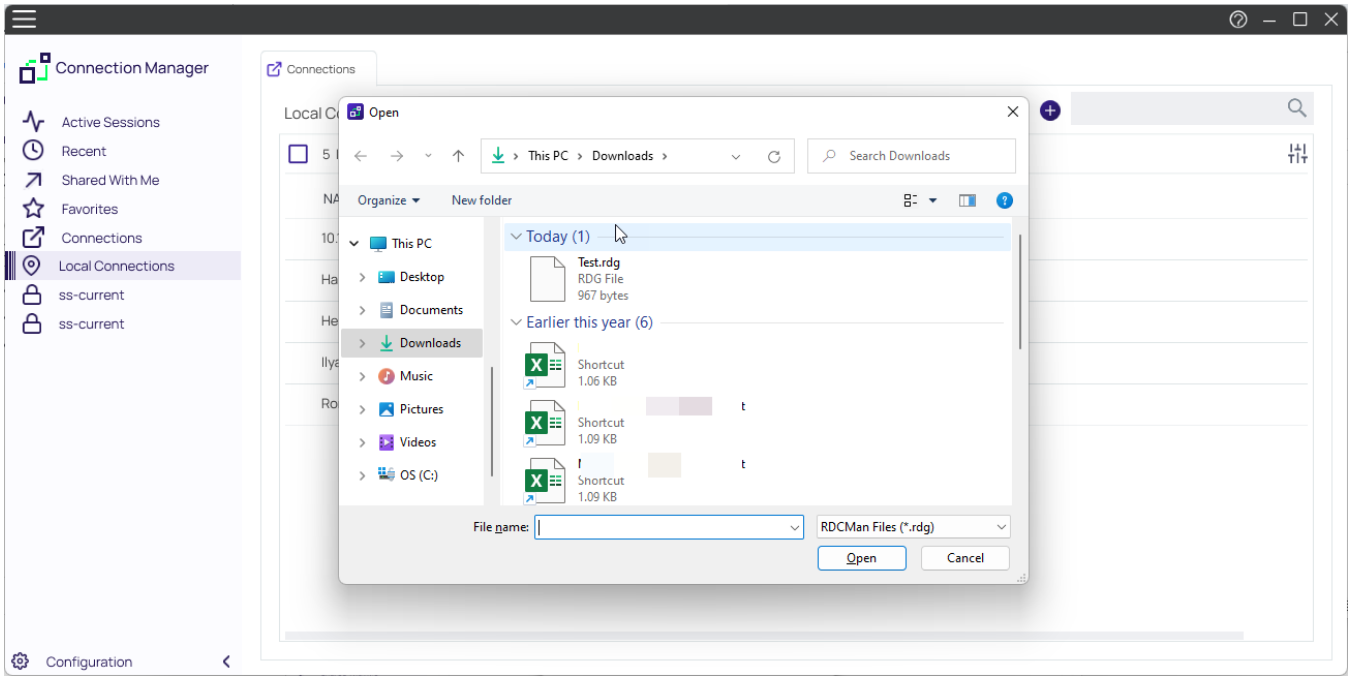
Importing RDG Files

Connection Manager supports the import of RDG files. To import an RDG file:

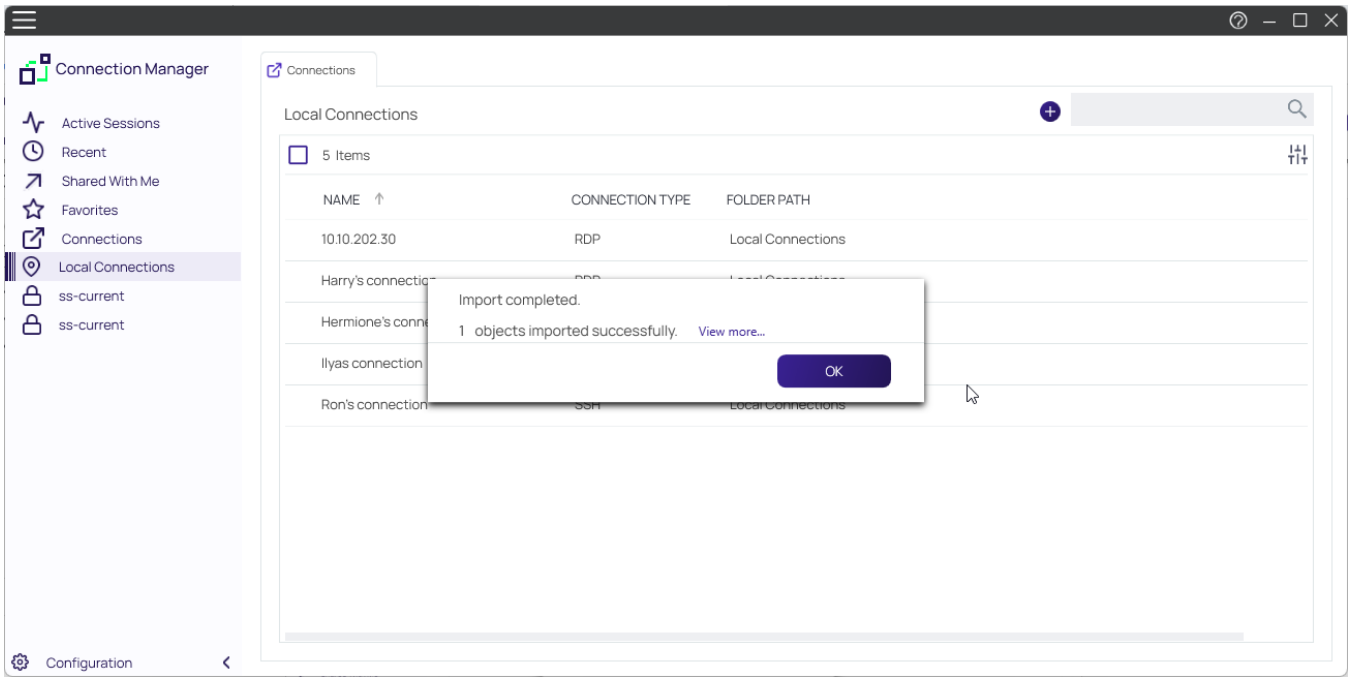
1. Right click on **Local Connections**
2. Hover over **Import** and select **RDG**



2. A dialogue window will appear. Select the files you would like to import.



3. After the import is complete, a confirmation window will appear that the import was successful.

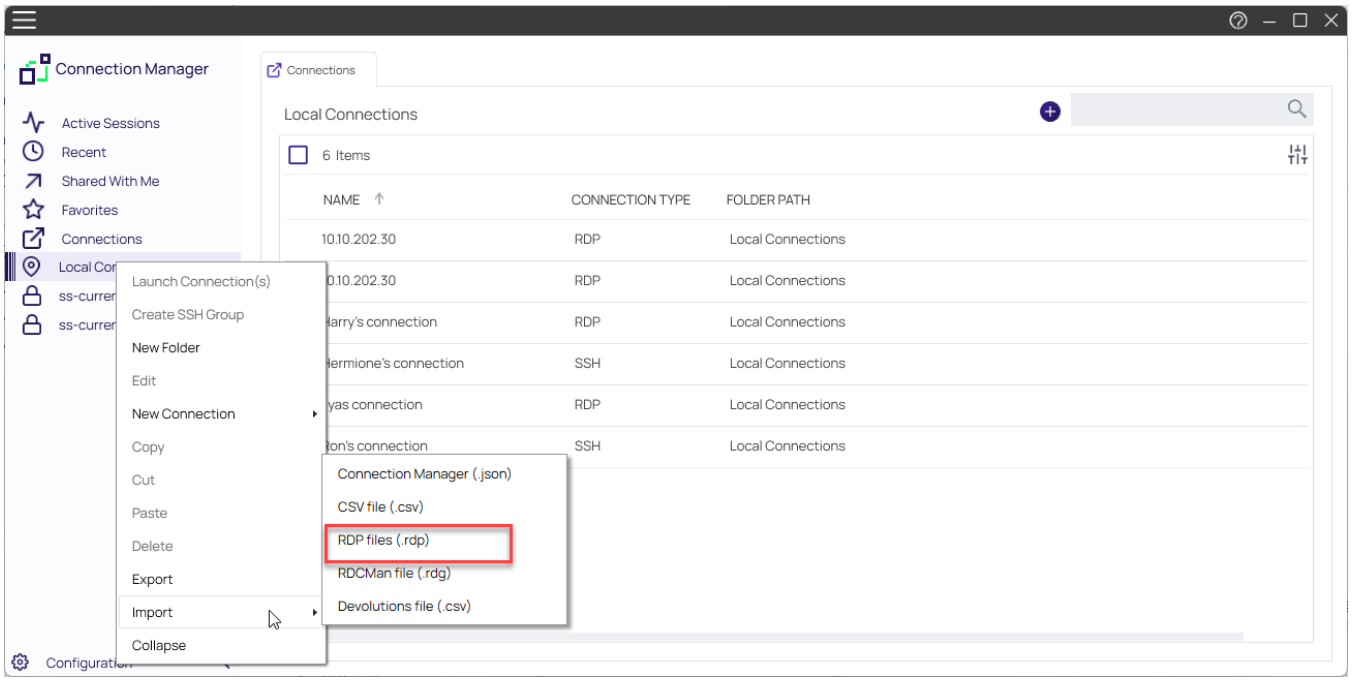


Click **OK** to return back to your Local Connections.

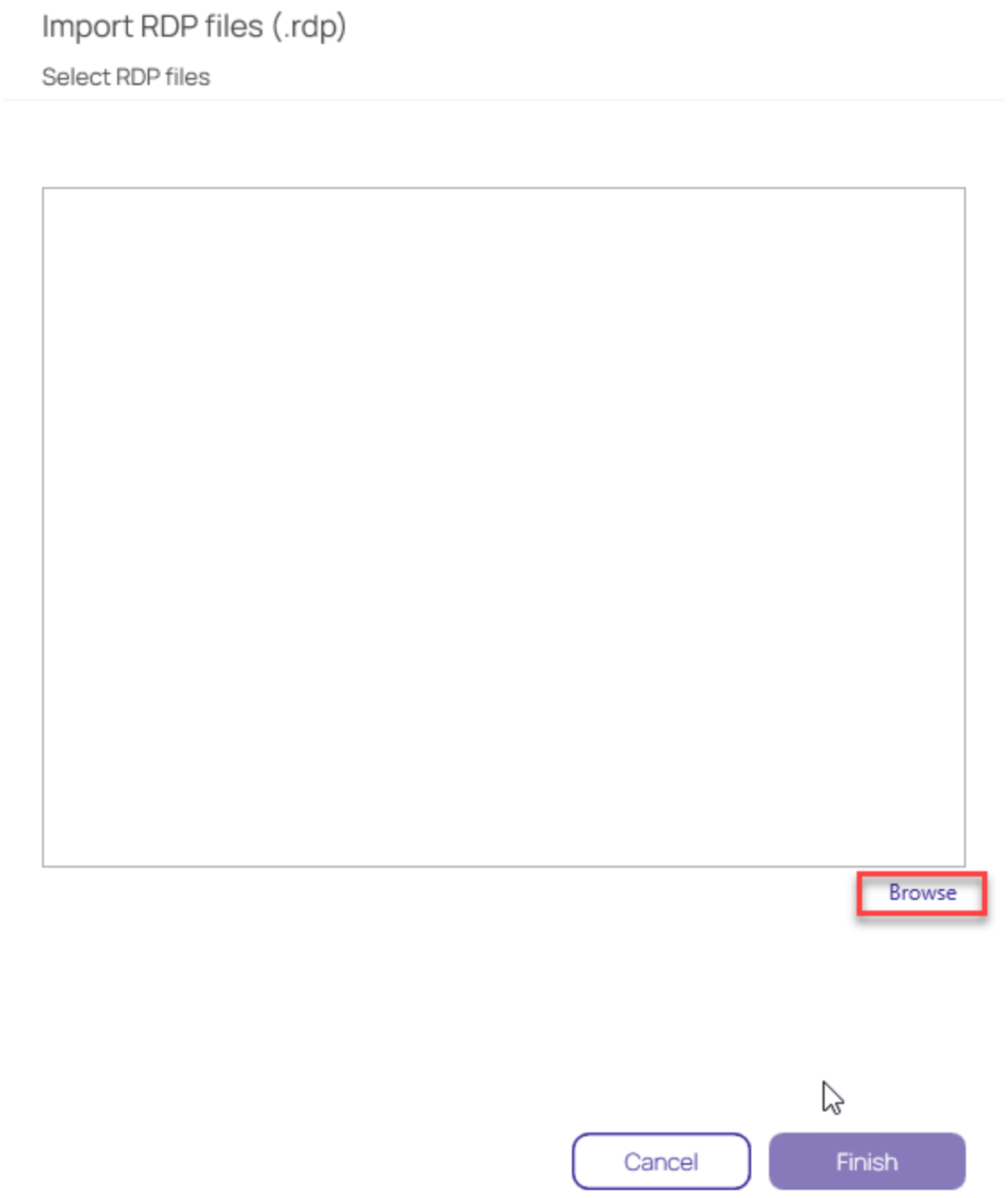
Importing RDP Files

Connection Manager support the import of RDP files. To import an RDP file:

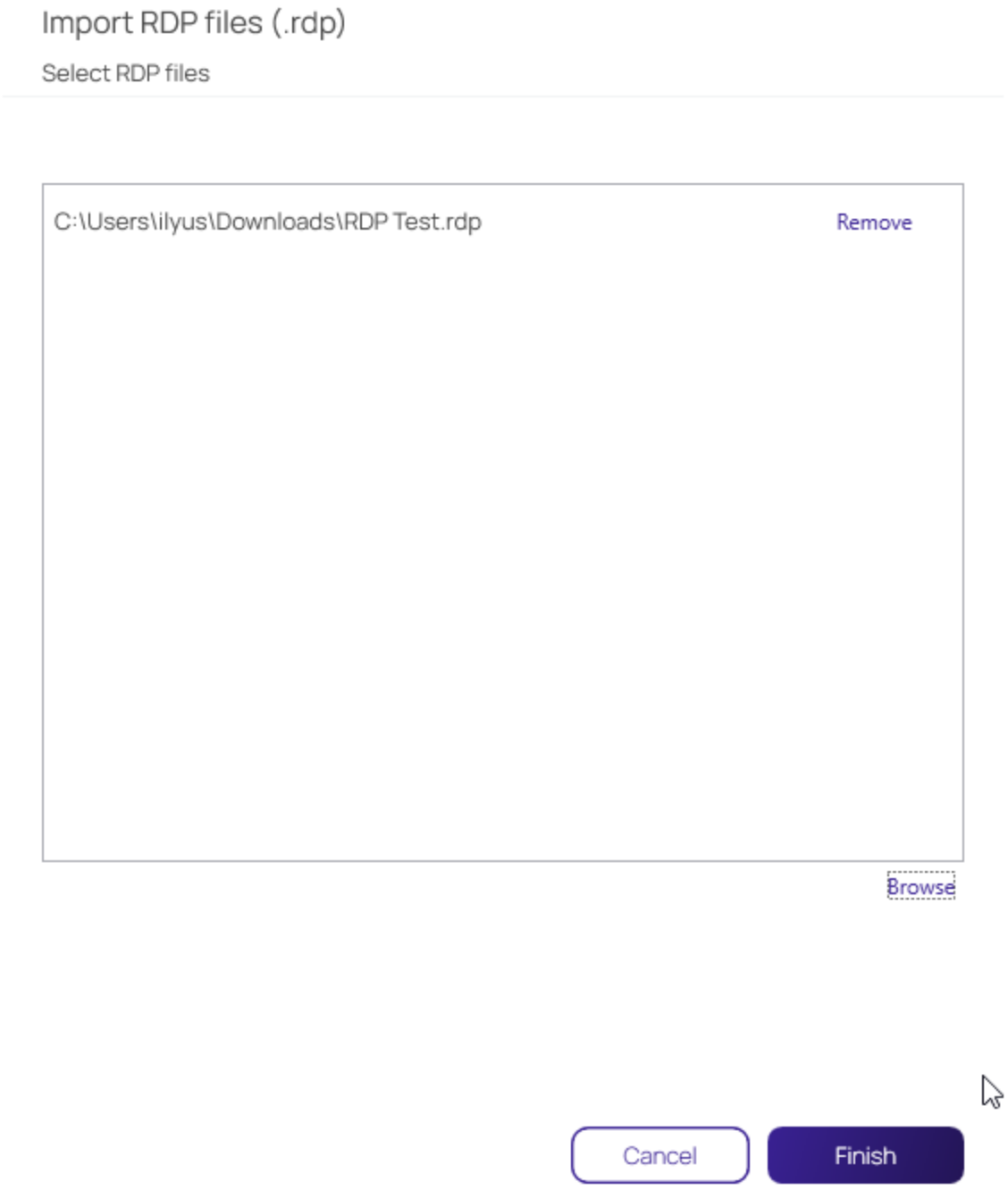
1. Right click on **Local Connections**
2. Hover over **Import** and select **RDP**



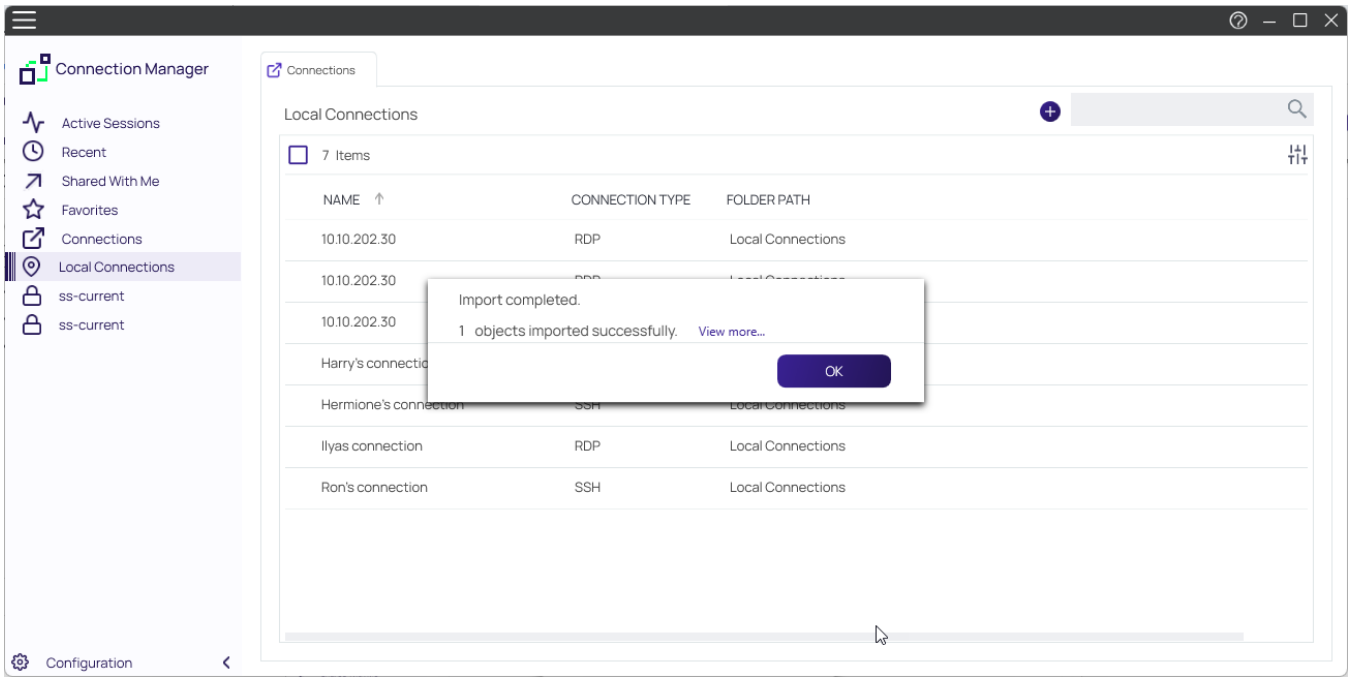
3. A new window will appear. Click **Browse** to start selecting RDP files to import.



4. Select all of the RDP files that need to be imported and click **Finish**



5. A confirmation window will appear that the import was successful.



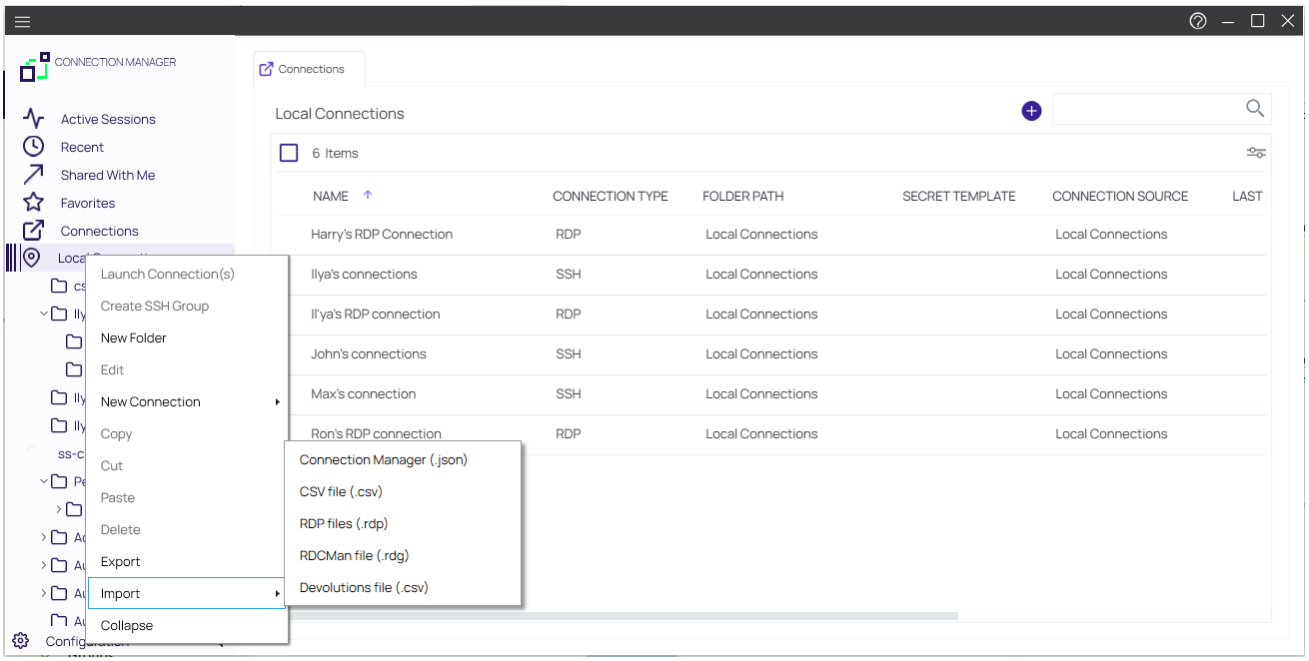
6. Click **OK** to return back to Local Connections.

Importing CSV Files

Connection Manager allows the import of Connection Manager .JSON, CSV, and RDP files for local connections data.

This example is for CSV file imports.

1. Right-click on **Local Connections**.
2. Select **Import**.

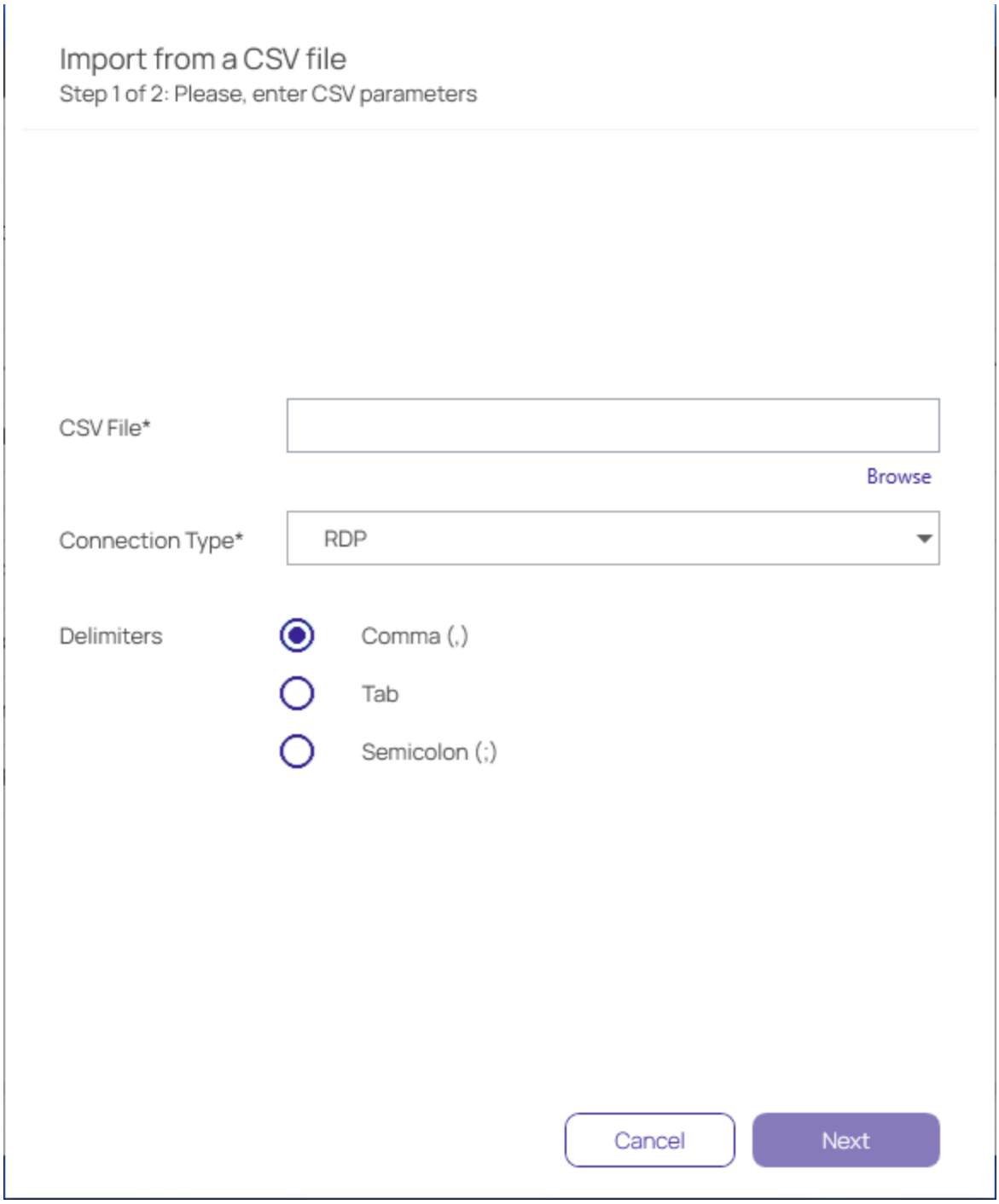


3. Select from the import options available based on your source file.

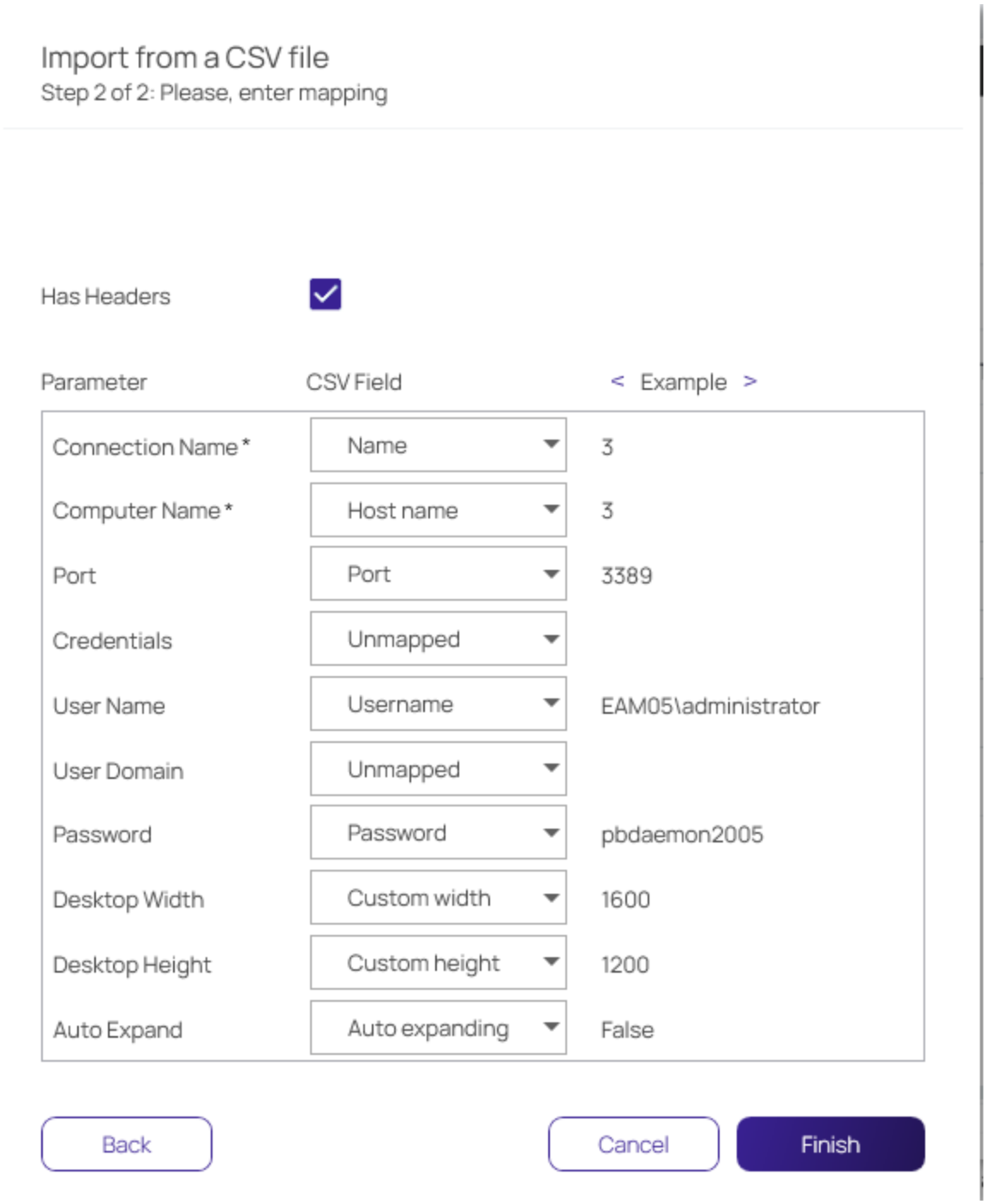
Import Local Connections

The following example shows what to expect when importing local connections via CSV file into your Connection Manager instance.

1. In Step 1 of 2 of the Import process,
   a. select the file to import,
   b. specify the connection type, and
   c. select which Delimiters are used in the import file, the default is comma separated.

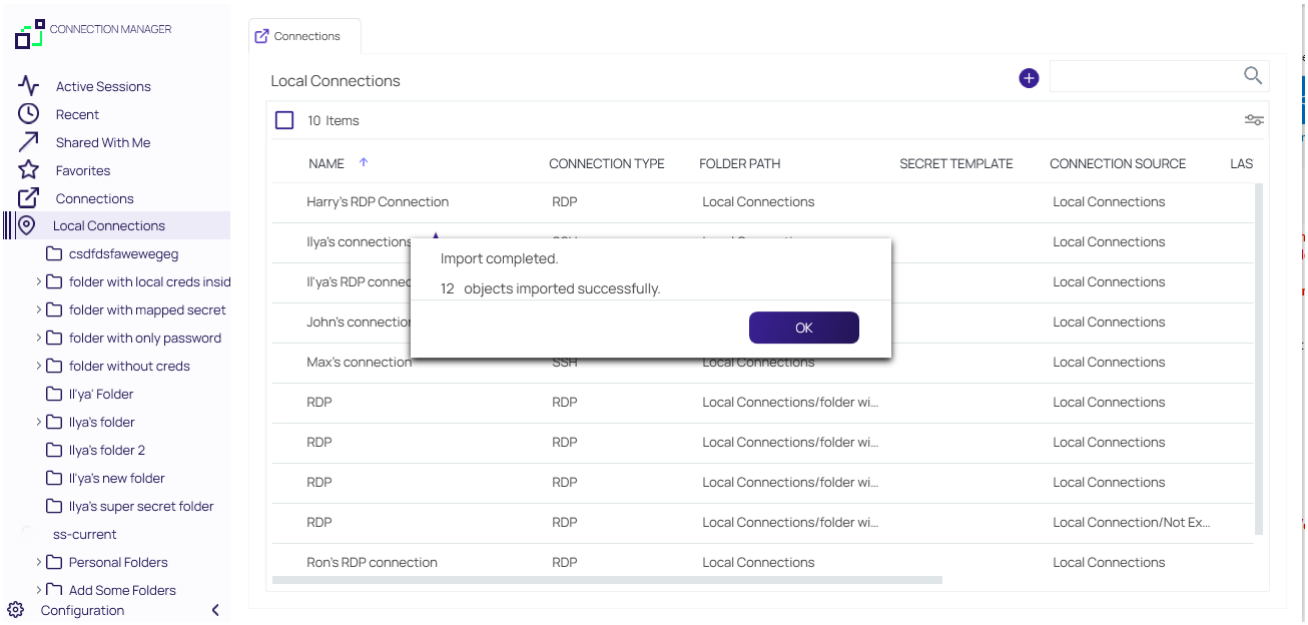

Import from a CSV file
Step 1 of 2: Please, enter CSV parameters
CSV File*
Browse
Connection Type*
RDP
Delimiters
Comma (,)
Tab
Semicolon (;)
Cancel
Next

2. Click **Next**.



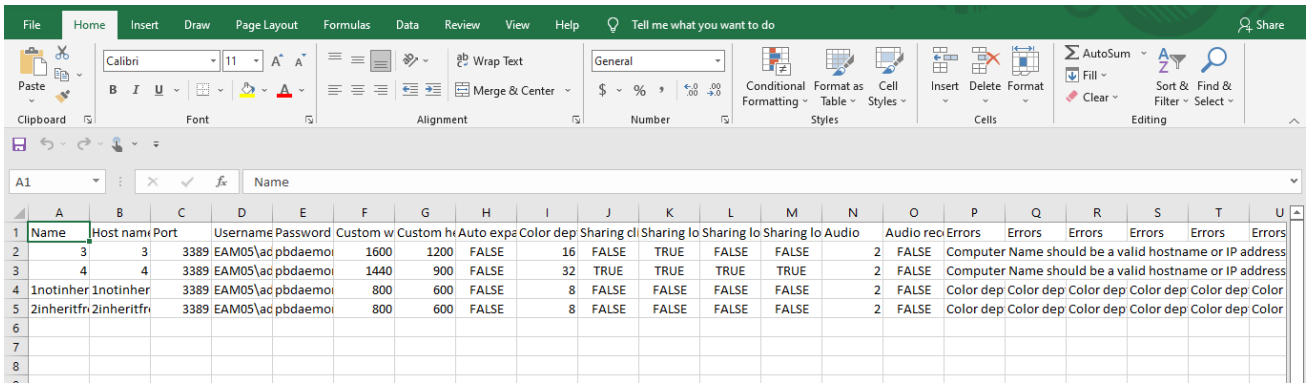
By default Connection Manager maps the data from the import file to field mappings for the local connection information. Any data not recognized/mapped is indicated as unmapped and duplicate mappings are highlighted red. These potential errors can be fixed prior to the import.

3. Click **Finish**.



Each connection in the file is imported as a Local Connection. Links to informational or error reports will be displayed, but only if the import encountered errors or if it automatically mapped fields during the import.

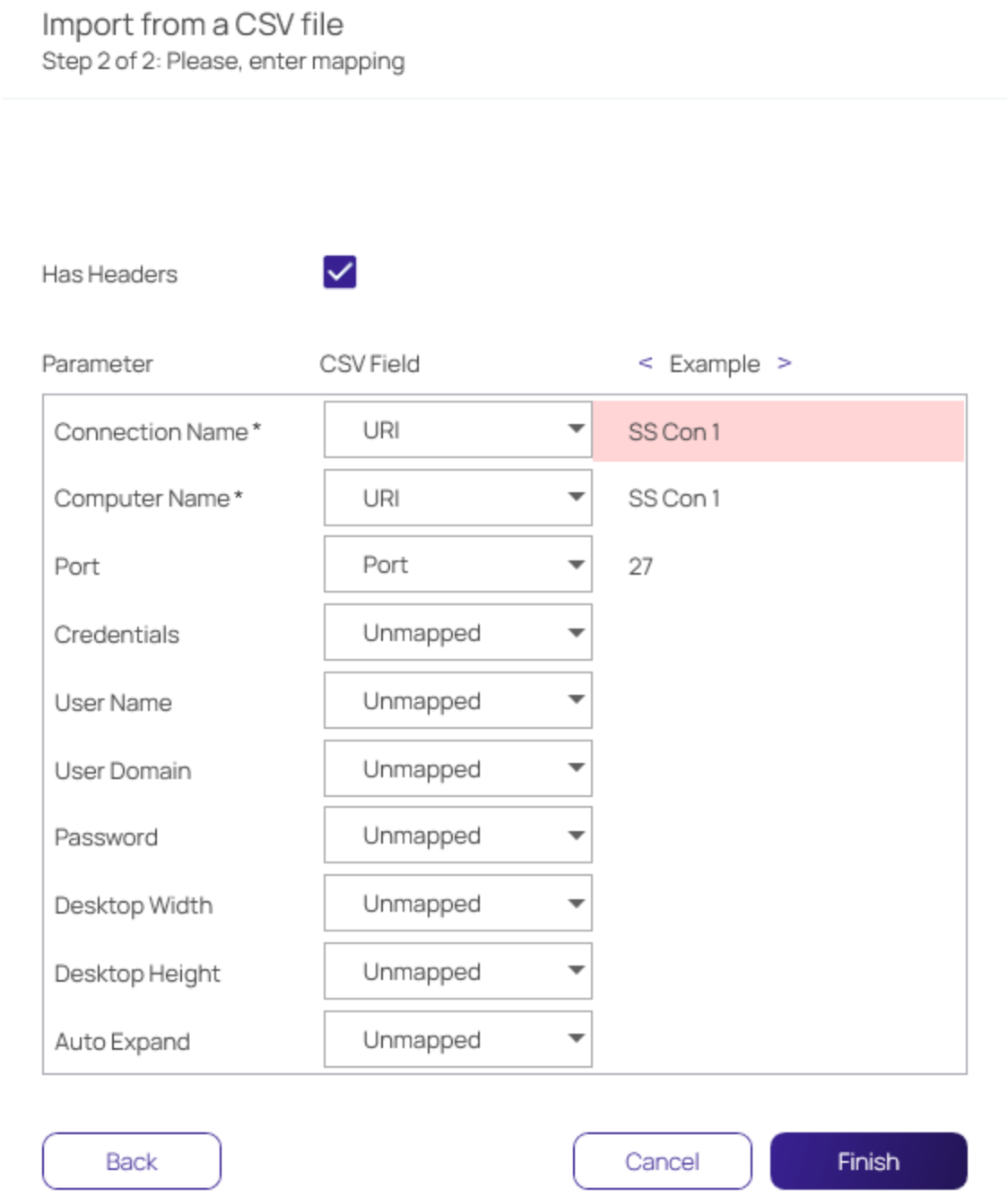
4. To further examine which information failed to import, click **View more...**.



Connection Manager saved the connection data that failed to import in a separate Excel file. The data can be edited and the file can be used to retry the import for the remaining connections.

5. Back in the Connection Manager UI, click **OK** to close the **Import completed** window.

Example of Step 2 of 2 window showing errors:



Field Values and Types

Note: The CSV import file does not need to include all of the fields shown below.

Name	Type	Applies to	Values
Connection Name (required)	String	RDP, SSH	
Computer Name (required)	String	RDP, SSH	
Port	Number	RDP, SSH	1 - 65535
Credentials	Enumeration: 0,1,2	RDP, SSH	0 - None 1 - Inherited 2 - Embedded
User Name	String	RDP, SSH	
User Domain	String	RDP, SSH	
Password	String	RDP, SSH	Cleartext
Desktop Width	Number	RDP	
Desktop Height	Number	RDP	
Auto Expand	Boolean	RDP	TRUE FALSE Or 1 0
Color Depth	Number	RDP	15 16 24 32
Run As Admin	Boolean	RDP	
Clipboard	Boolean	RDP	
Drives	Boolean	RDP	
Printer	Boolean	RDP	
Smart Cards	Boolean	RDP	
Audio Playback	Enumeration: 0,1,2	RDP	0 - Use local computer 1 - Disabled 2 - Use remote computer
Audio Recording	Boolean	RDP	

Name	Type	Applies to	Values
Remote Character Set	String	SSH	
Font	String	SSH	
Font Size	Number	SSH	1-72
Connection Type	Enumeration: 1 - RDP, 2 - SSH		1 - RDP 2 - SSH

Desktop Size

The following combinations of Desktop Width/Desktop Height are valid (if combination is not valid, the default value is used):

//4:3 resolutions

- 640x480
- 800x600
- 960x720
- 1024x768
- 1280x960
- 1400x1050
- 1440x1080
- 1600x1200
- 1856x1392
- 1920x1440
- 2048x1536

//16:10 resolutions

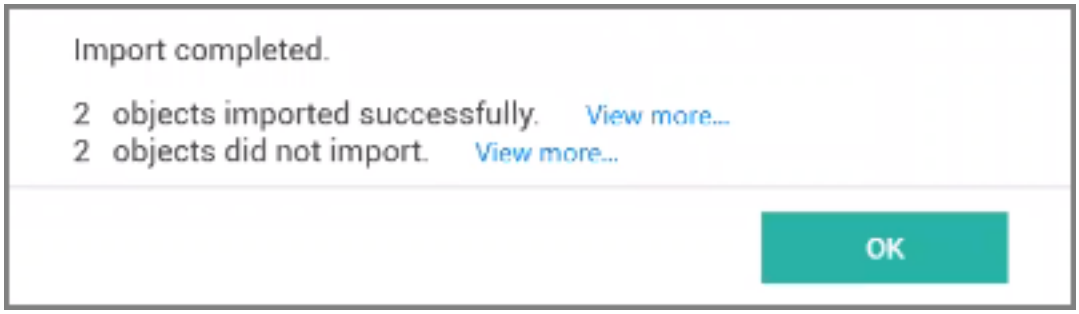
- 1280x800
- 1440x900
- 1680x1050
- 1920x1200
- 2560x1600
- 2880x1800

//16:9 resolutions

- 1024x576
- 1152x648
- 1280x720
- 1366x768
- 1600x900
- 1920x1080
- 2560x1440
- 3840x2160
- 7680x4320

Import Completed Reports

Imports and trigger none, one, or up to two reports.



- Successful: This report lists all objects that have been successfully imported.
- Not imported: This report lists all objects that failed to import. The report can be used to remediate the import issue(s) and the remaining connections can be reimported.

CSV Import Differences

If you are working with Devolutions type connection .csv files, do not use the standard .csv import option. Devolutions .csv files require a different mapping scheme than standard .csv. Connection Manager only imports RDP/SSH connections from Devolutions. Imports of "Folders","Workstation", or "Domain" data returns a "Import failed. Invalid file format" message.

Global Configuration Settings

Using global configuration settings, a user can set default values to be used for new local connections, connections made directly from Secret Server, and connections made when Connection Manager is acting as a protocol handler.

Global configuration settings can be changed (over-ridden) on individual connections, and those override settings will not be impacted by subsequent changes to global configuration settings.

Global configuration settings do not impact existing local connections, even if they were exported and imported.

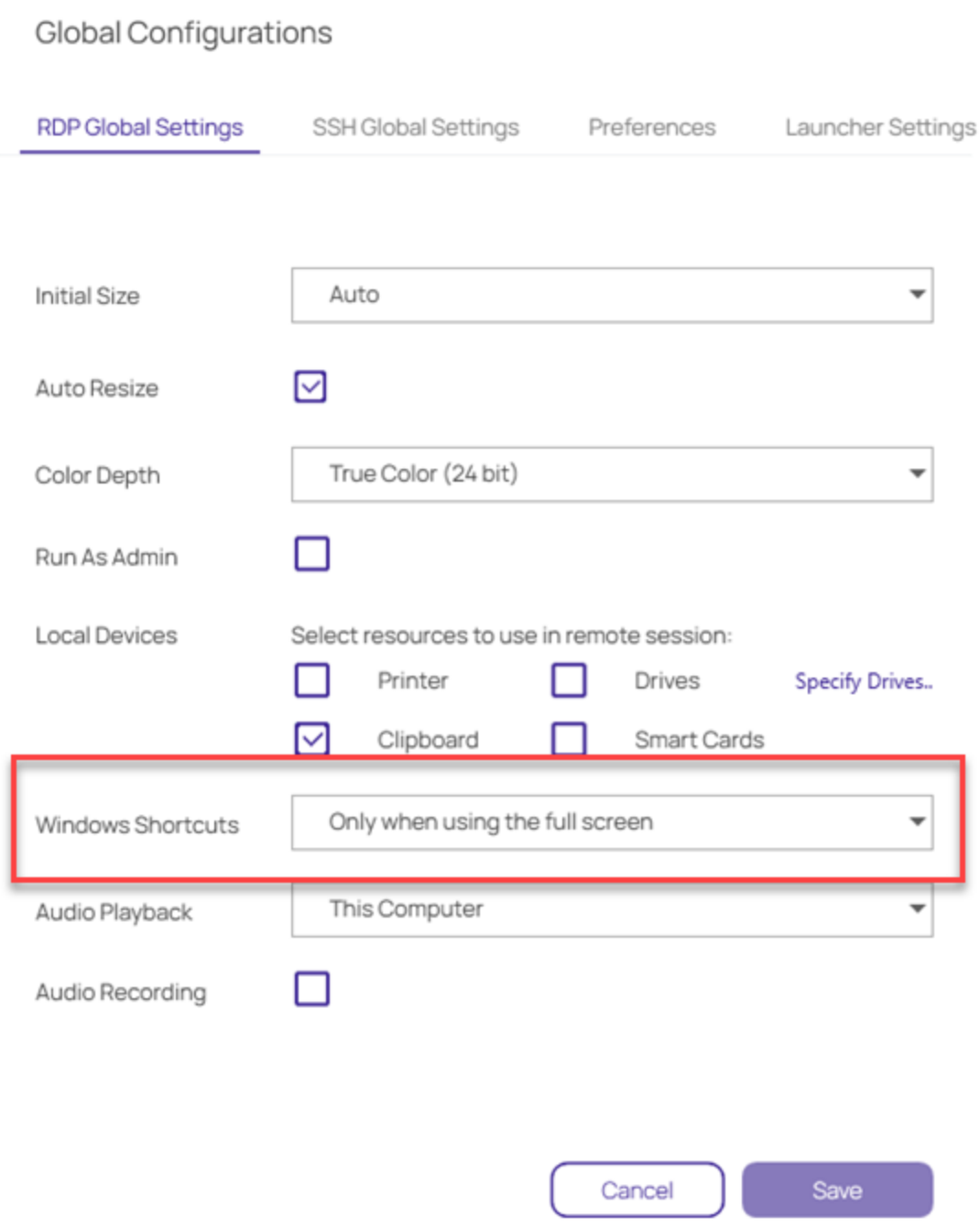
Connections from Secret Server do not support all available parameters. In such cases the default parameters are substituted.

On the Configuration menu, click **Global Configurations**. The Global Configurations dialog box opens to the **RDP Global Settings** tab, where you can configure settings such as **Desktop Size**, **Color Depth**, and **Local Devices**.

Windows Shortcuts

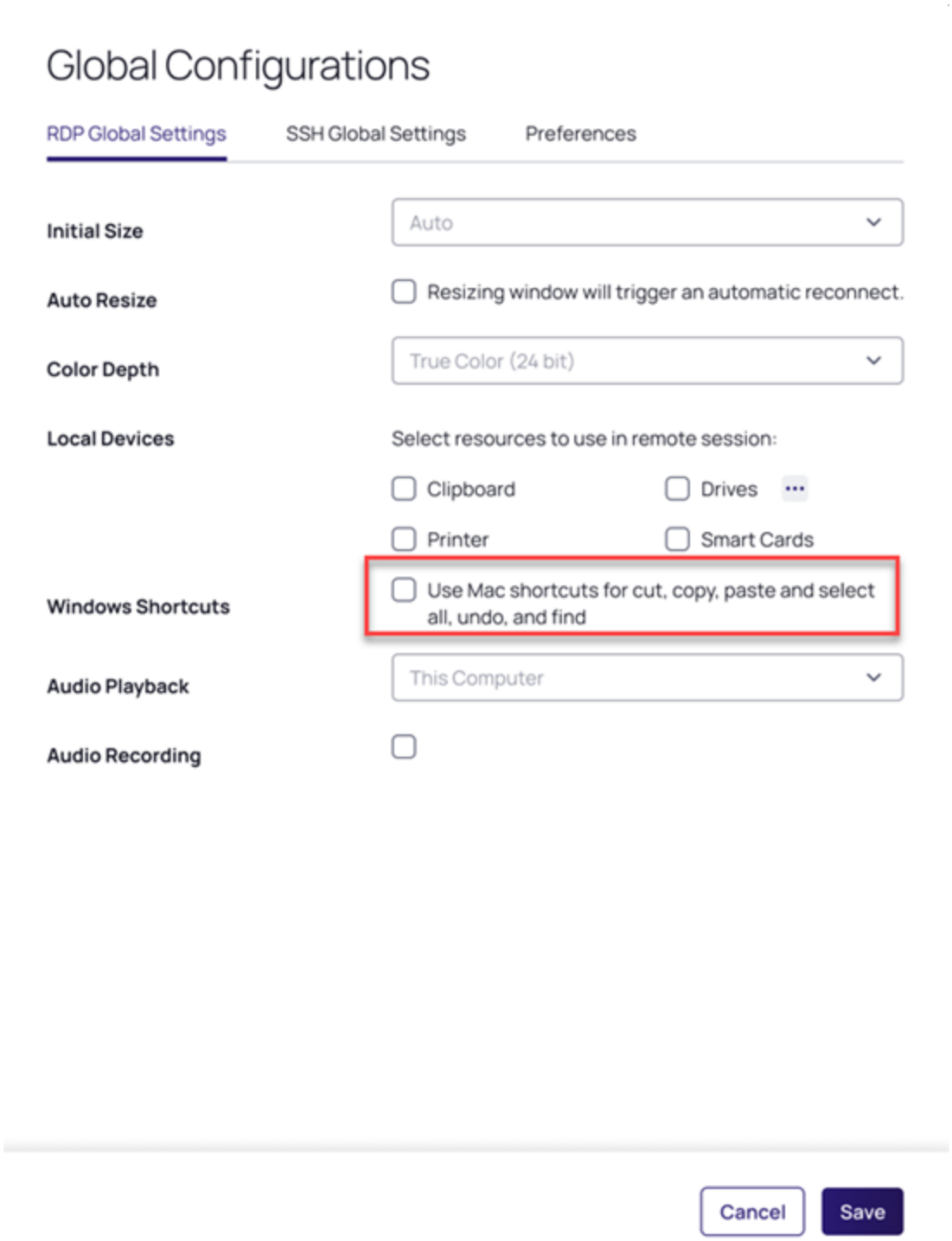
The **Windows Shortcuts** field can be set individually or in bulk and offers the following three options:

- On this computer: Windows shortcuts will execute on the local computer.
- On the remote computer: Windows shortcuts will execute on the remote computer.
- Only when using the full screen: Windows shortcuts will execute on the remote computer only when you are in full-screen mode.



Map Windows Shortcuts on MacOS

If you are on macOS, check the **Use Mac shortcuts** box to use this feature.



Audio Playback and Audio Recording

You have three audio playback options to choose from:

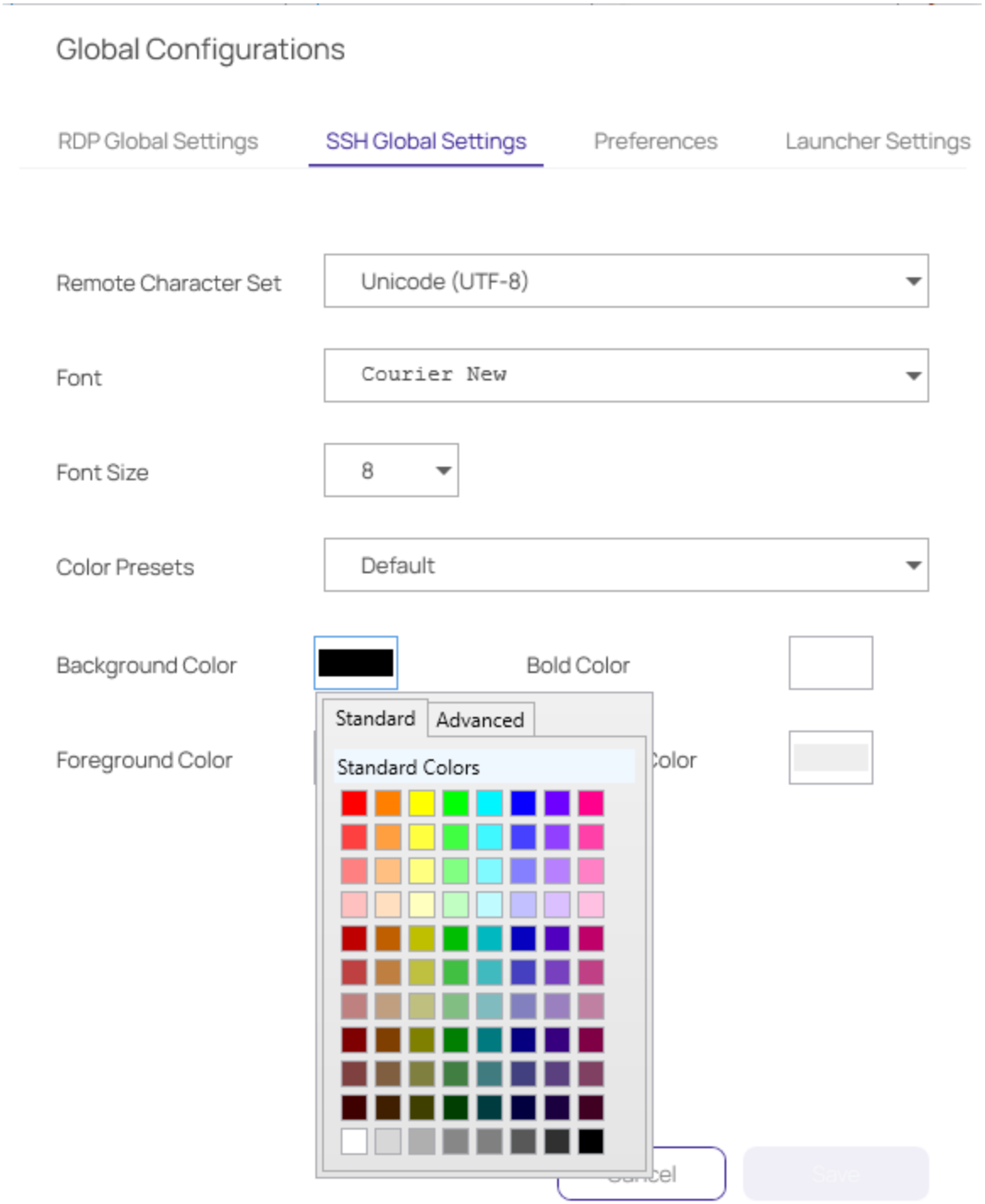
- This computer: Audio will play on the computer used to connect.
- Remote computer - Audio will play on the computer you are connected to.
- Do not play - Data from audio and microphone will not be transmitted.

If you would like to use a microphone during remote connection, be sure to check the Audio Recording box.

SSH Global Settings

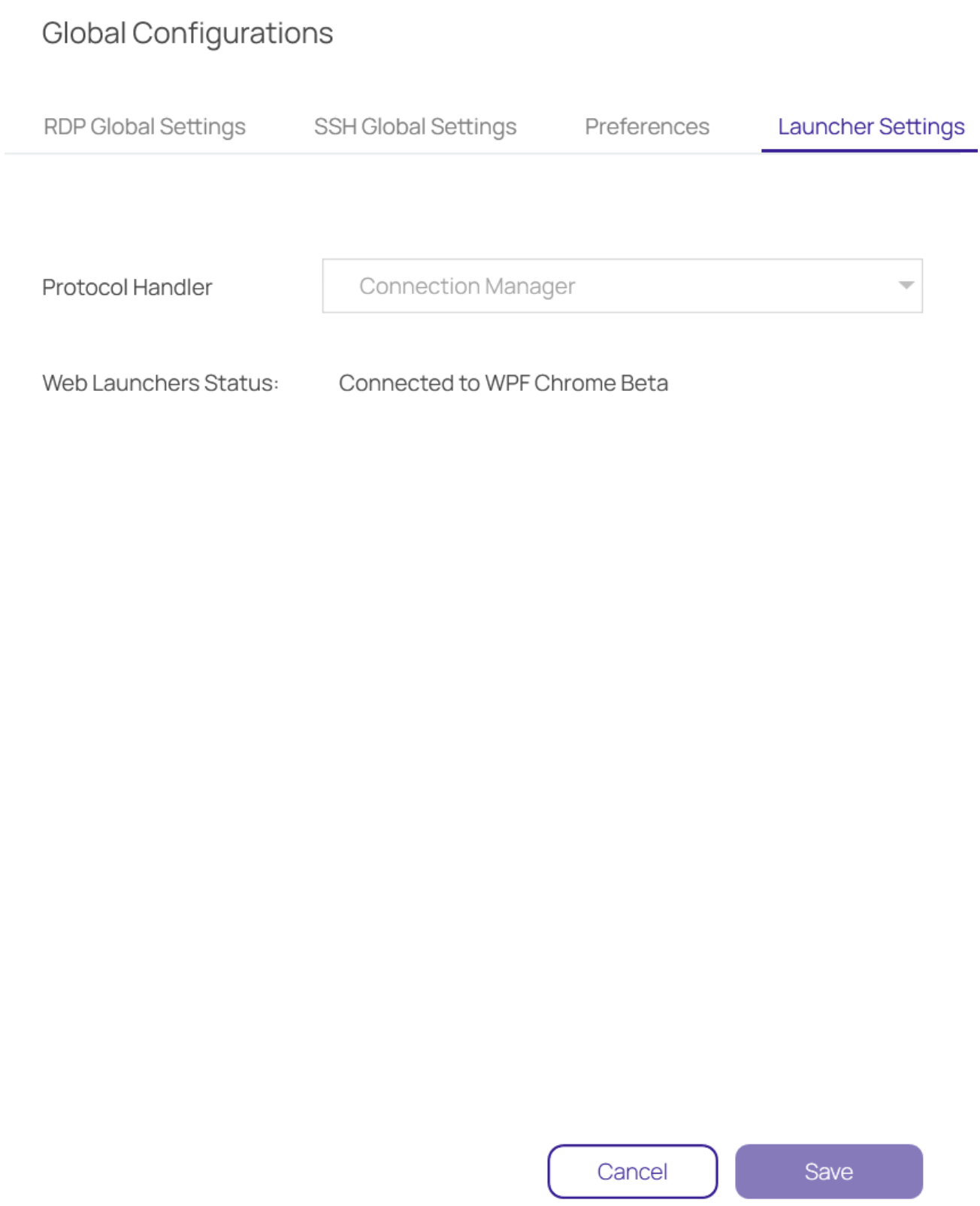
On the **SSH Global Settings** tab, you can configure settings such as **Font** and **Font Size**. You can choose one of the **Color Presets** or you can create a Custom color scheme by changing the individual values for **Background Color**, **Foreground Color**, **Bold Color**, or **Underlined Color**.

Important: These settings will be applied to all of your vault connections. If you would like to adjust the settings for local connections, see "Editing Local Connections " on page 86.



On the **Launcher Settings** tab, administrators can choose to use the Connection Manager protocol handler or the legacy protocol handler, Secret Server Launcher. Users can also switch between the two protocol handlers. If both protocol handlers are installed and the administrator uninstalls one of them, the other protocol handler will register itself as the protocol handler for all users on installation.

In addition to this, you will see the web launcher connection status. This is useful if you are launching secrets created with the Web Password Filler template.

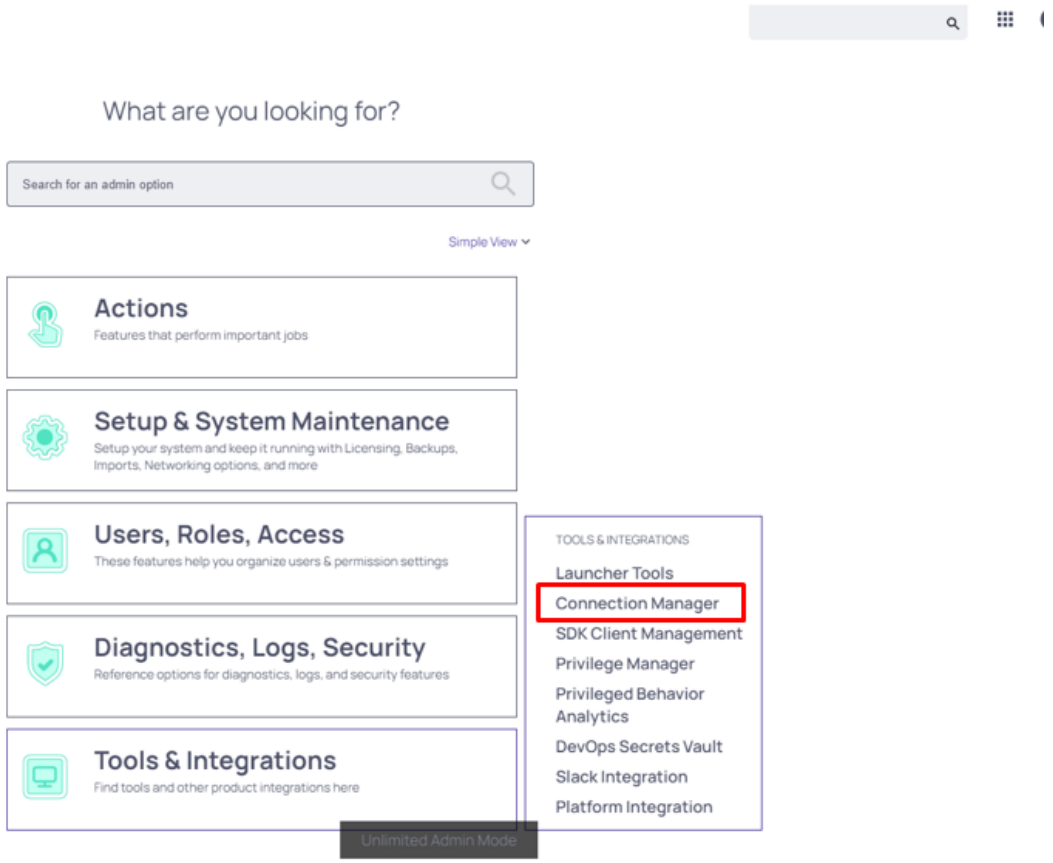

Global Configurations
RDP Global Settings
SSH Global Settings
Preferences
Launcher Settings
Protocol Handler
Connection Manager
Web Launchers Status:
Connected to WPF Chrome Beta
Cancel
Save

Globally Enforced Secret Server Settings

The following settings can be configured in Secret Server and will be applied globally for any Connection Manager application that is connected to it.

To access this in Secret Server:

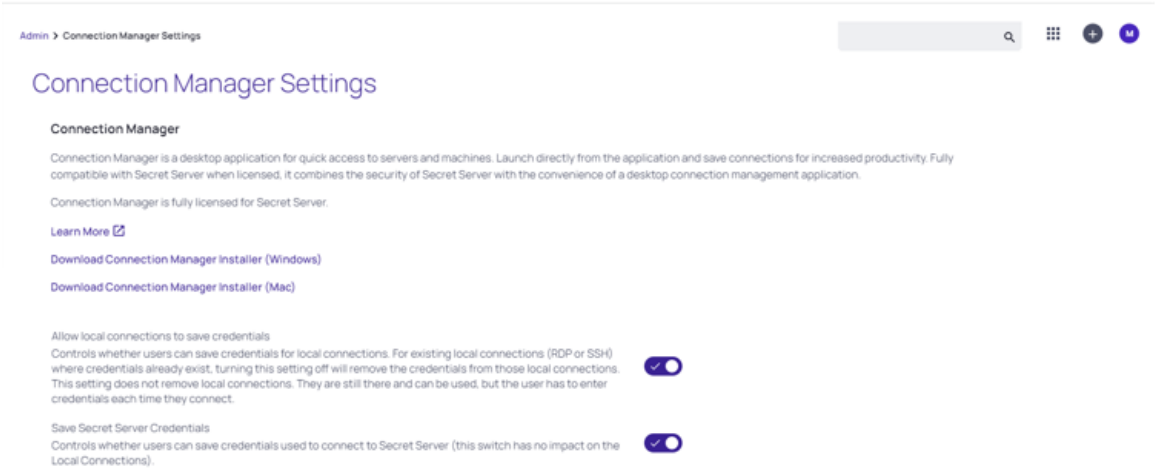
1. Navigate to **Admin | See All**.
2. Select **Tools & Integrations**.



These options are by default enabled:

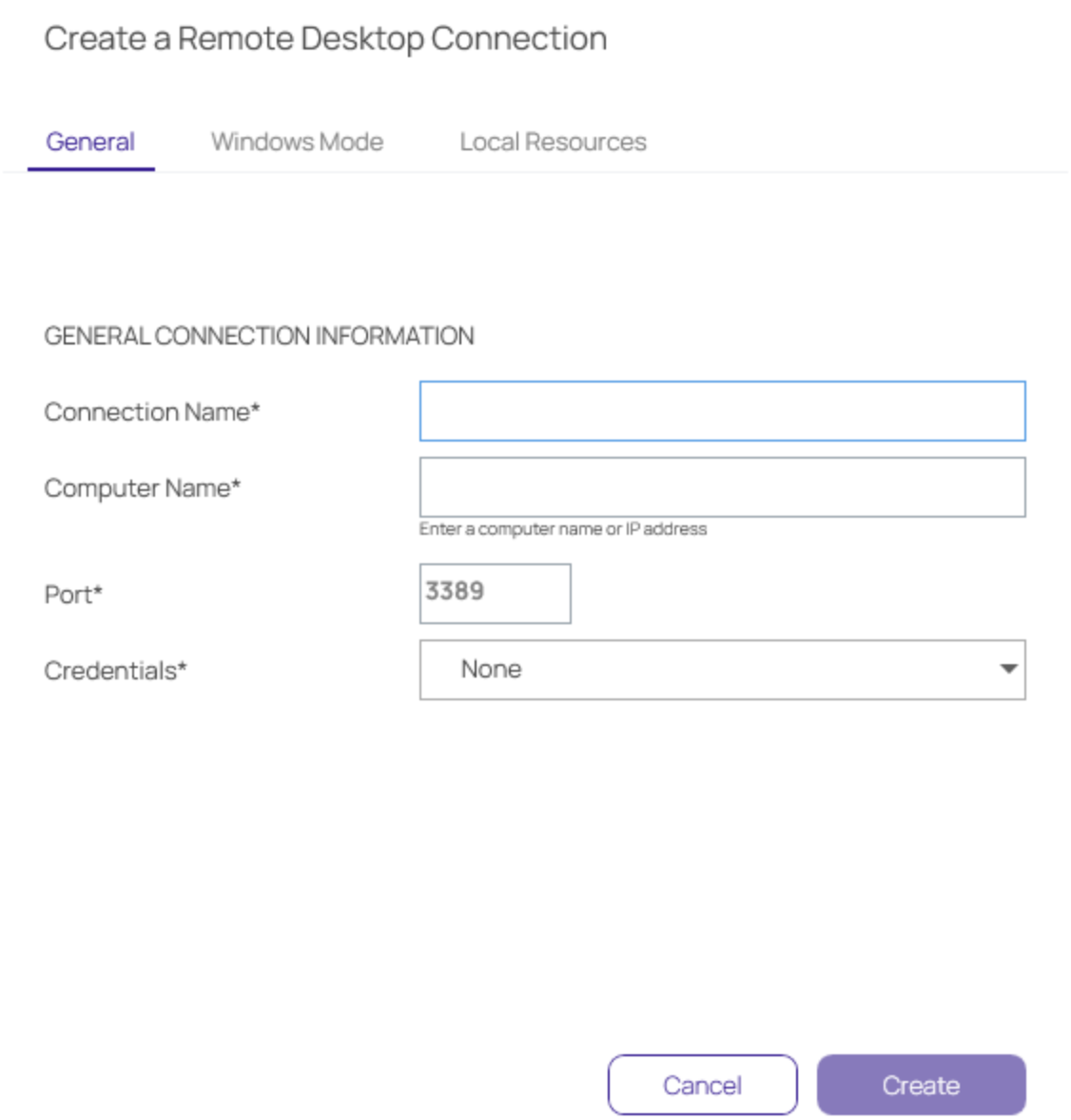
- Allow Local Connections – Allows or disables saving credentials for any Local Connections. The default is Yes.
- Allow Saving Credentials - Allows or disables saving credentials for any Secret Server connections. The default

is Yes.



If Connection Manager is connected to multiple Secret Server Instances, and those instances have different values for these new settings, then Connection Manager will always use the more secure option set for security purposes. For example, if Connection1 allows Local Connections, and Connection2 does not allow Local Connection, then Connection Manager will not allow Local connections at all.

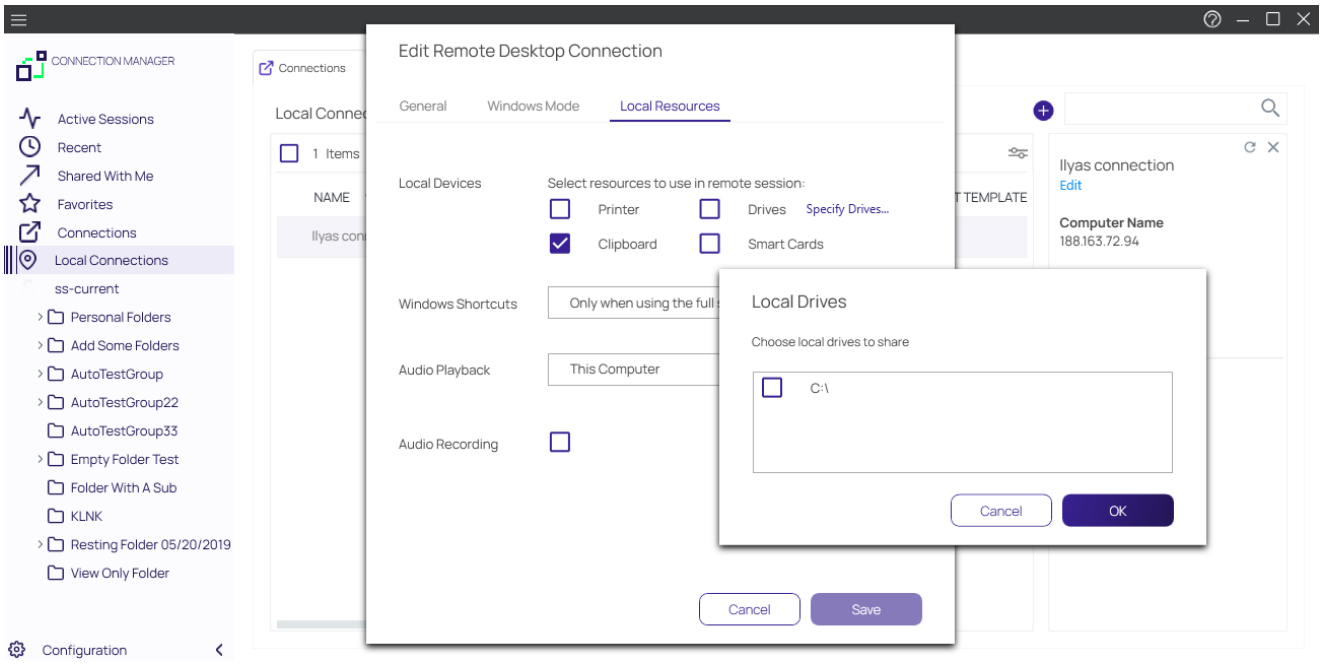
If "Allow Local Connections" is set to "off" and user imports local connection(s), credentials are not imported but the local connections are created.



If you already have Local Connections saved, and the **Allow Local Connection** option is disabled, then the next time the Secret Server instance is connected to the Connection Manager instance we will prompt the user that the Local Connections will be deleted. If they agree, then Secret Server connects and the local connections are deleted. If they say No, then we prevent Secret Server from connecting.

The behavior is the same for saving credentials when setting the **Allow Saving Credentials** flag.

When creating or editing a Remote Desktop Connection, you can select and map the local drives you wish to share. On the **Local Resources** tab, click **Drives** and then click **Specify Drives**. Select the drives you wish to map and deselect any drives you don't want to map. If you choose to map all available local drives, the **Drives** box displays a check mark. If you decide to map only some of the available local drives, the **Drives** box displays a dash.



Using a Custom Logo in the Connection Manager Interface

In Connection Manager version 1.6.0 and higher, you can substitute the default logo in the Connection Manager interface with your own company branded logo using either of the two procedures below.

Manual Procedure

1. Create two versions of your logo image file in PNG format, with names exactly as specified below:
   - One sized to 250 x 50 pixels, named `logo.png`. This version is the full-sized logo that will appear in the main interface.
   - One sized to 100 x 50 pixels named `logo_collapsed.png`. This version is the collapsed logo that appear when the left navigation panel is collapsed
2. Store both image files in the following location (if you don't have this folder structure already, you'll need to create it): `C:\ProgramData\Delinea\Connection Manager\Resources\`
3. Assign all users permissions to read, execute, and list folder content from this location.
4. Restart Connection Manager

Command Line Procedure

Users with administrator privileges can specify the location of custom logo files during installation by running the following command:

Windows:

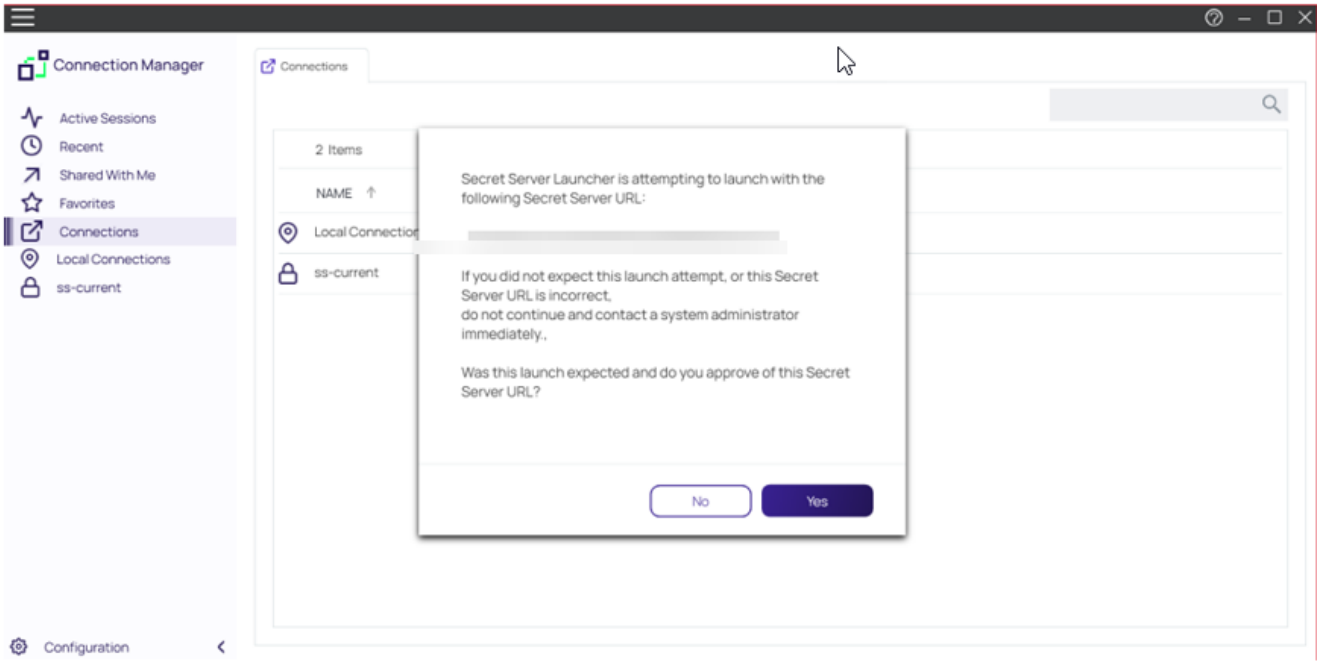
```
Delinea.ConnectionManager.WindowsInstaller /quiet RUNCM=runCM KEYS="-logo
C:\install\logo.png -logocollapsed C:\install\logocollapsed.png"
```

MacOS:

```
sudo defaults write /Library/Preferences/com.Delinea.ConnectionManager installparams -dict
\
logo "/Users/[username]/Downloads/my-logo.png" \
logocollapsed "/Users/sergii/Downloads/my-logo-collapsed.png" && sudo installer -pkg
~/Downloads/Delinea.ConnectionManager.2.9.0.MacOSInstallerRC10.pkg -target /
```

Protocol Handler Approved URLs

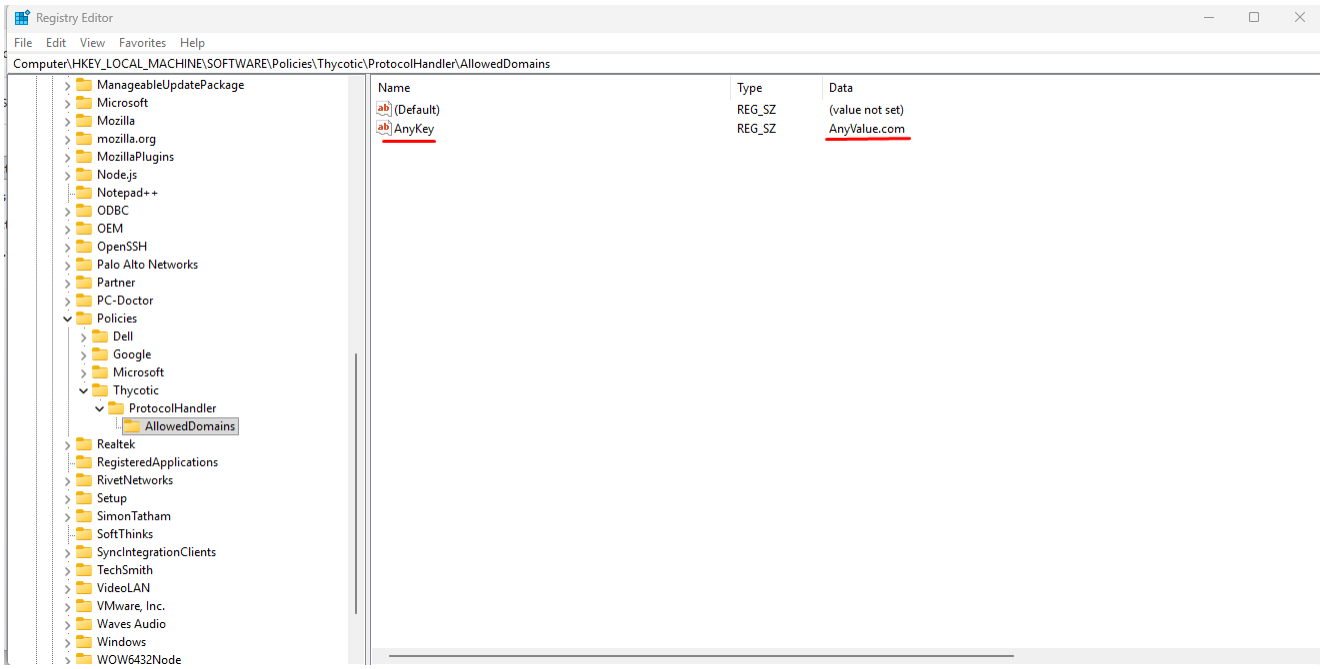
When launching protocol handler,Connection Manager checks the source URLs of the Secret Server that launched the secret. If a user does not have a previously approved URL, Connection Manager will display a message requesting the user to either approve of deny approval URL and the system will automatically remember this selection for future use.



Connection Managerwill not run secret from denied Secret Server URLs. If the user denied the Secret Server URL by mistake, and wants to fix this issue, they should delete the ApprovedSsUrlStorage.dat file located in the application's data folder (reload application).

Protocol Handler Allowed Domains in the Registry Editor

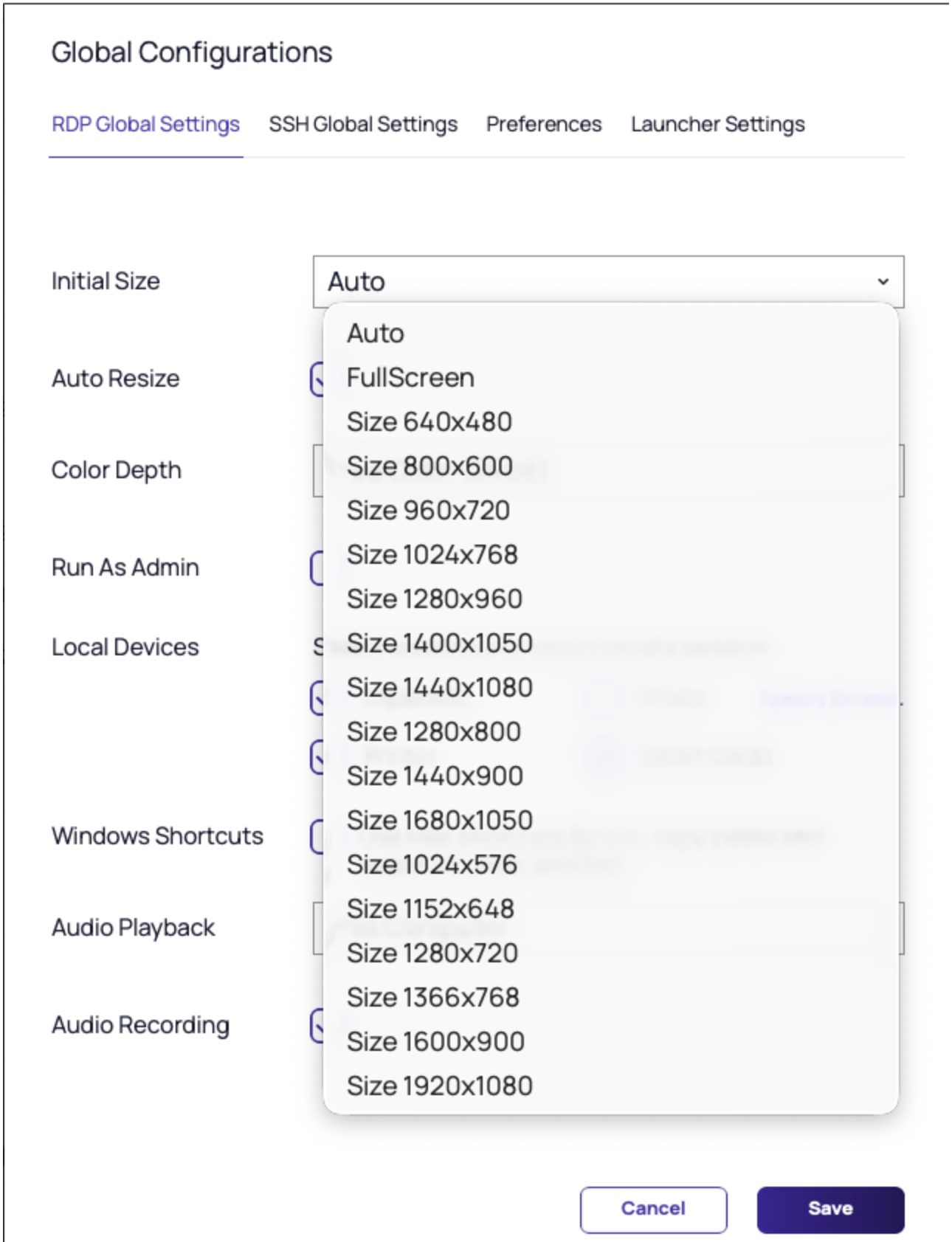
If you have a list of allowed domains in the registry editor, Connection Manager will only allow you to connect to the URLs in this allowed list via external browser:



If no values are added, all URLs will be allowed.

Desktop Size and Auto Expand

In the Global RDP Settings, users are able to select either a full screen, automatic or fixed desktop size:


Global Configurations
RDP Global Settings
SSH Global Settings
Preferences
Launcher Settings
Initial Size
Auto
Auto Resize
Color Depth
Run As Admin
Local Devices
Windows Shortcuts
Audio Playback
Audio Recording
Auto
FullScreen
Size 640x480
Size 800x600
Size 960x720
Size 1024x768
Size 1280x960
Size 1400x1050
Size 1440x1080
Size 1280x800
Size 1440x900
Size 1680x1050
Size 1024x576
Size 1152x648
Size 1280x720
Size 1366x768
Size 1600x900
Size 1920x1080
Cancel
Save

Note: Auto Resize is not supported on target systems running Windows Server 2012 or older.

Important: Auto resize is unavailable on macOS when proxy is enabled. Full screen mode is also unavailable for proxied connections launched via protocol handler.

The table below should be used as a guide into how an RDP session will be displayed depending on the chosen desktop size. The following settings are applicable for both Local and Global RDP connections.

Initial Size	Auto Resize	Connect	Expand	Shrink
Auto	Yes	Fill CM window	No rescale, border	Rescale image, no scrollbars
Auto	No	Fill CM window	No rescale, border	No rescale, scrollbars
Fixed	Yes	Fixed size, border	Fixed size, border	Rescale image, no scrollbars
Fixed	No	Fixed size, border	Fixed size, border	No rescale, scrollbars

Note: If RDP proxy is ON, no reconnect will be attempted because RDP proxy requires a one time password and it is impossible to reuse the same credentials to reconnect.

Automatic Back Up for .DAT Files and Configurations

Starting with the 2.7.0 release, Connection Manager automatically backs up your .dat files and application configurations by default.

Default Settings

By default, the parameters are set as follows:

On Windows:

```
<setting name="SettingsAutoBackup" serializeAs="String">
    <value>True</value>
</setting>
```

Note: Possible values are `True` or `False`.

```
<setting name="SettingsAutoBackupInterval" serializeAs="String">
    <value>UpgradeOnly</value>
```

```
</setting>
```

Note: The `SettingsAutoBackupInterval` can be set on a weekly or monthly basis. Available values are: *Weekly*,*Monthly* or *UpgradeOnly*.

On MacOS

```
defaults write com.Delinea.ConnectionManager Env.SettingsAutoBackup -bool true
```

Note: Possible values are `True` or `False`.

```
defaults write com.Delinea.ConnectionManager Env.SettingsAutoBackupInterval -UpgradeOnly
```

Note: The Env.SettingsAutoBackupInterval can be set on a weekly or monthly basis. Available values are: *Weekly* , *Monthly* or *UpgradeOnly*.

Adjusting the Default Settings

These settings can be adjusted in the `Delinea.ConnectionManager.exe.config` file on Windows or the `com.Delinea.ConnectionManager.plist` file on MacOS.

If you do not want Connection Manager to backup your .dat files and app configurations by default, set the value in the parameters listed above to `false`.

The following .dat files will be backed up:

- ApprovalSslStorage.dat
- Connection manager.dat
- PublicKeyFingerPrintStorage.dat
- Settings.dat
- TlsValidationStorage.dat

Restoring .DAT Files From Backup Location

To restore files from the backup location, select and copy the needed .dat files and paste them into the default .dat file folder:

Windows:

C:\Users\{username}\AppData\Roaming\Delinea\Connection Manager\ConnectionManager

MacOS:

/Users/{username}/Library/Application Support/Delinea/Connection Manager

Backup Locations

Windows:

- C:\Users\{username}\AppData\Roaming\Delinea\Connection Manager\ConnectionManager\Backups

MacOS

- /Users/{username}/Library/Application Support/Delinea/Connection Manager/Backups

Authenticating With WebAuthn

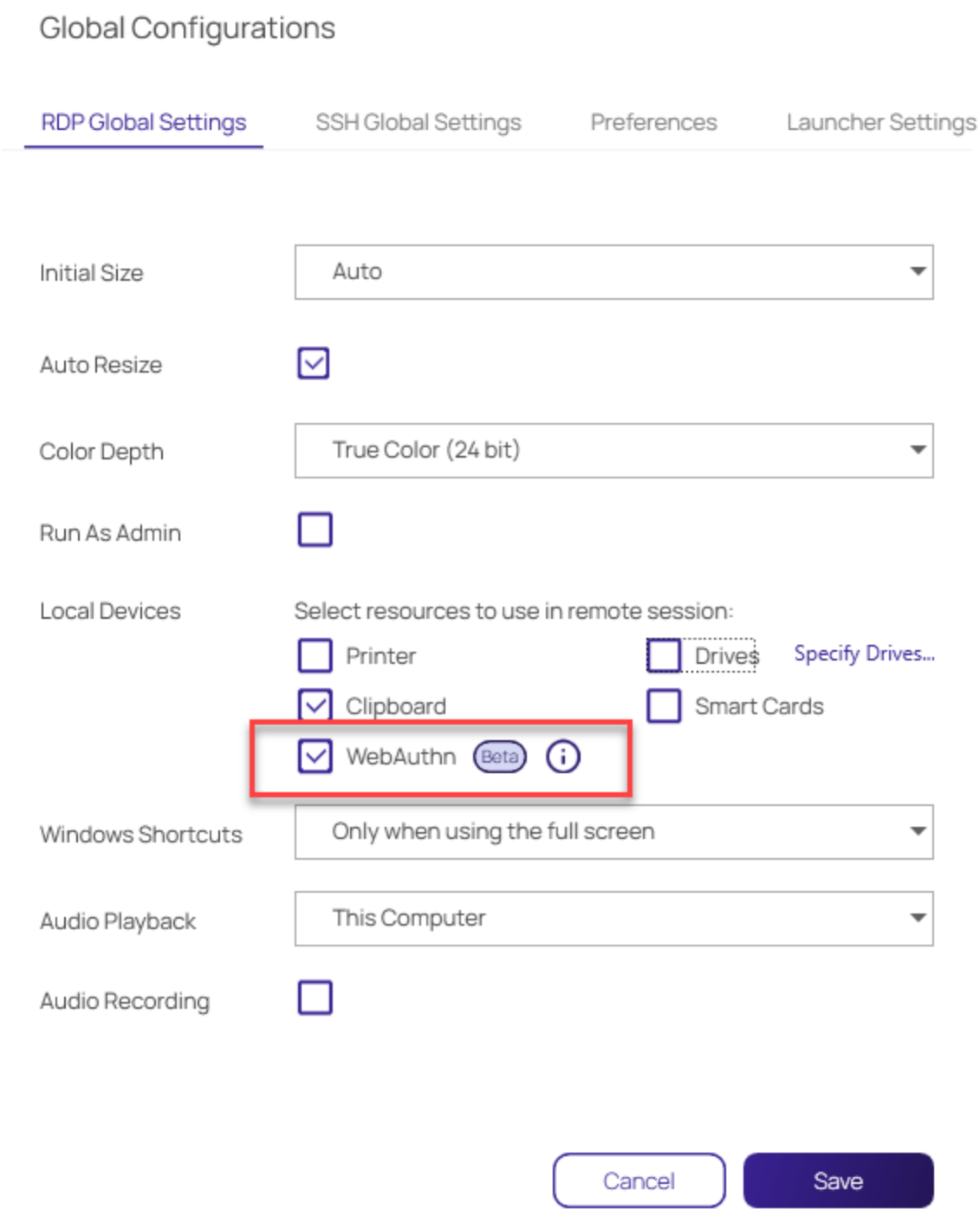
WebAuthn enables secure passwordless authentication using hardware security keys, biometrics or platform authenticators during remote RDP sessions. This feature is in beta and may change in future updates.

Note: WebAuthn redirection is not supported with distributed engine proxy.

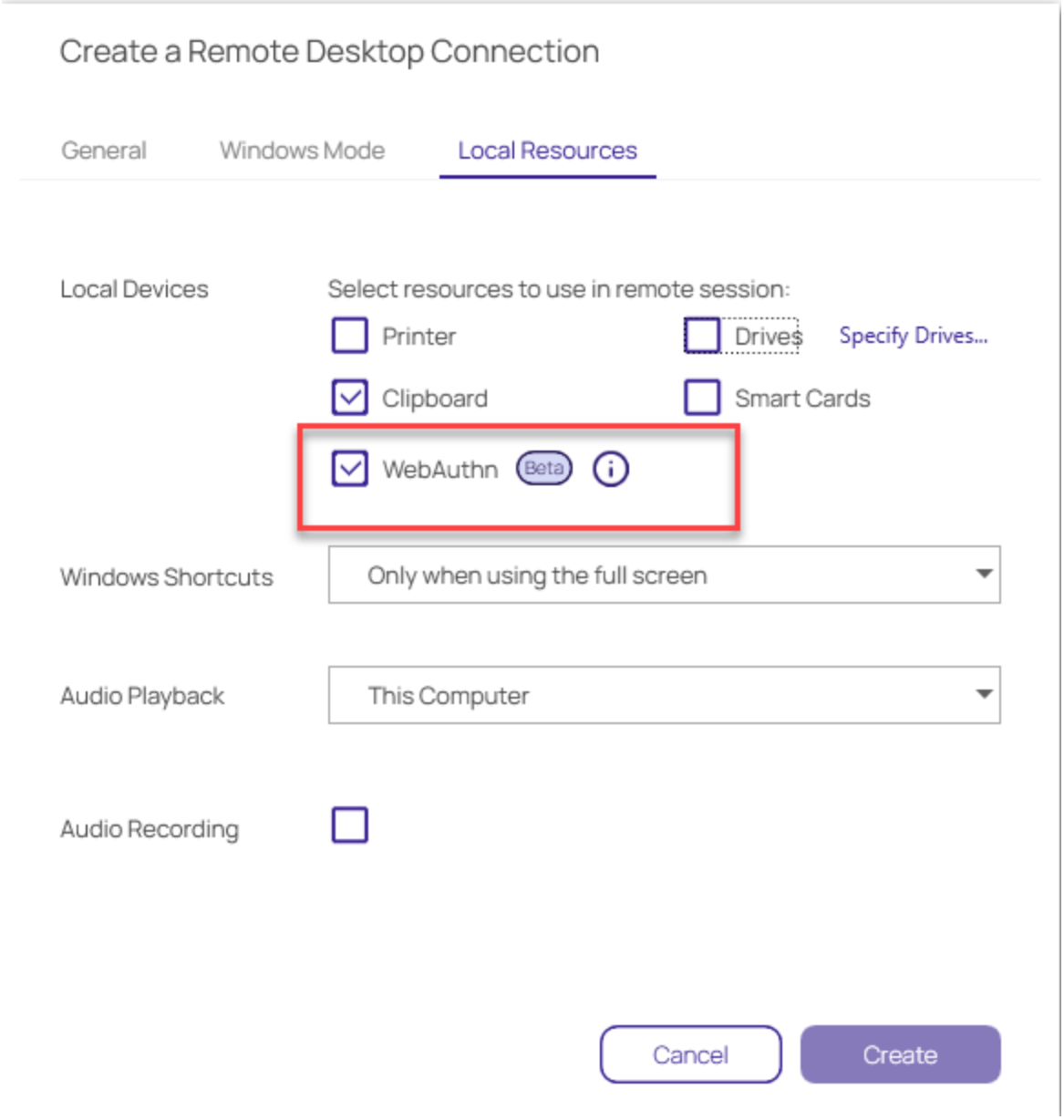
Enabling WebAuthn

WebAuthn is disabled by default. To enable WebAuthn authentication follow the steps below.

1. In the Global Configuration settings, check the WebAuthn box:



You can also enable WebAuthn redirection for local connections as well:



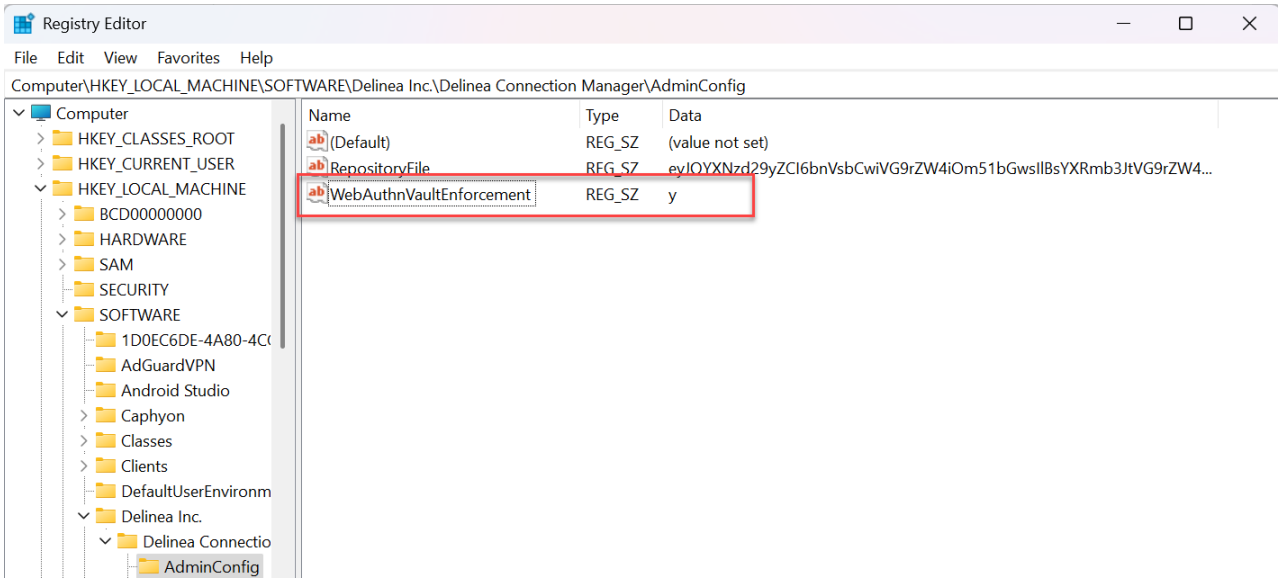
2. After you launch the application you will be able to use Yubikey as a FIDO2 key.

Enforcing Vault Authentication for WebAuthn on Windows

Admins can use these instructions to enforce whether users can connect to a vault with WebAuthn authentication.

1. Open the Connection Manager Registry editor which can be found via the following path:
   `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Delinea Inc.\Delinea Connection Manager\AdminConfig`

2. Create a value in the Registry called `WebAuthnVaultEnforcement` and input `y` as the parameter.



Enforcing Vault Authentication for WebAuthn on MacOS

Run the following command in the terminal:

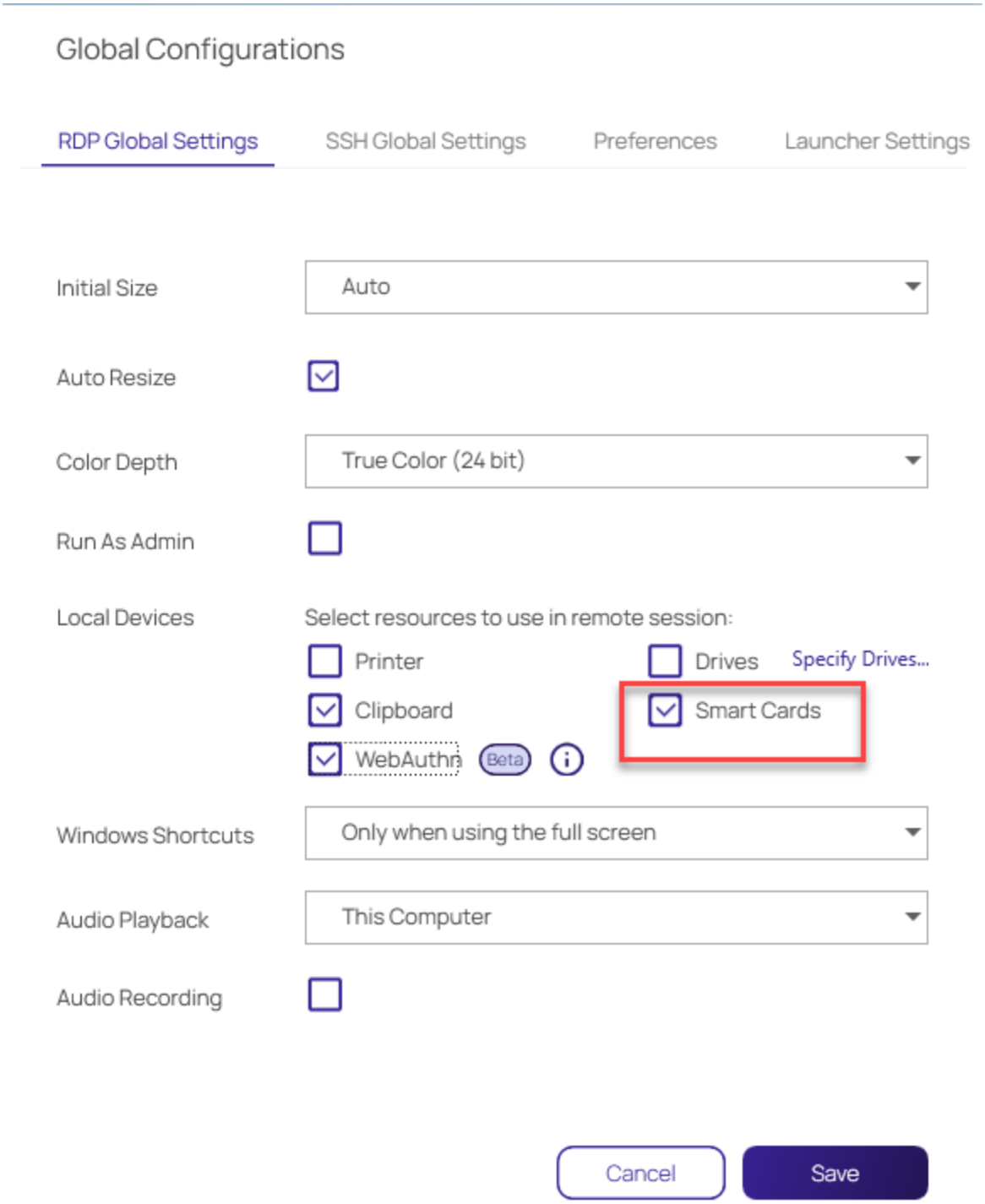
```
defaults write com.Delinea.ConnectionManager webauthnvaultenforcement y
```

Using Smart Cards With Connection Manager

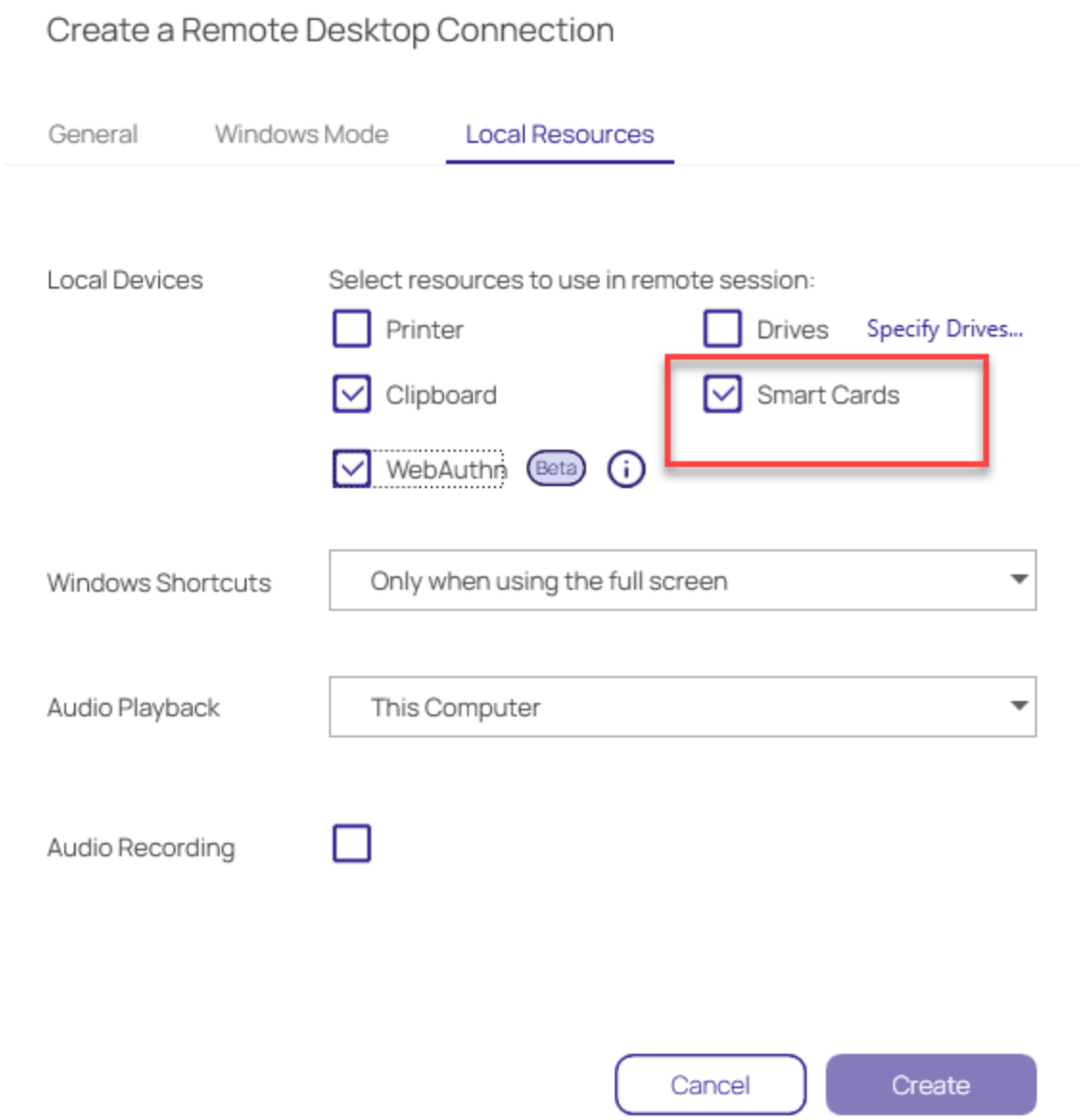
Smart Card Settings

If you are using local secrets, you can enable Smart Card sharing in the Global Configuration Settings and your local vault:

Global Configurations:


Global Configurations
RDP Global Settings
SSH Global Settings
Preferences
Launcher Settings
Initial Size
Auto
Auto Resize
Color Depth
True Color (24 bit)
Run As Admin
Local Devices
Select resources to use in remote session:
Printer
Drives
Specify Drives...
Clipboard
Smart Cards
WebAuthn
Beta
Windows Shortcuts
Only when using the full screen
Audio Playback
This Computer
Audio Recording
Cancel
Save

Local Vault:

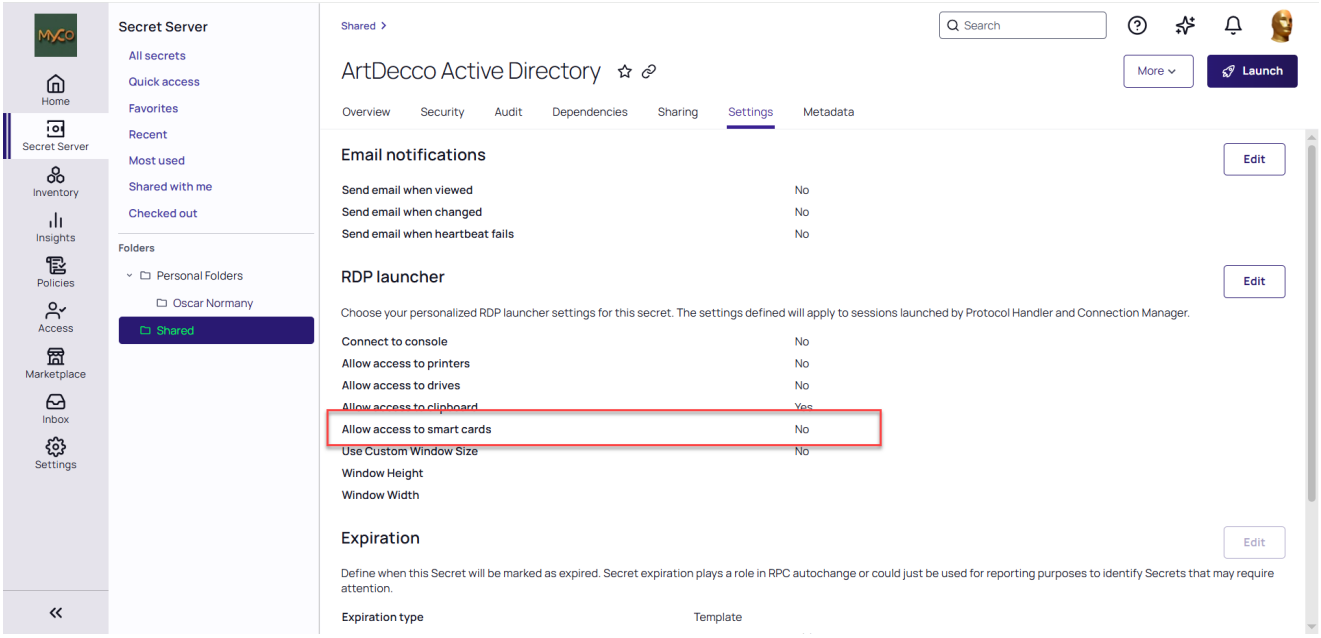


Note: For local secrets, the Smart Card settings on the secret override the Global Configuration Settings.

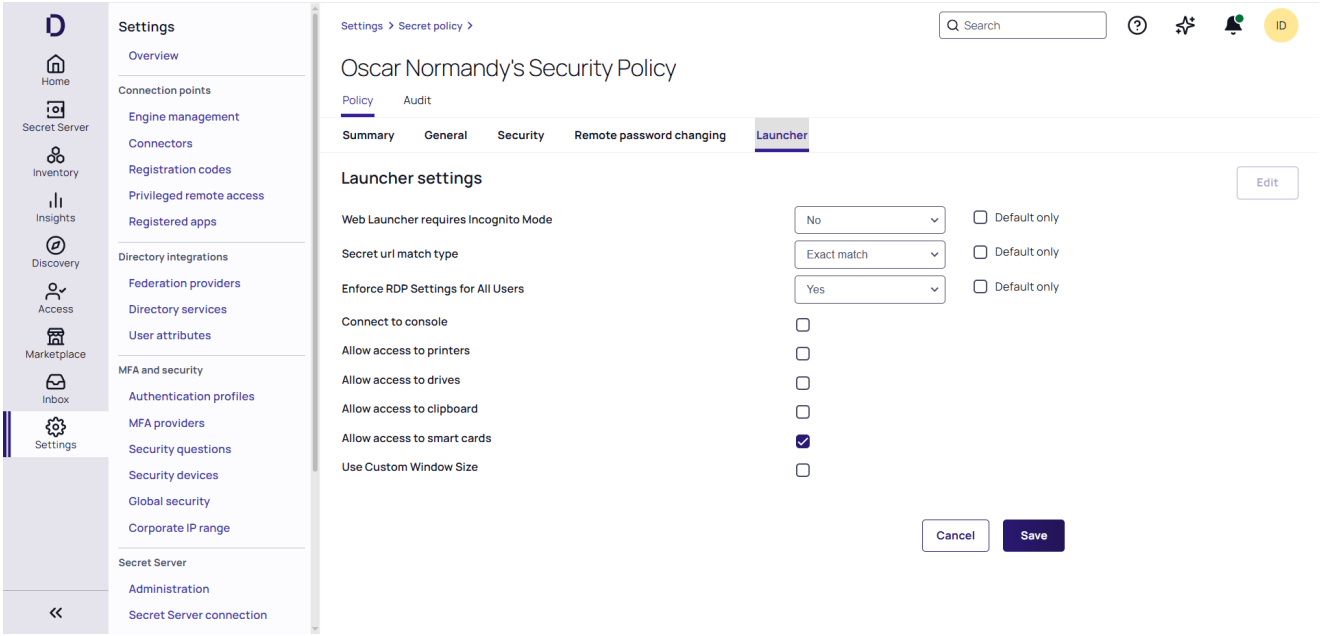
If you are accessing secrets stored in a Delinea vault, the Smart Card settings will also depend on the server's RDP policy:

Secret Settings:

Global Configuration Settings



Security Policy:



Note: For secrets stored in a Delinea vault, the Smart Card settings on the secret override the policy settings.

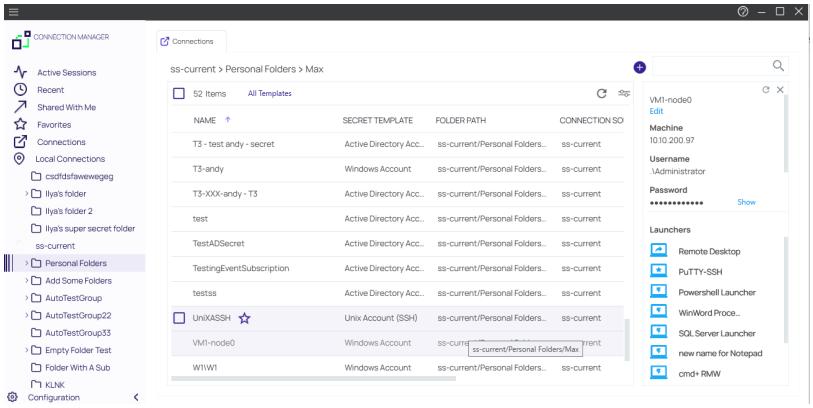
If you are experiencing issue when using Smart Cards, refer to "Troubleshooting Issues With Smart Cards" on page 226.

Launchers

Connection Manager can act as a protocol handler, which means that Connection Manager can launch Secret Server Secrets that use other Launcher types directly from the Connection Manager UI. Connection Manager supports any launcher that is supported by Secret Server and includes, but is not limited to: PowerShell, CmdLine, MS Word, Notepad, Excel. These launchers also support opening a tab in Connection Manager, session recording, and workflows.

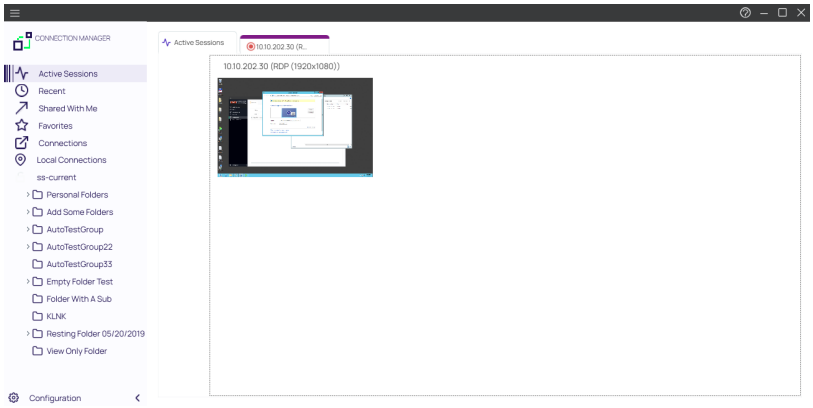
Note: Launching Secret Server session connector launchers is supported on Windows only.

Note: ActiveX components will not be recorded.



Note: The number of launchers visible in the right navigation panel will depend on your screen size, screen resolution, and text size. The below matrix offers approximate guidance in terms of the number launchers visible:

Screen Size	Screen Resolution	Screen Scale	Font Size	# of Launchers
27 in	4k	100%	Normal	25+
15 in	4k	225%	Normal	<25



The Secrets with launcher can be launched in the Secret Server UI and have the protocol handler open and run the launcher in Connection Manager. The Secret needs to be configured to use the protocol handler, and when launched it uses Connection Manager if available. When Connection Manager opens, it will be in a "Locked" state, with only the Secret Server launched session(s) being available. Please note that when launching a connection from protocol handler you will not be able to reconnect.

If Connection Manager is launched using the protocol handler and is in the "Locked" state, users have a "Sign In" option available to fully log into Connection Manager to use their other connections.

When a remote session is connecting over a proxy, the connection tab displays the remote host name instead of the local host name.

Note: Local Connections are limited to RDP and SSH launchers.

Proxy Tabs Show Remote Host Name

When a session is connecting through a proxy, the tab label displays the identity of the remote host.

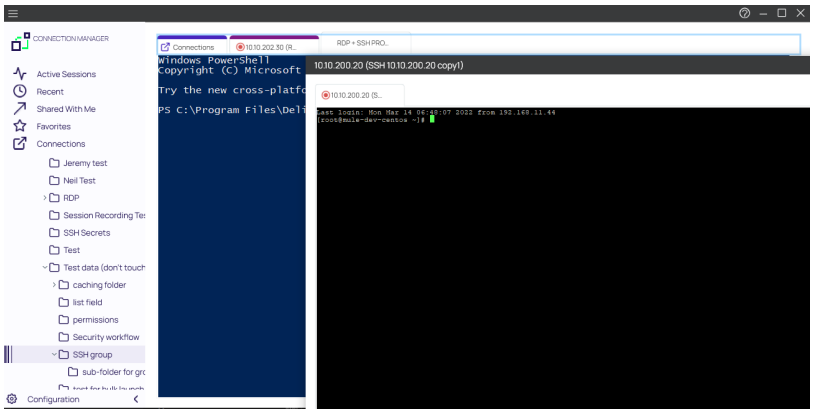
Screen Resolution for New Session Window Views

When you maximize an active RDP session window or you drag it as a standalone window to a second monitor, the session automatically disconnects and reconnects so it can use the highest supported screen resolution for the new window view. When you do the same with an active RDP *Proxy* session window, the session cannot automatically reconnect because RDP Proxy sessions launch with a one-time password (OTP) that cannot be regenerated. Therefore an RDP Proxy session cannot use the highest supported screen resolution for a new window view. Note: no RDP session of any kind can use the highest supported screen resolution for a new window view if the default setting for Desktop Size has been changed from **Auto** to a fixed size under RDP Global Settings.

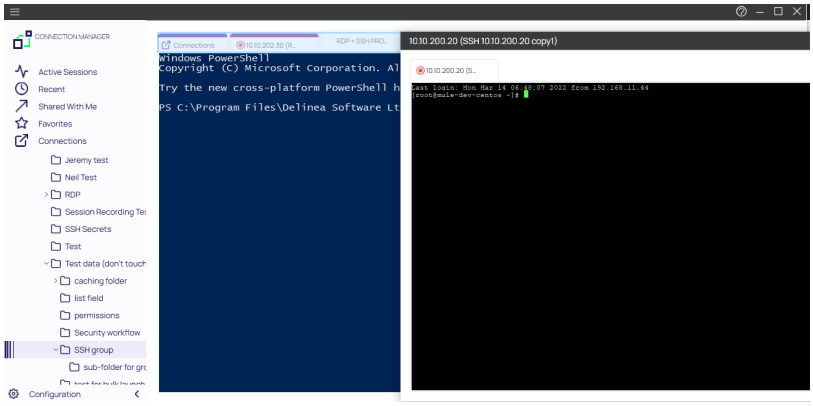
Moving and Reorganizing Session Tabs and Windows

You can undock, move, and redock session tabs and windows in Connection Manager. To undock a session window, click the session tab and drag it out of the tab dock area. The tab becomes a standalone session window, which you can drag to another monitor or to another location on your desktop.

To redock a session window, click and drag it toward the row of docked tabs in the main Connection Manager window. As you drag the window close to the tab dock, a blue line appears around the dock:



When you drag the window onto the tab dock, the dock turns light blue to indicate that you can drop the window:



Session Recording

If session recording is configured to run only on the primary secret, only the primary session will be recorded. If the secret is configured to record multiple windows, Connection Manager honors the setting and all sessions started from the initial session are also recorded.

For third-party launchers, session recording is limited to using the *custom app* option, rather than batch scripts. This is because, with the custom app option, Connection Manager can accurately identify the process ID of your application and ensure that the main window is recorded and sent to the server. This approach helps Connection Manager deliver a consistent and high-quality recording experience for your sessions.

The default screenshot queue limit is set to 0 in the Application Configuration file, but, if you are experiencing a slow internet connection speeds or interruptions, Delinea recommends increasing the *ScreenshotsQueueLimit* to any positive value, such as 30 screenshots. The greater the value you set, the more screenshot data will be queued before the session is terminated. Please see "Setting the Screenshot Queue Limit" on page 180 for more information.

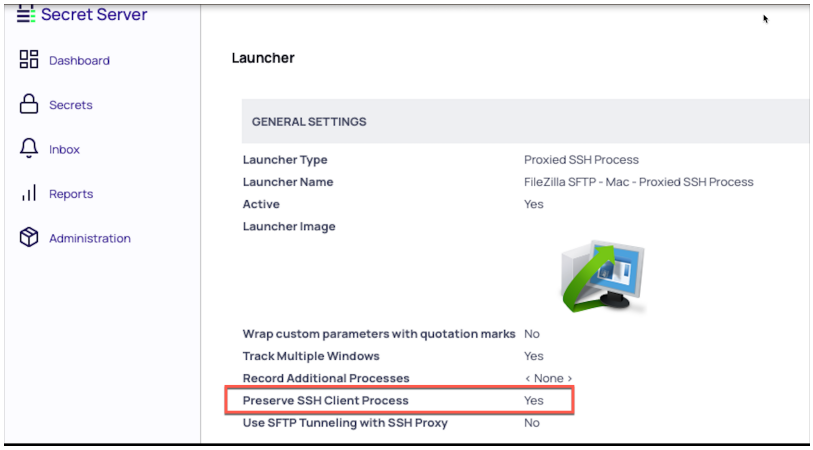
A typical example are Xming implementations of Secure Shell (SSH) to securely forward X11 sessions from other computers. While recording an Xming session, all windows created are recorded and if a user tries to use X11 forwarding for example in Chrome, the new Chrome window will be recorded too.

Note: Connection Manager requires a connection to the internet for the session recording functionality to work.

Note: If you are running Windows 11 applications, such as Notepad or Paint, while session recording is enabled, make sure to close these application windows before starting the recording.

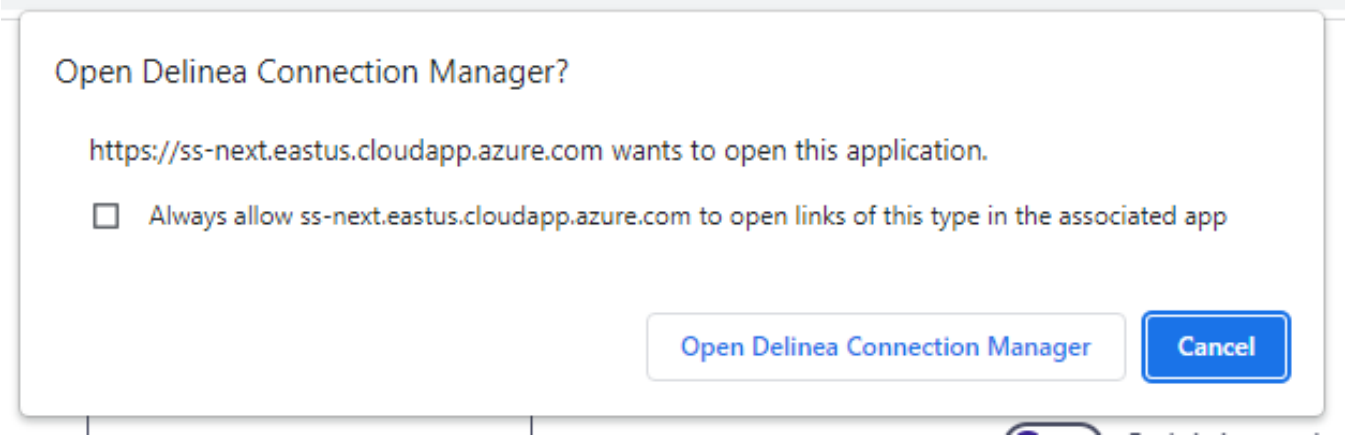
Working With Third-Party Applications (Preserve SSH Client Process)

When using Connection Manager with third-party applications, users will need to create a custom launcher for their application. If the user closes the Connection Manager tab, the third-party application will not close unless *Proxied SSH Process* is set and the flag *Preserve SSH Client Process - True* is enabled.

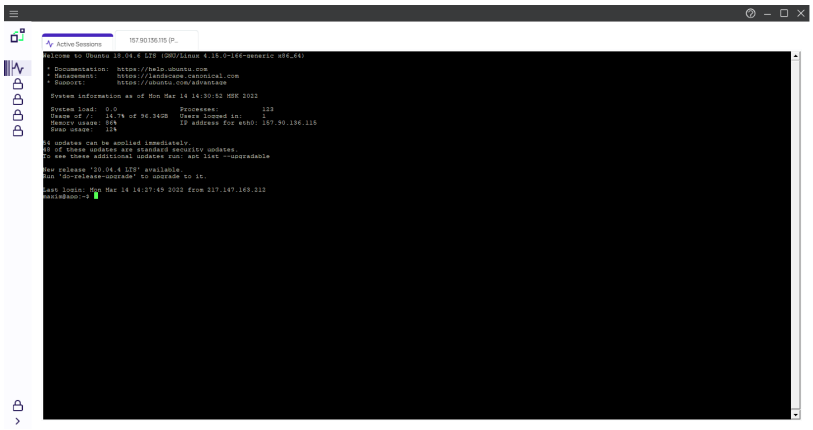


Launching from Secret Server without Connection Manager Open

If a protocol handler is launched from Secret Server, without having an open Connection Manager, the **Open Connection Manager?** window opens:

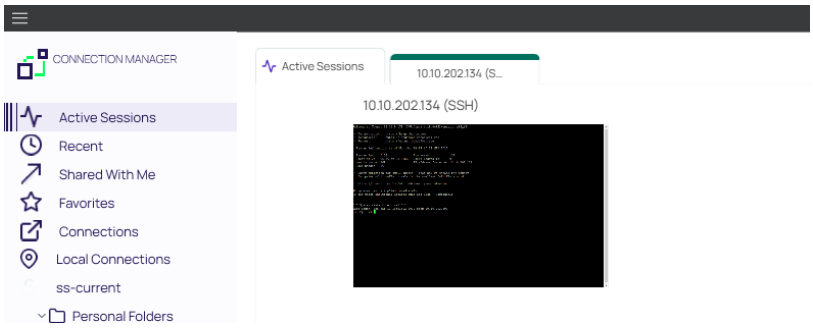


Click **Open Connection Manager** and an active session is launched in Connection Manager:



In this example the application was opened and placed inside the new tab. Certain applications won't fit in the tab and will be opened in an independent window outside the tab. Other windows opened by the user won't be placed inside the tab either, but everything that originated from the originally launched application will be tracked.

For applications launched from within a Secret Server, the other configured local and existing Secret Server connections remain locked in Connection Manager.

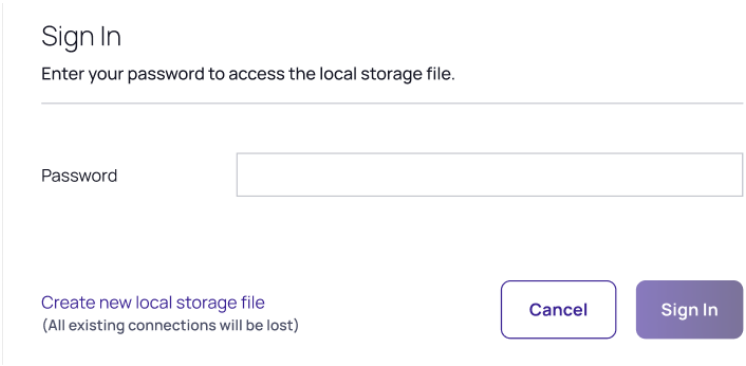


Only navigation between different Active Session tabs initiated from Secret Server is possible.

Signing In After the Launch

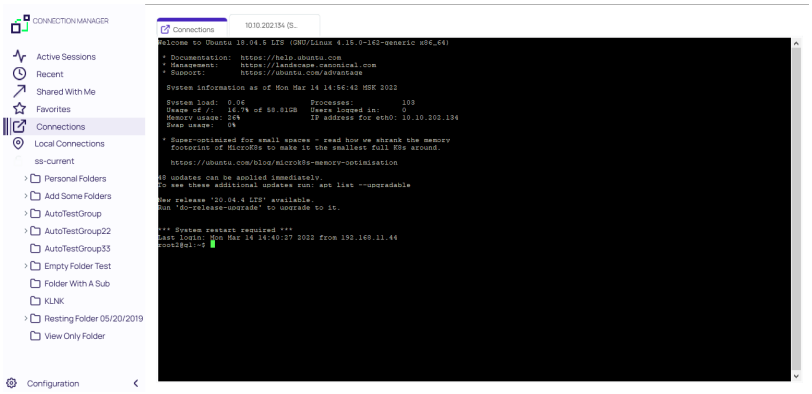
To sign in after an app launch was initiated from Secret Server,

1. From the hamburger menu, select **File | Sign in** or right-click on Active Session and select **Sign in**.



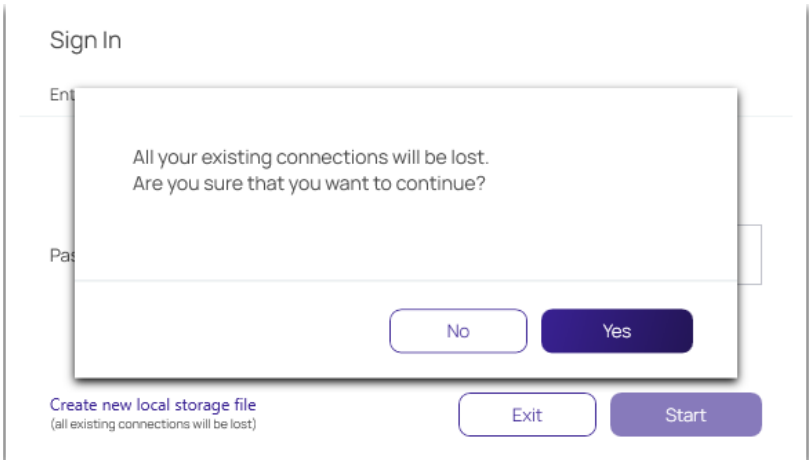
2. Enter your password.
3. Click **Sign In**.

Once signed in, the user has access to all connections and all Connection Manager functionality is unlocked.



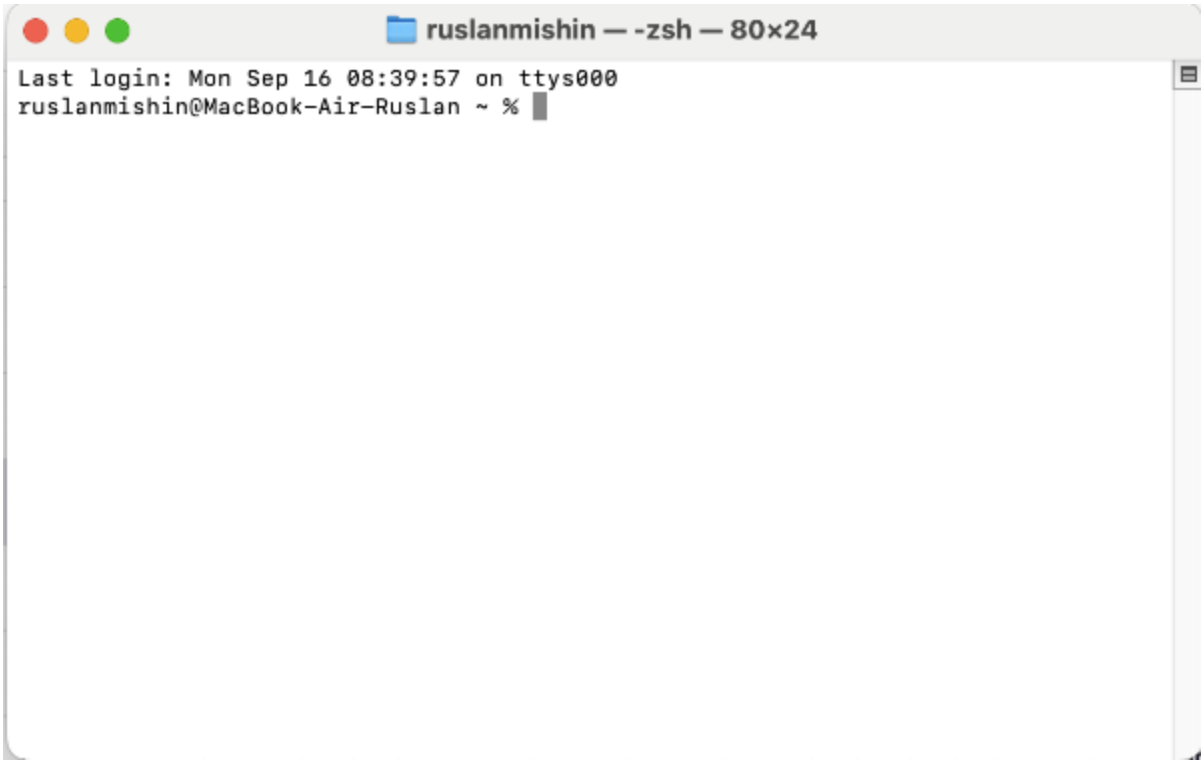
Creating a New Local Storage File

During the sign in, users can select to create a new local storage file by clicking the link in the sign in window:



Note: If this option is used, existing connections will be lost.

Solution Guide: Launching SSH Sessions with Mac-Native SSH Client



These instructions show how to launch SSH sessions through Delinea Connection Manager to the Mac-native SSH client on MacOS. This allows users to use the Mac-native SSH client as their preferred terminal implementation.

Use Cases

Starting in Connection Manager 2.5.3, the Mac-native SSH client supports the ability to launch usernames and passwords as well as private keys over proxy. It does not support private keys without proxy or sessions with session recording.

Prerequisites

Prior to using the Mac-Native SSH Client, users need to verify that they have:

1. Connection Manager version 2.5.3 installed or newer on the client machine.
2. A secret configured with SSH proxy to the target machine
3. GPG installed on the client machine. This can be accomplished by running the following terminal command:

```
brew install gpg
```

Note: Connection Manager will look for GPG in the default homebrew folder. If users want to install GPG in a different location, users must pass the modified path to the folder as a launcher argument: *--environment-path /your/path*

Setup

Step 1: Create a Custom Launcher in Secret Server

Follow the directions for creating a custom launcher using the parameters named below:

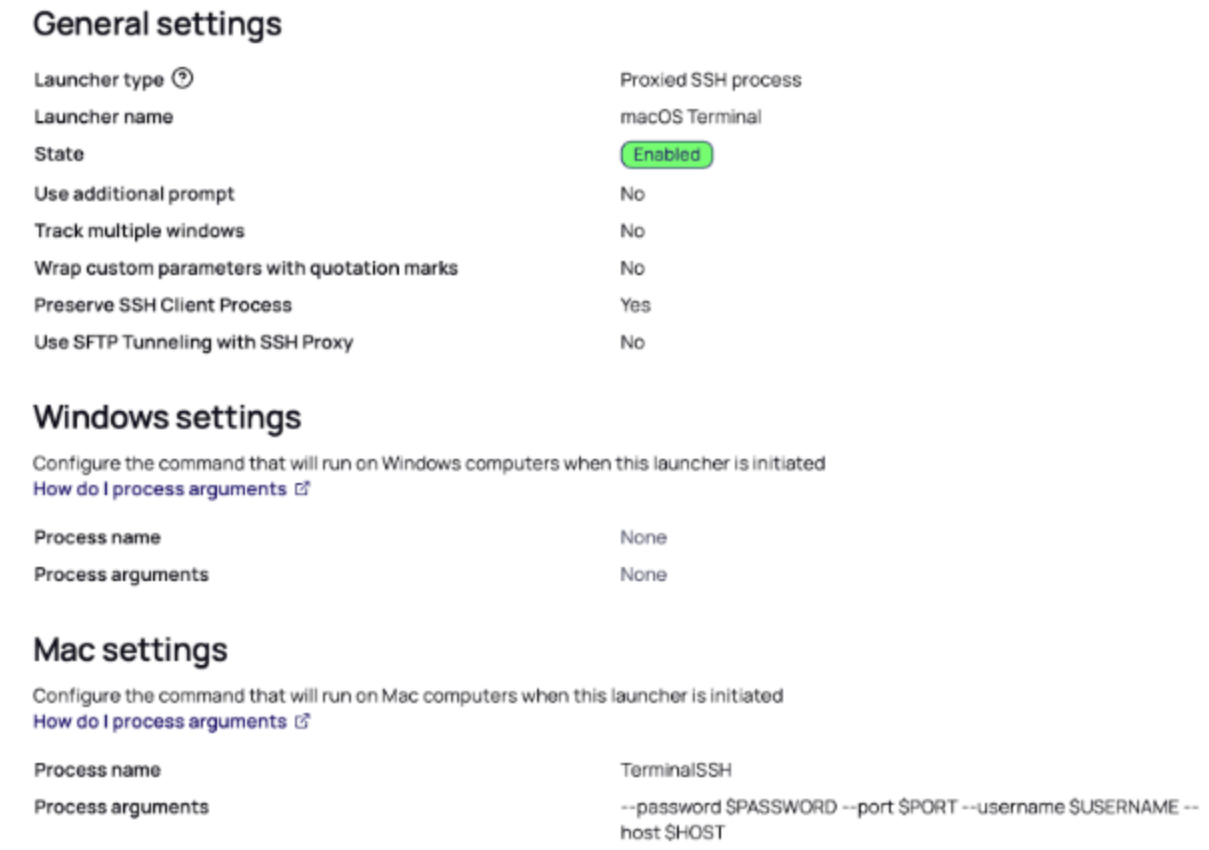
General Settings

- **Launcher Type**: Proxied SSH process
- **Launcher Name**: macOS Terminal
- **State**: Enabled
- **Preserve SSH Client Process**: Yes

MacOS Settings

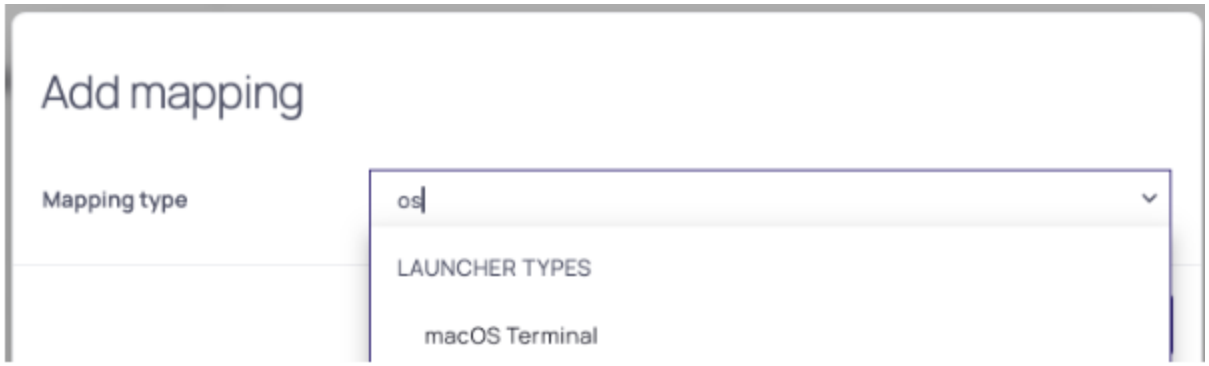
- **Process Name**: TerminalSSH
- **Process Arguments**: *--password $PASSWORD --port $PORT --username $USERNAME --host $HOST*

Note: *If GPG was installed to a non-default location, add the following process argument: --environment-path /your/paths*



Step 2: Map the New Launcher to the SSH Secret Template in Secret Server

Follow the directions for editing a secret template to map the macOS Terminal launcher to the appropriate SSH secret template (e.g., Unix Account (SSH)). Be sure to map the launcher fields as shown below.



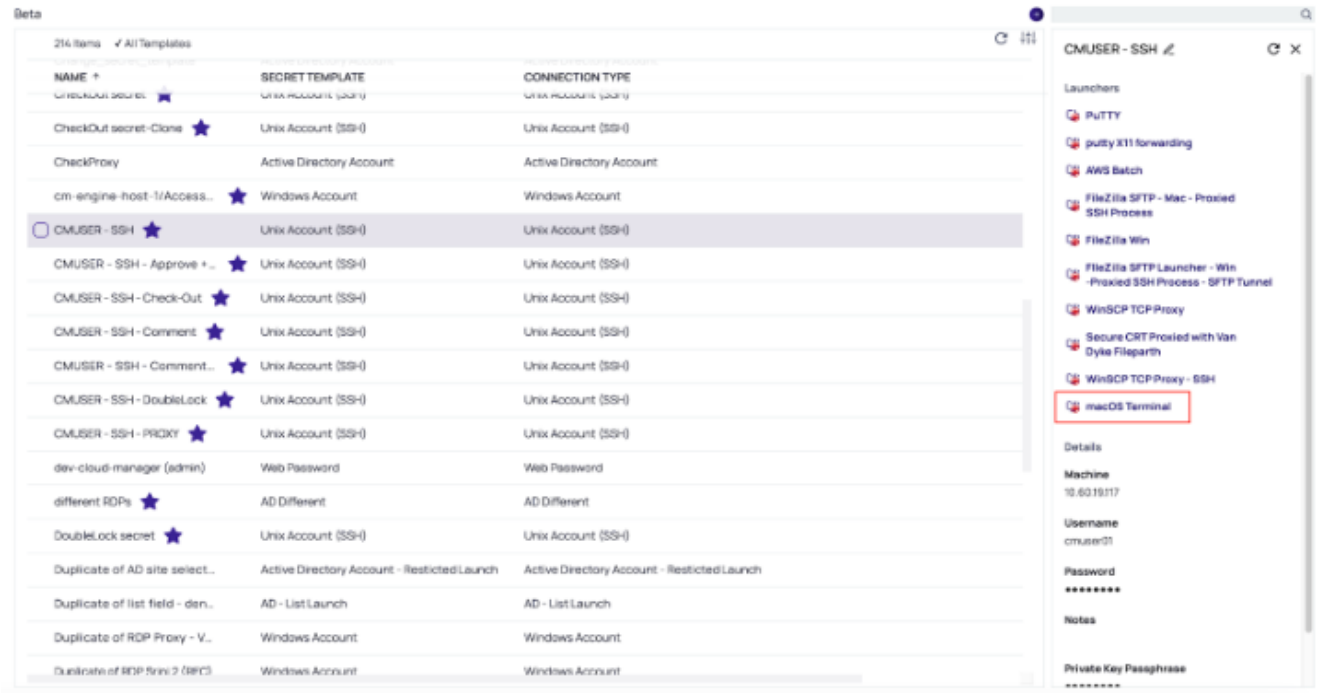
Launchers

Launcher name	macOS Terminal	Remove Edit
Restrict user input	No	
Fields		

LAUNCHER FIELD	SECRET FIELD
Host	Machine
Password	Password
Port	22
Username	Username

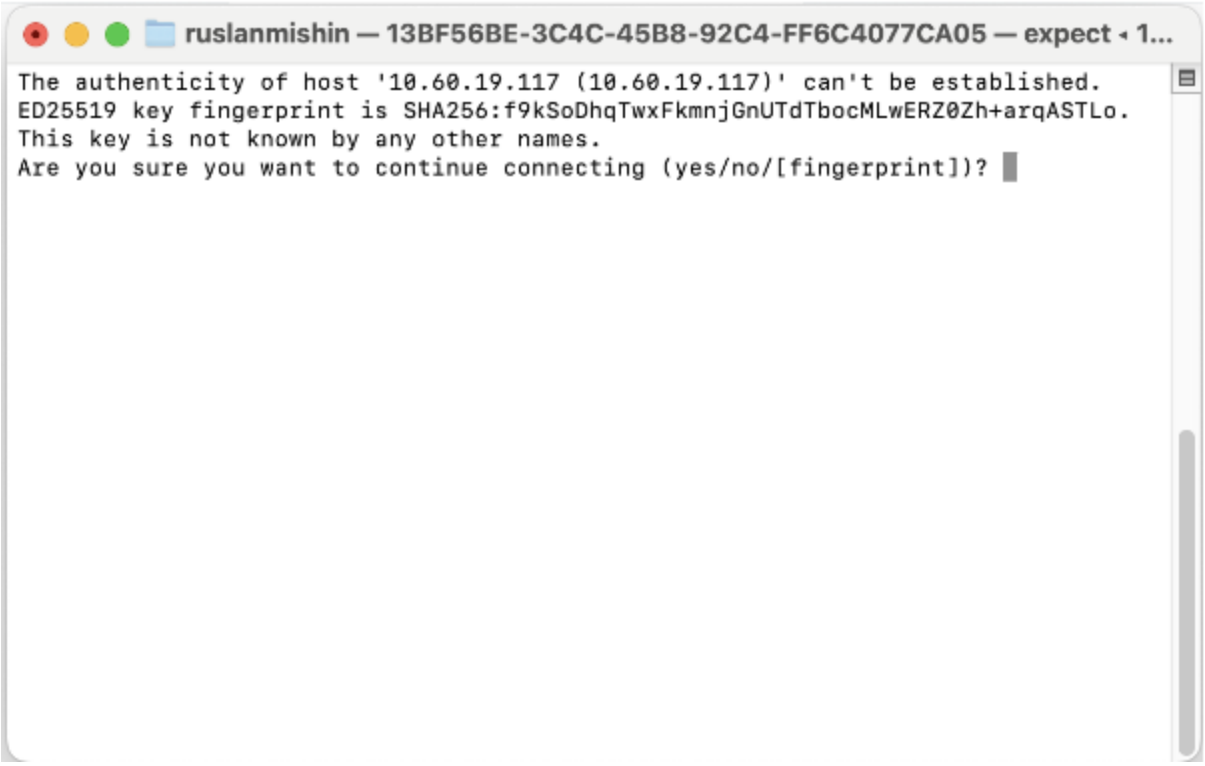
Step 3: Launch SSH Secret from Connection Manager

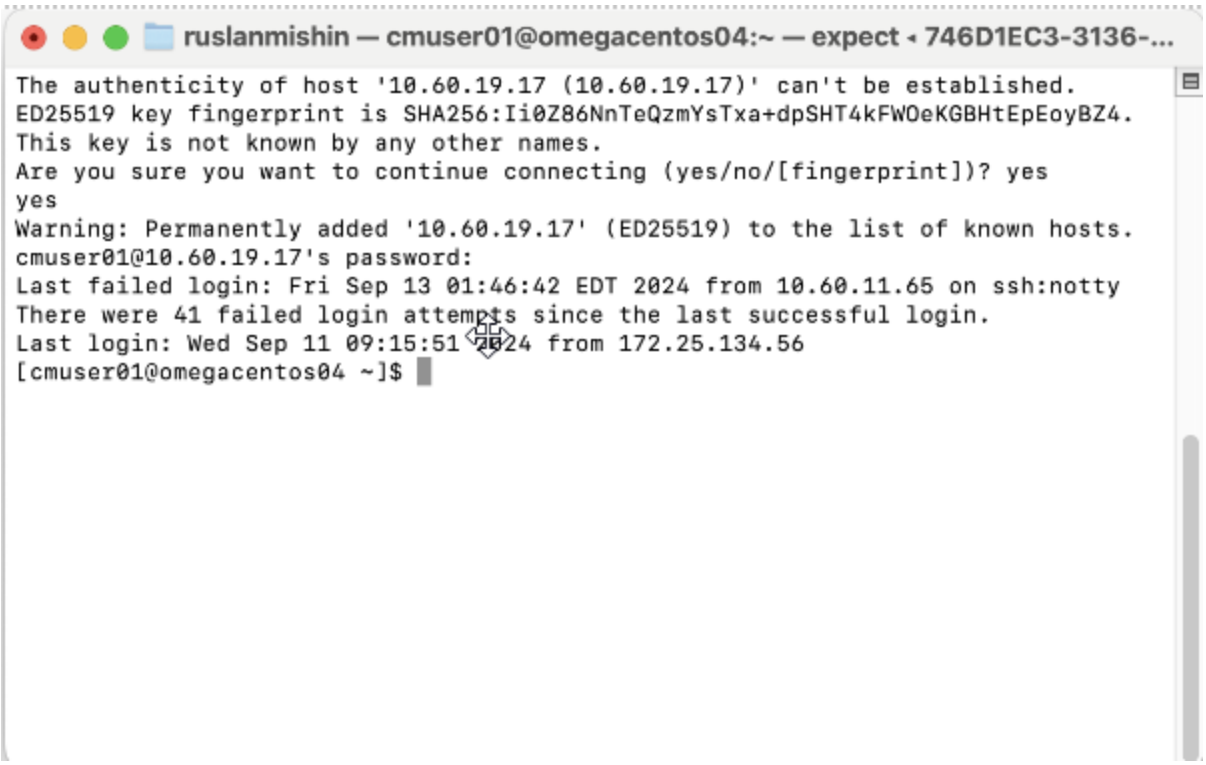
Within the Connection Manager application, authenticate to the desired vault and use macOS Terminal as the secret launcher rather than PuTTY.



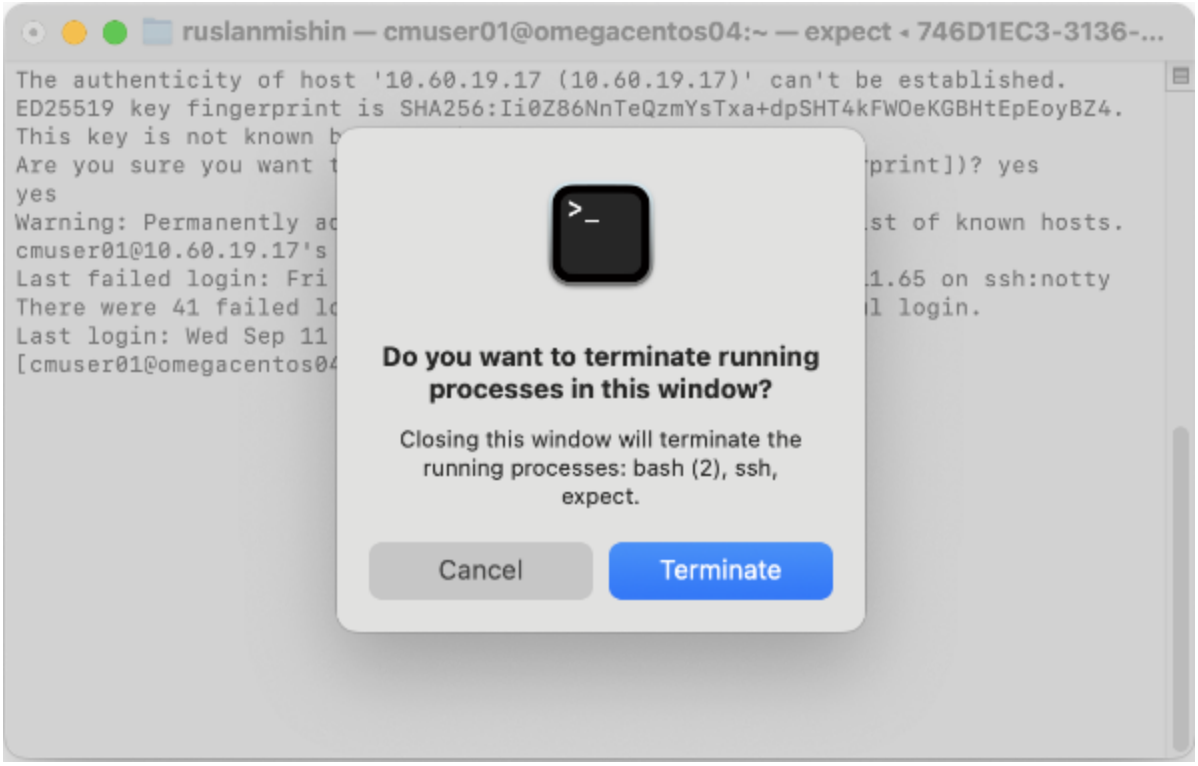
The macOS Terminal should open for the selected secret.

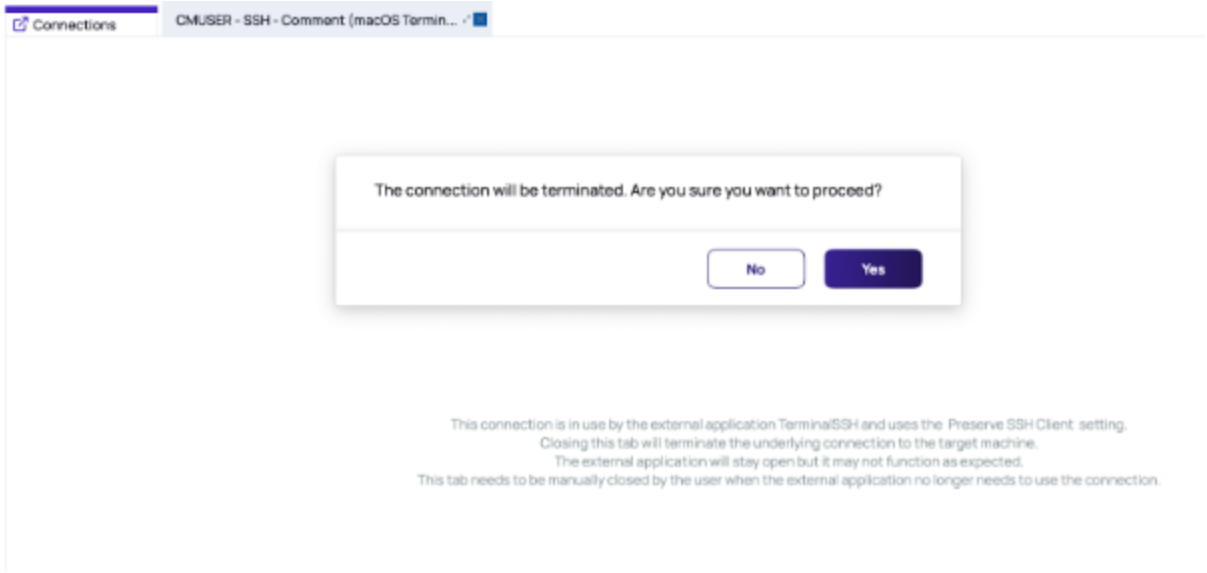
On first launch, users may see a terminal window asking to save the fingerprint key. Enter yes to confirm the connection fingerprint as a known host.





When tasks on the connection are complete, please ensure the terminal is terminated. Because the Preserve SSH Flag setting is required, it is important to close these tabs correctly.

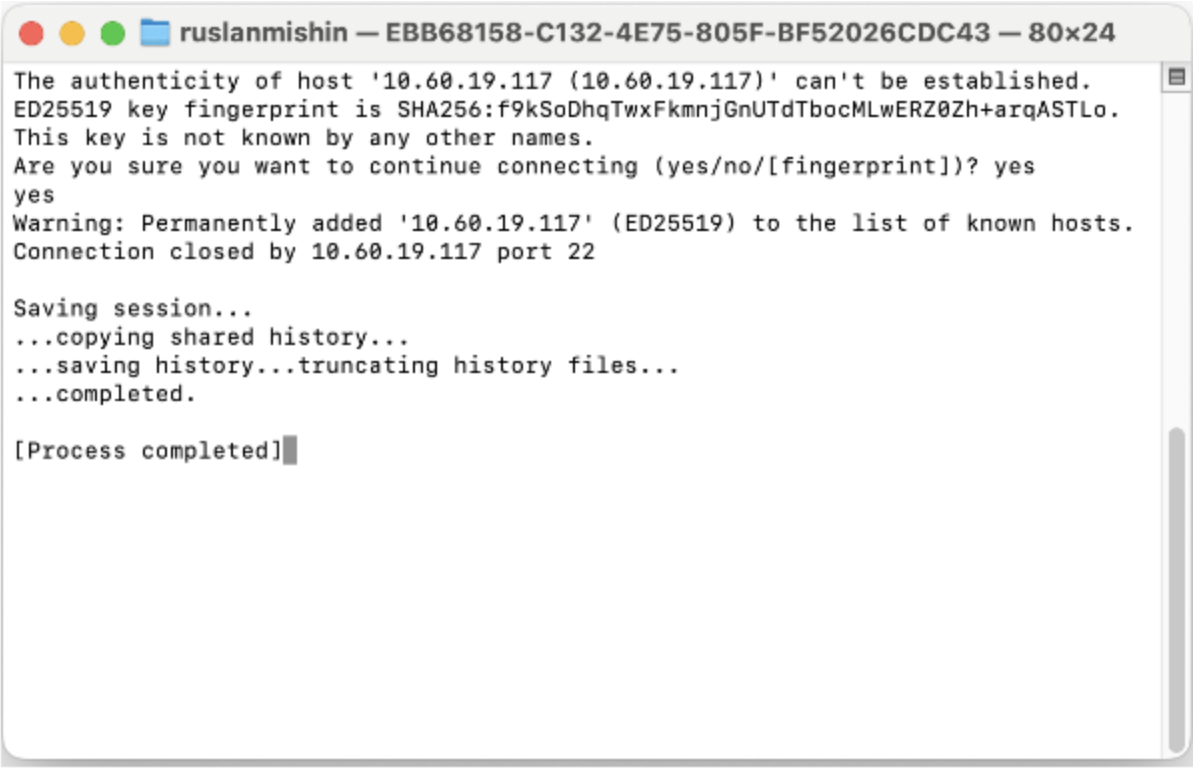

ruslanmishin — cmuser01@omegacentos04:~ — expect ◂ 746D1EC3-3136-...
The authenticity of host '10.60.19.17 (10.60.19.17)' can't be established.
ED25519 key fingerprint is SHA256:Ii0Z86NnTeQzmYsTxa+dpSHT4kFWOeKGBHtEpEoyBZ4.
This key is not known b
Are you sure you want t
print])? yes
yes
Warning: Permanently ad
st of known hosts.
cmuser01@10.60.19.17's
Last failed login: Fri
1.65 on ssh:notty
There were 41 failed lo
l login.
Last login: Wed Sep 11
[cmuser01@omegacentos04
Do you want to terminate running processes in this window?
Closing this window will terminate the running processes: bash (2), ssh, expect.
Cancel
Terminate


Connections
CMUSER - SSH - Comment (macOS Termin...
The connection will be terminated. Are you sure you want to proceed?
No
Yes
This connection is in use by the external application TerminalSSH and uses the 'Preserve SSH Client' setting.
Closing this tab will terminate the underlying connection to the target machine.
The external application will stay open but it may not function as expected.
This tab needs to be manually closed by the user when the external application no longer needs to use the connection.

Known Issues

Fingerprint Confirmation

If the fingerprint is confirmed after 2 minutes or longer, it will still be accepted by the system; however, the user will need to reconnect because the connection will timeout.



Attaching Files to Secret Launchers

This section contains information about:

- "Attaching Files to Secret Launchers on Windows " below
- "Attaching Files to Secret Launchers on MacOS" on page 152

Attaching Files to Secret Launchers on Windows

Step 1: Creating a Custom Launcher

1. Navigate to the **Secret templates** page in Secret Server and click the Launchers tab.
2. Click **Create**.
3. Enter the launcher information as shown below:

   General Settings

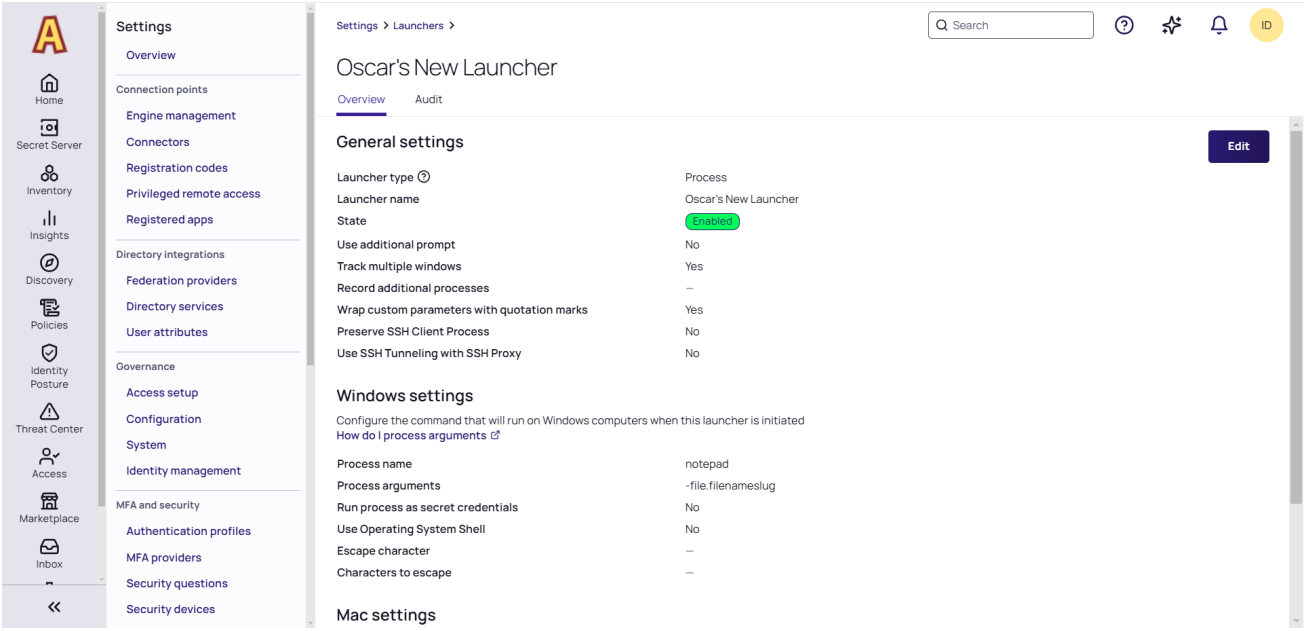
- **Launcher Type**: Process
- **Launcher Name**: [Enter launcher name]
- **State**: Enabled
- **Preserve SSH Client Process**: No
- **Use SSH Tunneling with SSH Proxy**: No

Windows Settings

- **Process name**: [Full path to file]
- **Process arguments**: -file.filenameslug

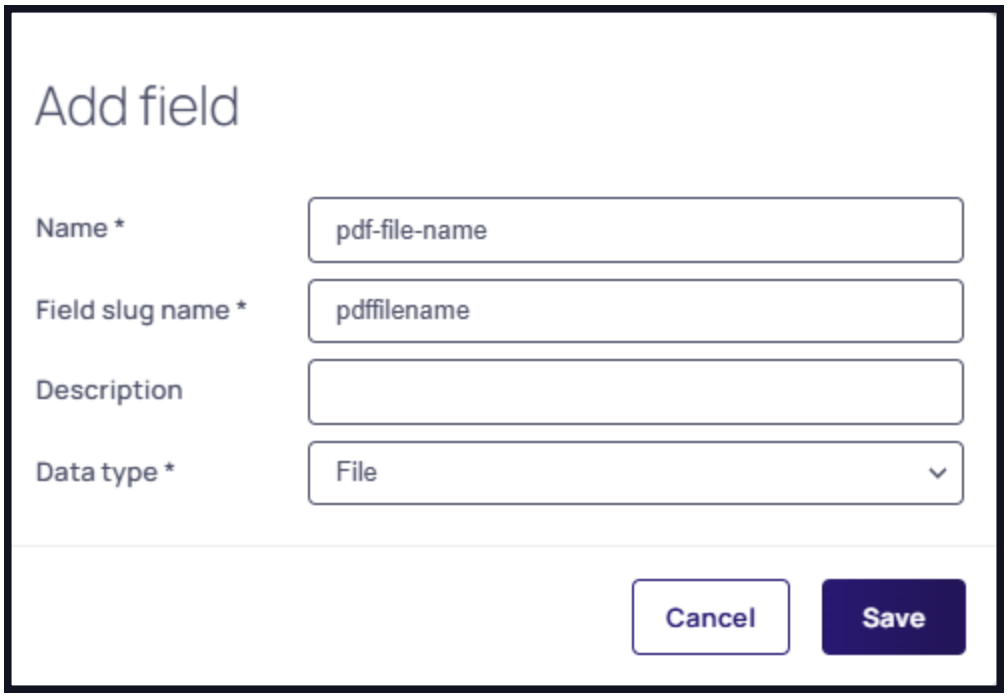
> **Note:** -file.filename slug must match the field in the secret template where the attachment is located.

- **Run process as secret credentials**: No
- **Use Operating System Shell**: No

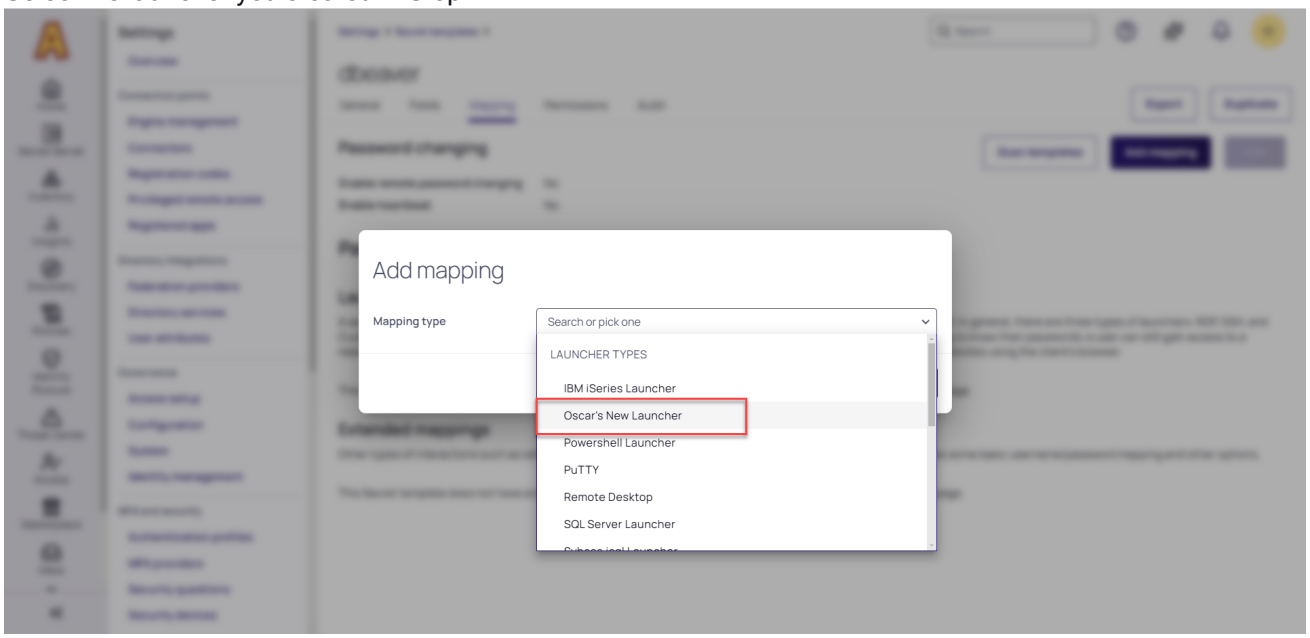


Step 2: Creating a Custom Template

1. Create a new template inside Secret Server
2. Select the **Fields** tab and add a new field for each file you would like to launch. Make sure that the *Data type* is set to **File**.



3. Select the **Mapping** tab and click **Add mapping**.
4. Select the launcher you created in Step 1:



5. Map the fields from the templates to the launcher.
6. Launch the secret.

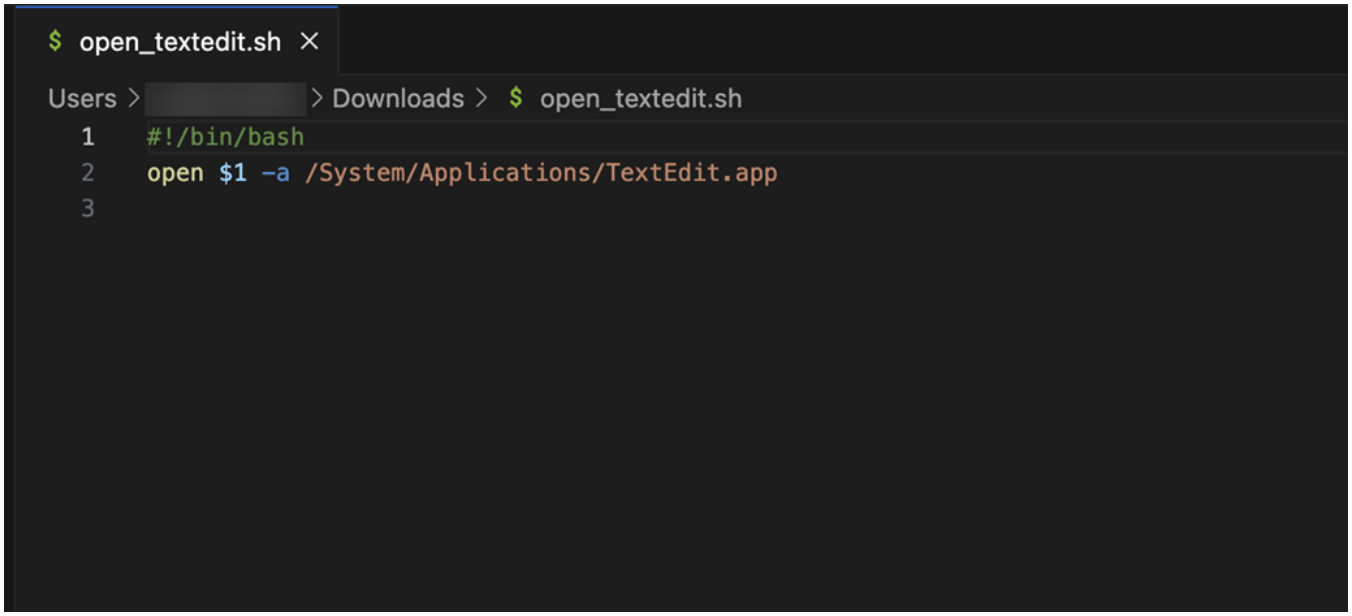
Attaching Files to Secret Launchers on MacOS

Step 1: Creating a Custom Script for Your Application

Create a shell script, containing the full file path to your application, in the following format:

```
#!/bin/bash\
open $1 -a "/Applications/PDF/[AppName].app
```

Example:



Step 2: Creating a Custom Launcher

1. Navigate to **General Settings > Secret Templates > Launchers**.
2. Click **Create**.
3. Enter the launcher information as shown below:

   General Settings

   - **Launcher Type**: Batch file
   - **Launcher Name**: [Enter launcher name]
   - **State**: Enabled
   - **Use additional prompt**: No
   - **Track multiple windows**: Yes
   - **Record additional processes**: None
   - **Wrap custom parameters with quotation marks**: Yes

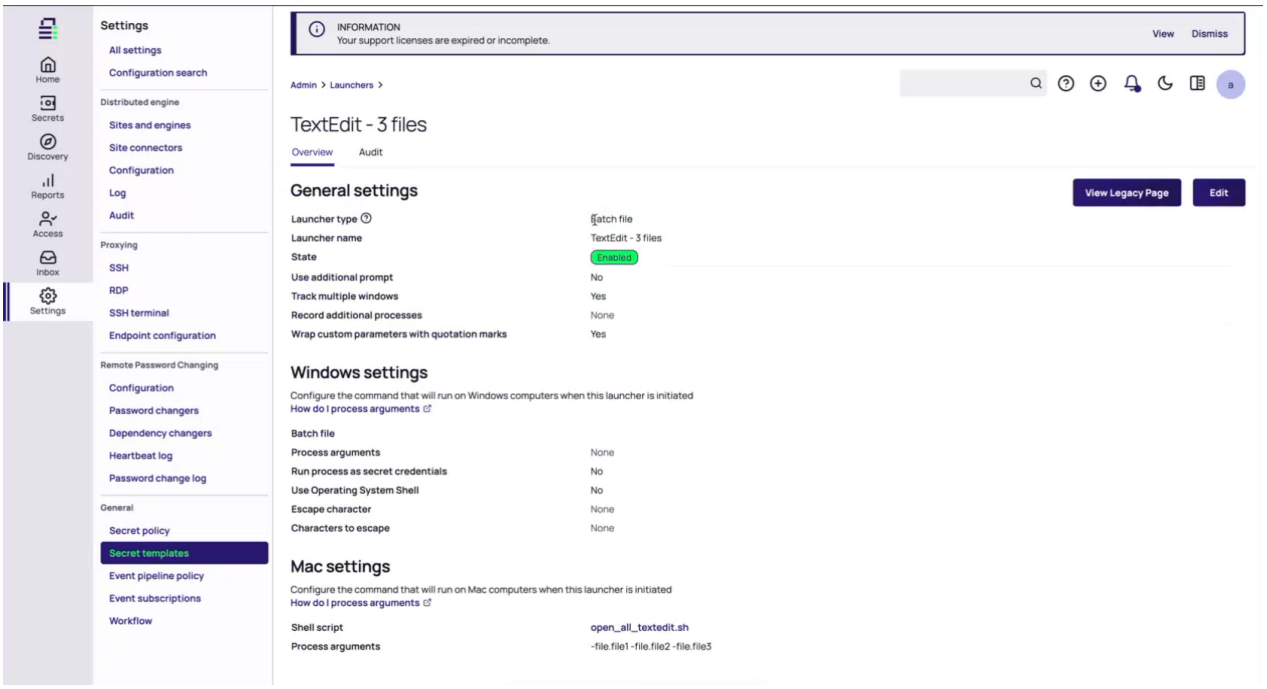
   Windows Settings

- **Batch file**: None
- **Process arguments**: None
- **Run process as secret credentials**: No
- **Use Operating System Shell**: No
- **Escape character**: None
- **Characters to escape**: None

Mac Settings

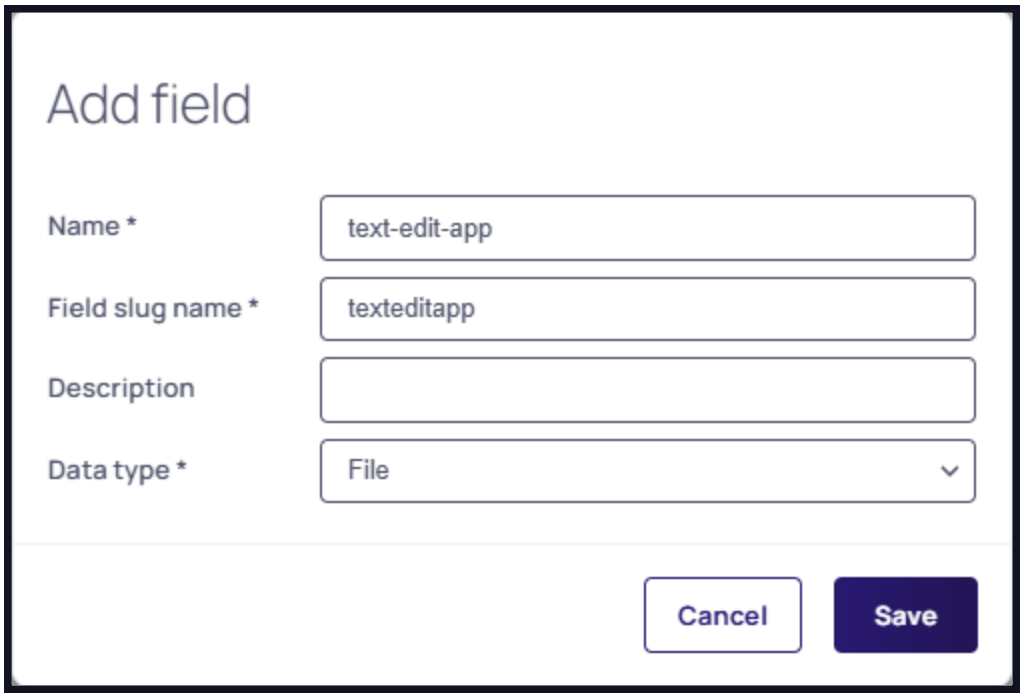
- **Shell script**: [Custom script from Step 1]
- **Process arguments**: [Your file names]

> **Important:** Paths to arguments must be in the following format: `-file.[slug from secret template]`
> Multiple files can be inserted as shown in the screenshot below:



Step 3: Creating a Custom Template

1. Create a new template inside Secret Server.
2. Select the **Fields** tab and add a new field for each file you would like to launch. Make sure that the *Data type* is set to **File**.



3. Select the **Mapping** tab and click **Add mapping**.
4. Select the launcher you created in Step 1.
5. Map the fields from the templates to the launcher.
6. Launch the secret.

Launching Websites and Auto-Filling Credentials with the Web Password Template

Prerequisites

- Prior to launching websites and auto-filling credentials with the Web Password Template from Connection Manager, make sure that you have the Delinea browser extension installed on the desired browser and you are signed in.

  Note: If you do not have the Delinea browser extension currently installed, refer to the following documentation from Secret Server for more information.

- Check the Launchers tab in the Global Settings to make the launcher status is **connected**. See "Global Configuration Settings" on page 113 for more information.

  Important: Only the Web Password template is supported.

Important: The URL List field type is not supported.

Note: Upon restarting Windows, the Microsoft Edge process initiates automatically, potentially intercepting the connection with the Delinea browser extension. Therefore, even if the Edge browser is not actively running, a connection may established, and the settings will indicate that Delinea's Edge browser extension is selected.
If you would like to work inside a different browser, you will need stop the Edge process inside Task Manager.

Supported Browsers

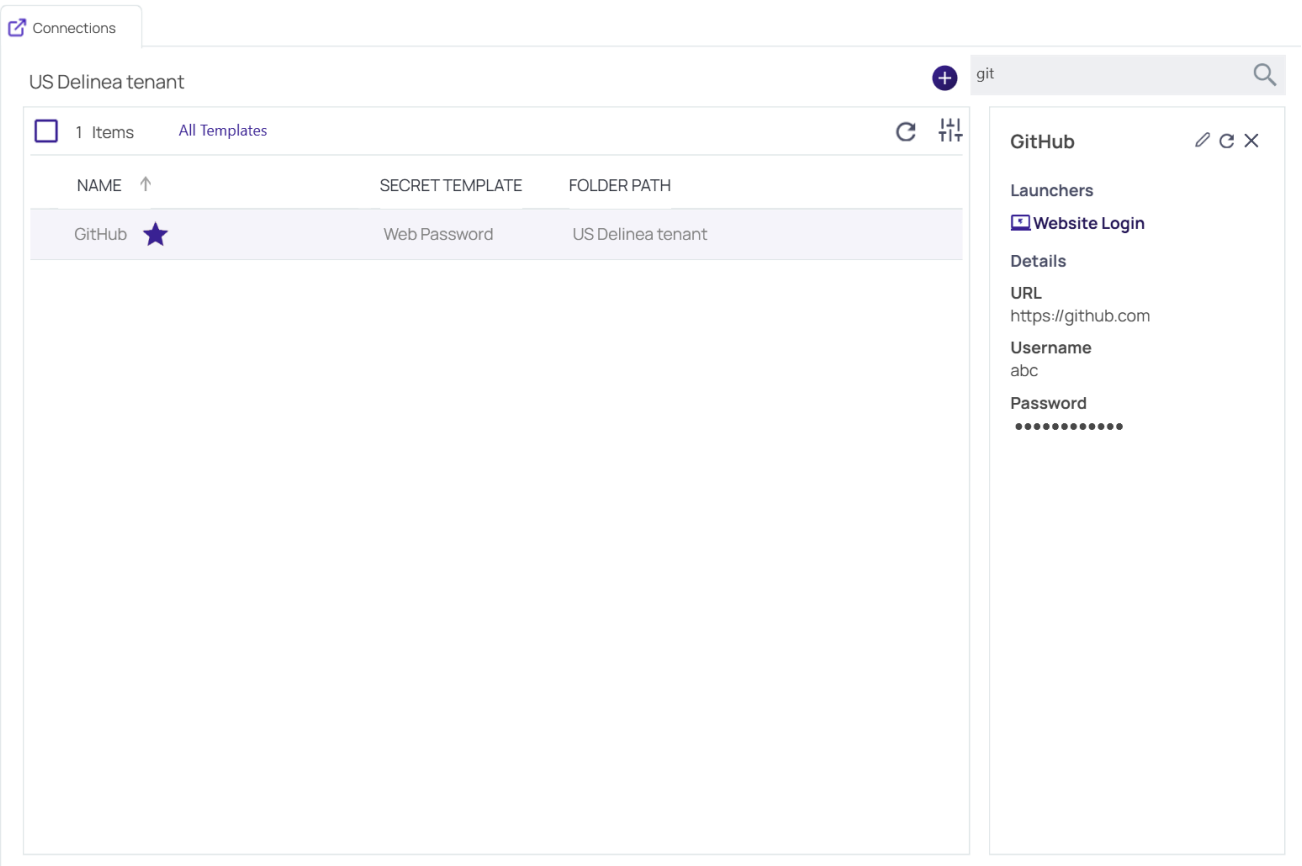
The following browsers are supported on both Windows and MacOS:

- Microsoft Edge
- Firefox
- Chrome

Launching Secrets

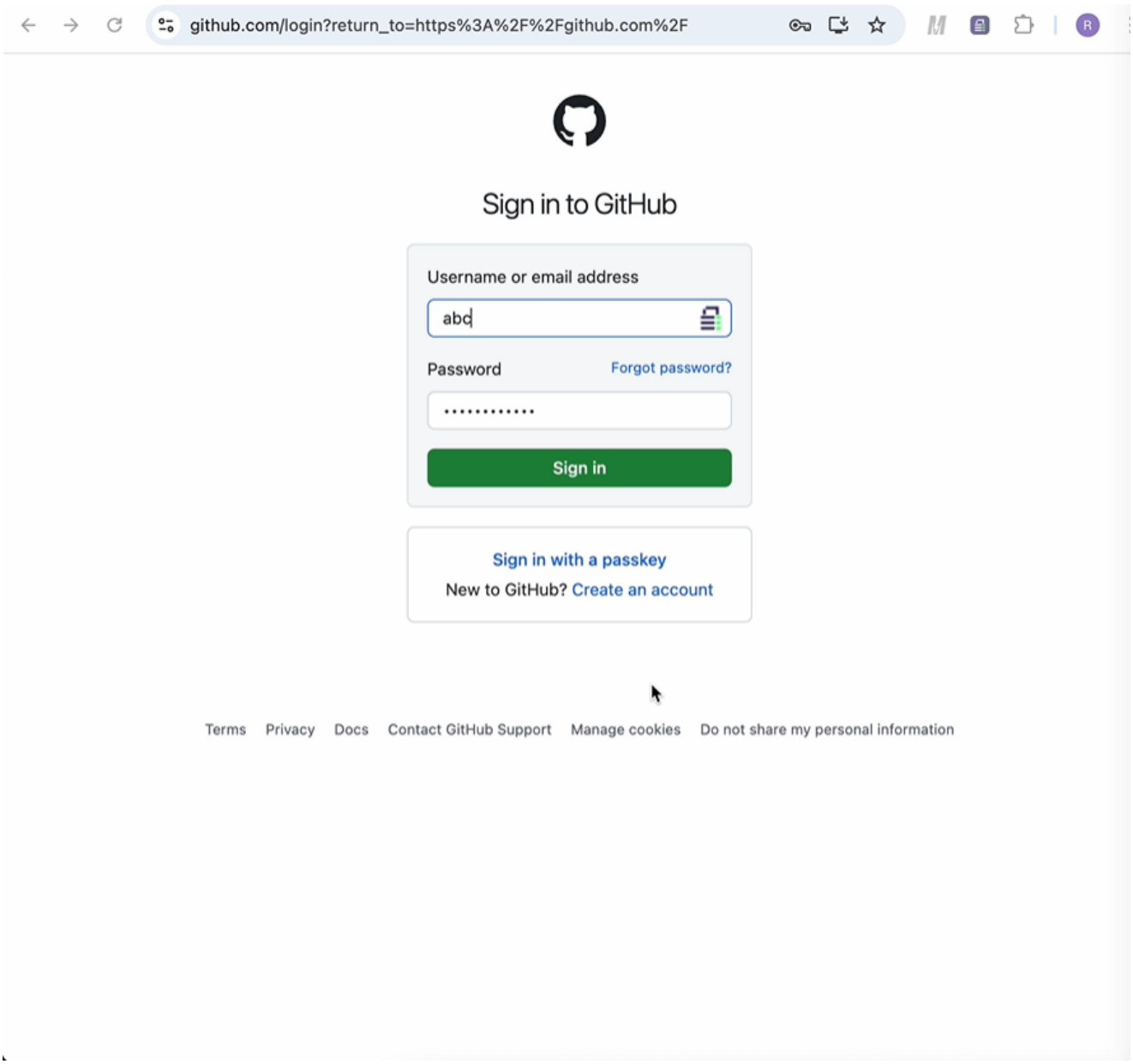
To launch websites and auto-fill credentials with the Web Password Template, click the **Website Login** under `Launchers`. Currently, users can only launch one website at a time directly from an external vault. Bulk launch and local vault is not supported.

Launchers



Note: Connection Manager selects the first browser opened after launching Connection Manager to launch the website login. If you would like to use a different browser you will need to close the current browser and open a new one.

A browser window will open and the required login fields will be filled in:



If you are experiencing issues with the website launcher, see "Troubleshooting Website Launcher Issues" on page 204.

For more information about launching secrets with Delinea browser extensions refer to the Delinea Credential Manager and Web Password Filler documentation.

Setting the Default Launcher via Registry

The `sslauncher:` URL protocol can be handled by either Delinea Connection Manager or the Secret Server Protocol Handler. You can control which one is used by default by editing the `command` subkey for the `sslauncher` protocol in the Windows registry.

Note: If the Secret Server Protocol Handler is not installed, only Connection Manager will be available to handle the protocol.

Registry Key Scope

The key can be set per-user or for all users. If both are set, the per-user (`HKCU`) value takes precedence over the all-users (`HKLM`) value.

Scope	Registry key
Current user	`HKEY_CURRENT_USER\Software\Classes\sslauncher\shell\open\command`
All users	`HKEY_LOCAL_MACHINE\SOFTWARE\Classes\sslauncher\shell\open\command`

Selecting the Launcher

Set the `(Default)` value of the `command` subkey to the path of the launcher executable, followed by `"%1"`.

Use Delinea Connection Manager

Set the `(Default)` value to the path to `Delinea.ConnectionManager.Win.ProtocolHandler.exe`. For example:

```
"C:\Program Files\Delinea\Delinea Connection
Manager\Delinea.ConnectionManager.Win.ProtocolHandler.exe" "%1"
```

Use the Secret Server Protocol Handler

Set the `(Default)` value to the path to `RDPWin.Bootstrapper.exe`. For example:

```
"C:\Program Files\Thycotic Software Ltd\Secret Server Protocol
Handler\RDPWin.Bootstrapper.exe" "%1"
```

Notes

- Only the `command` subkey value needs to change to switch launchers.
- The parent `sslauncher` key's `(Default)` value (`URL:Secret Server Launcher Protocol`) and its empty `URL Protocol` value are standard boilerplate that register the URL-protocol scheme. These are the same regardless of which launcher is active and do not need to be modified.
- Installation paths may vary depending on the environment (for example, custom install directories or `Program Files (x86)` on some systems). Confirm the actual executable location on the target machine before applying.

Common User Activities

Since there are many variations and configuration options for remote connectivity, it is not possible to cover all of them in detail. However, Connection Manager does support many variations.

- Folder Editing
- "Creating Connections" on page 83
- Integrated Connections
- "Re-authenticating to a Vault" on page 76
- Log File Location

Connections

The following Connections related topics are available:

- "Re-authenticating to a Vault" on page 76
- Remote connections
- Integrated connections

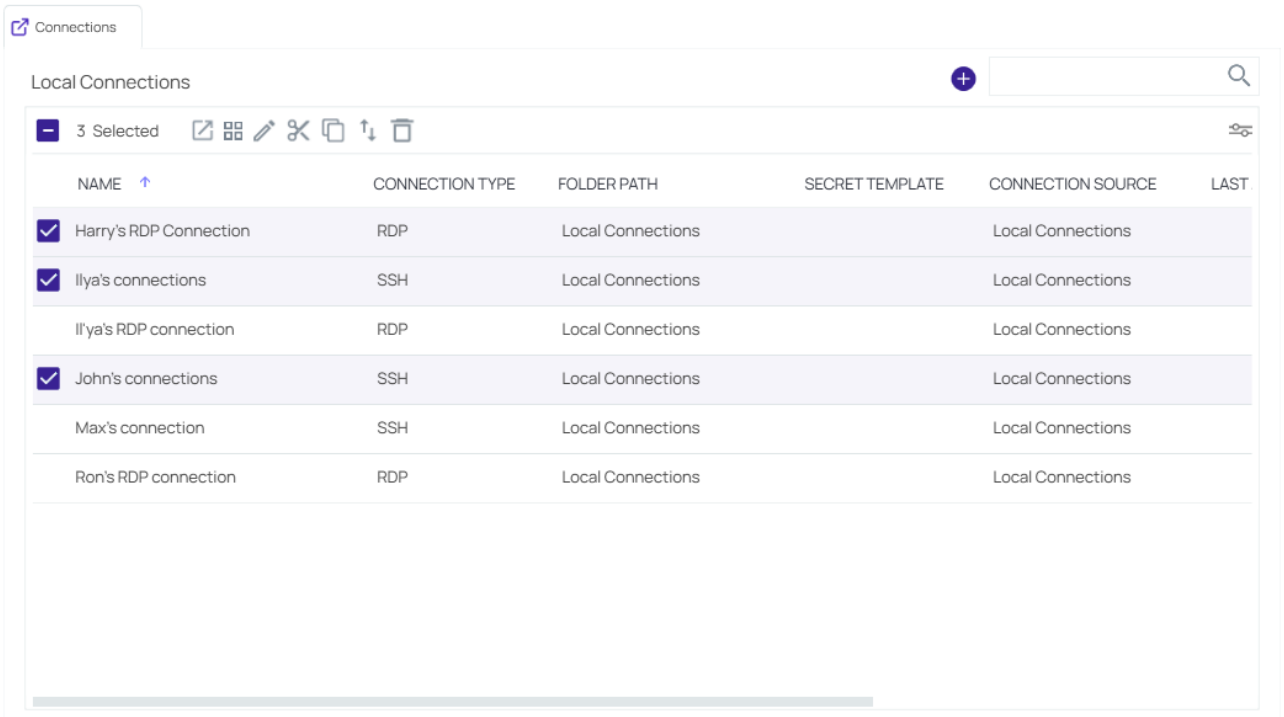
Batch Opening Connections

In Connection Manager there are several ways to simultaneously open multiple connections, including combinations of Secret Server and Local connections.

Batch Opening Connections Using Multi-select

You can batch open multiple Local and Secret Server Connections, even when they are in different folders

1. Click to check the box before each connection you wish to open.

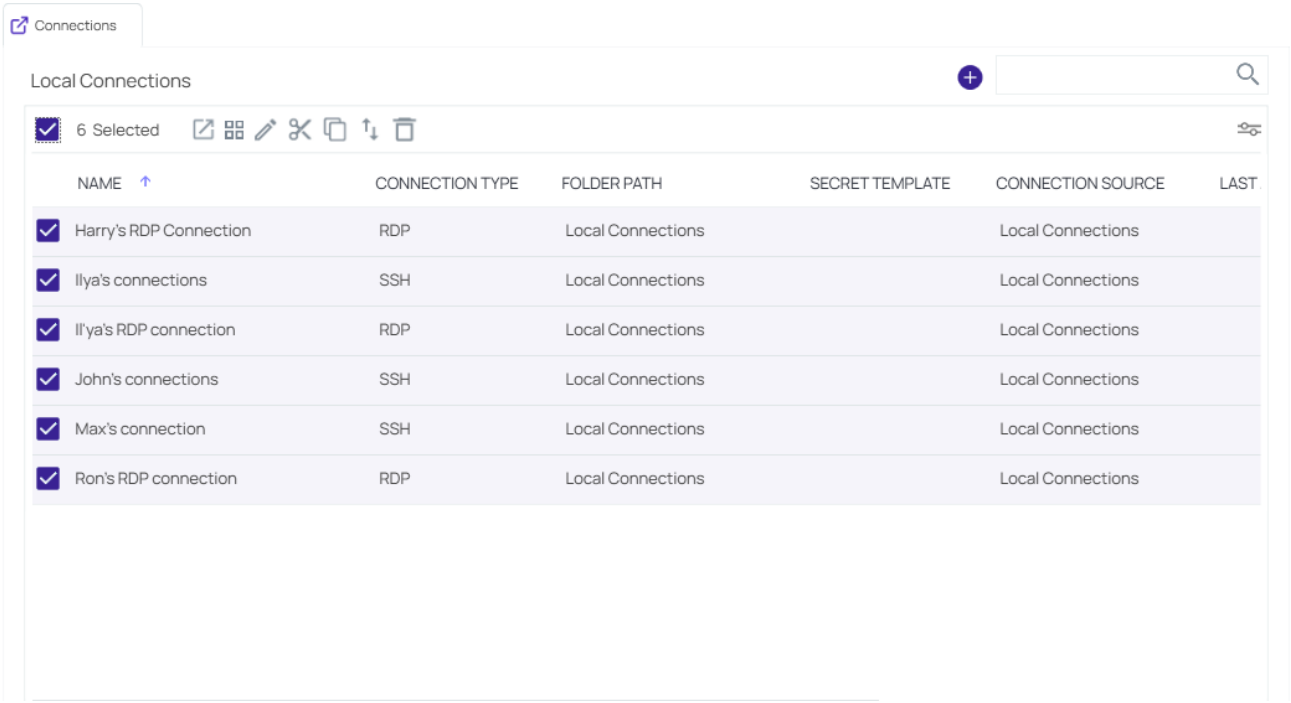


2. In the toolbar click the **Connect** icon.

Batch Opening All Connections in a Folder

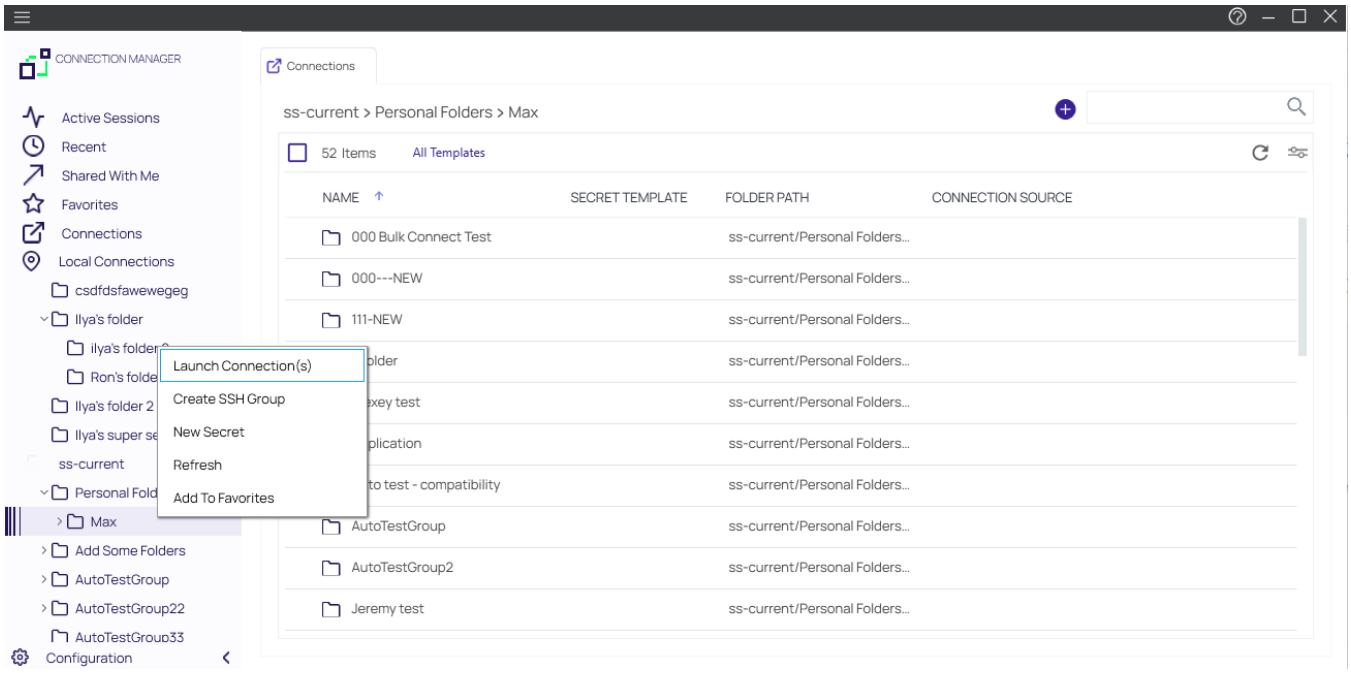
You can batch open all connections in a folder, at the folder level.

1. Click to check the box before the folder whose connections you wish to batch open.



2. In the toolbar click the **Connect** icon.

You can also open all connections in a folder by right-clicking the folder in the left-hand navigation and selecting **Launch Connection** from the context menu.



Batch Editing Local Connections

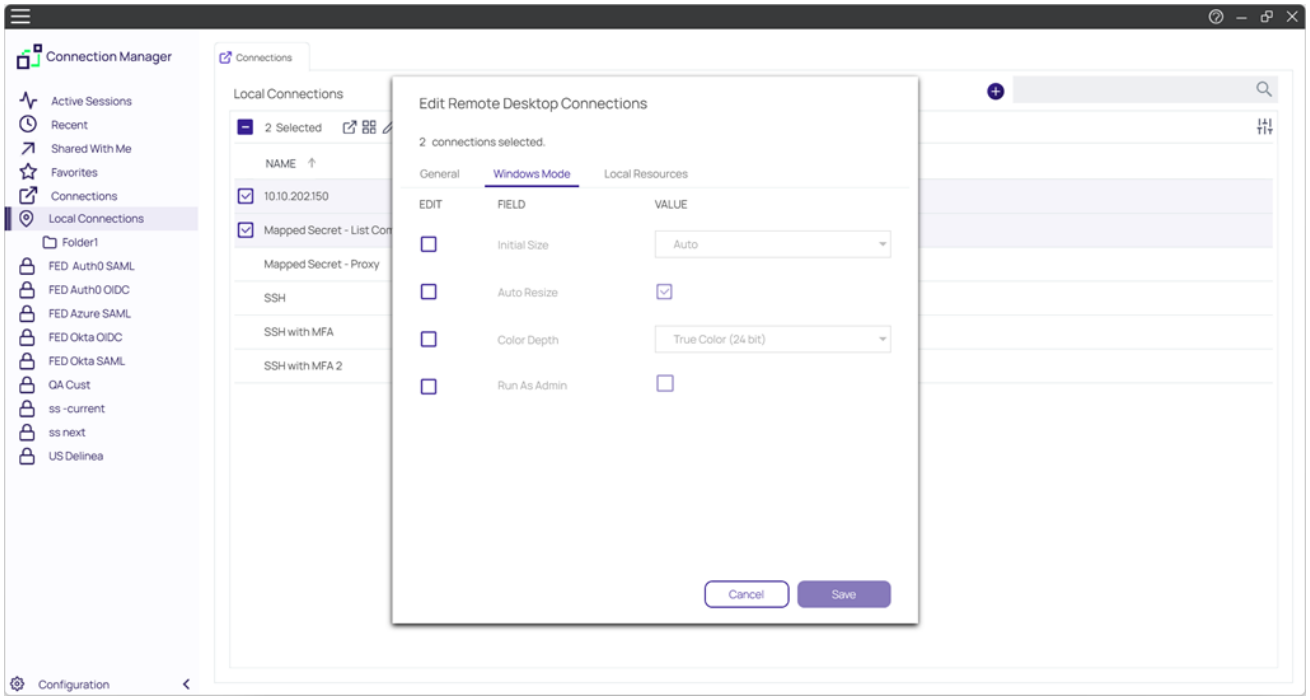
In Connection Manager there are several ways to batch edit multiple RDP connections or multiple SSH connections. You cannot edit RDP and SSH connections together.

Batch Editing Local Connections Using Multi-Select

You can batch edit parameters for multiple local connections (all RDP or all SSH) using multi-select.

1. Click to check the boxes for all connections you wish to batch edit

.

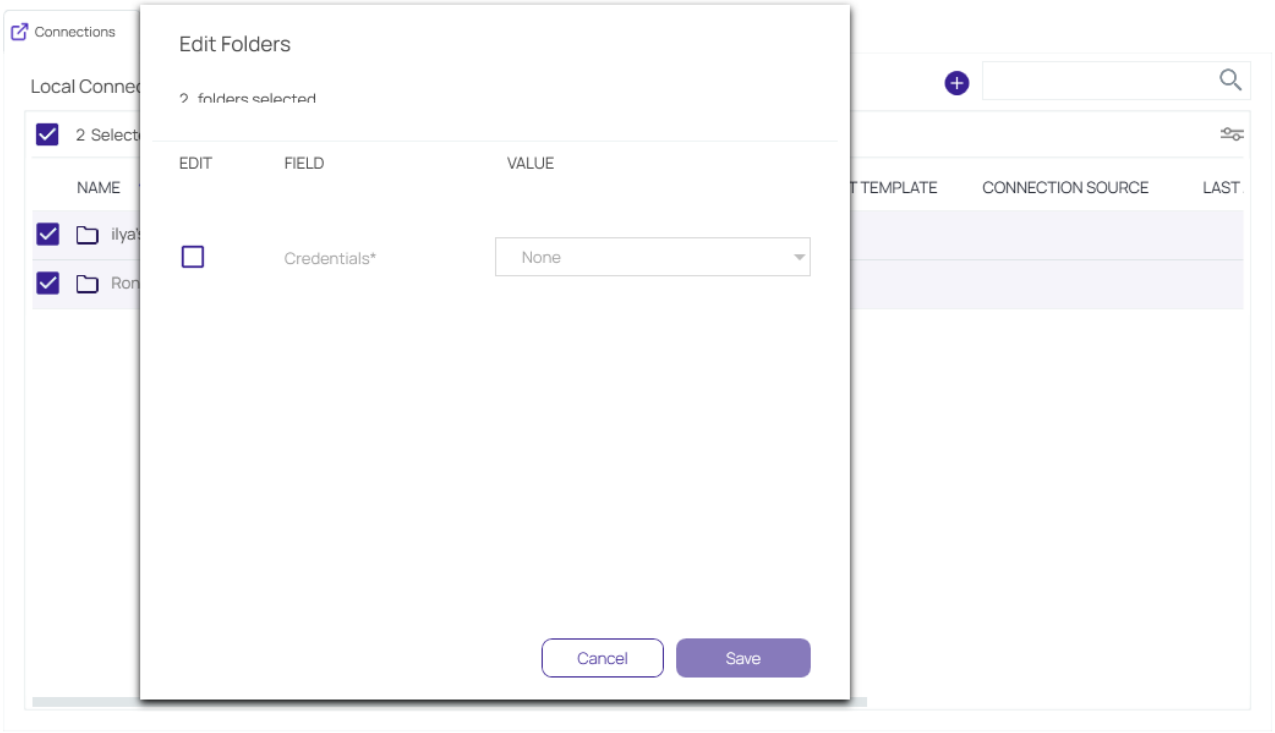


2. In the toolbar click the **Edit** icon.
3. Edit the settings you wish to apply to all of your selected connections and click **Save**.

Batch Editing Credentials for All Connections in One or More Folders

You can batch edit Credentials for all connections in one or more folders, at the folder level.

1. Click to check the boxes for the folder or folders whose connections you wish to batch edit.



2. In the toolbar click the **Edit** icon.
3. Edit the Credentials you wish to apply to all connections in your selected folder or folders and click **Save**.

Application Configuration via Windows Registry Editor

Application settings were moved to the Registry in the 2.8 release. If you are using an older version of Connection Manager, refer to the "Application Configuration File" on page 176.

Note: For your application settings to be automatically migrated from the configuration file to the Registry, you need to run Connection Manager as an administrator.

If Connection Manager is installed for all users of a machine, the registry settings can be adjusted in the following path:

`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Delinea Inc.\Delinea Connection Manager\AdminConfig`

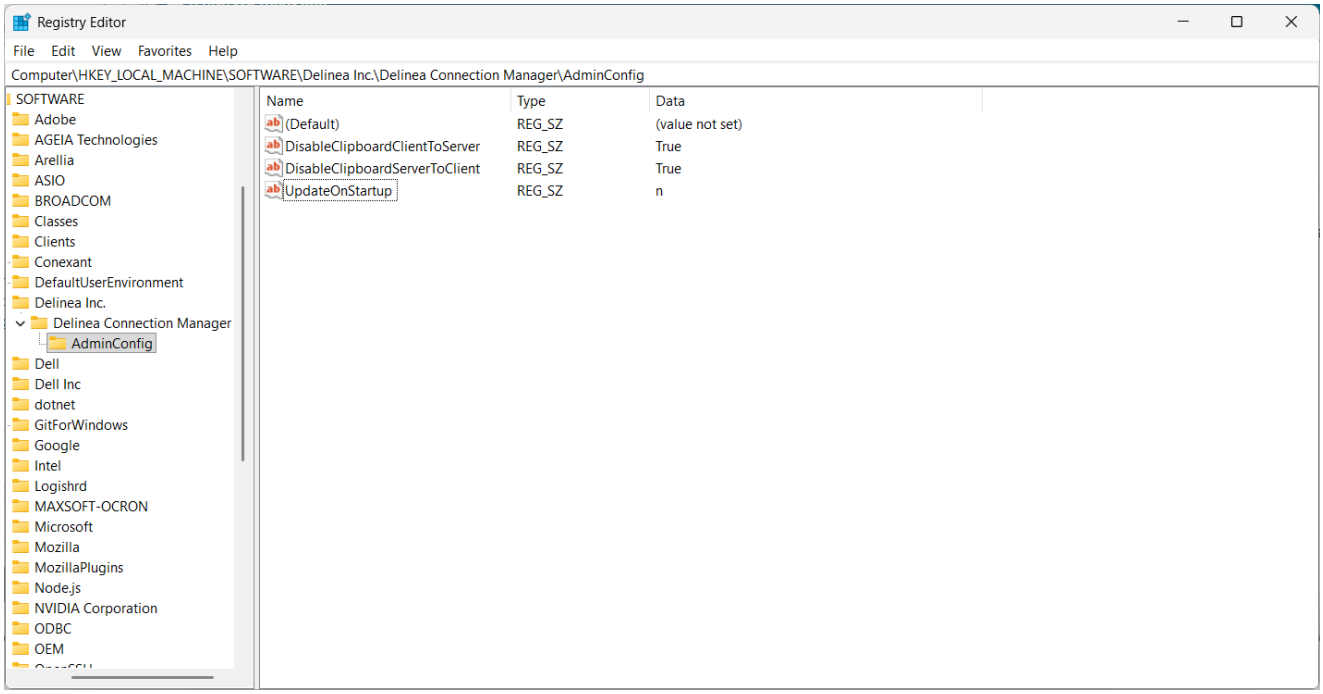
If you installed Connection Manager just for yourself in a per-user folder, the registry settings can be adjusted in the following path:

`Computer\HKEY_CURRENT_USER\Software\Delinea Inc.\Delinea Connection Manager\UserConfig`

Important: If you are upgrading to 2.8 from a previous version, your application configuration settings will be carried over from the application configuration file to the Registry editor if you run Connection Manager as an administrator. For new Connection Manager installations, the values will be set at their default value.

Disabling Update Check on Startup

To disable automatic checking for updates on startup, for Windows open the Registry editor and change the value to *n* as shown below:

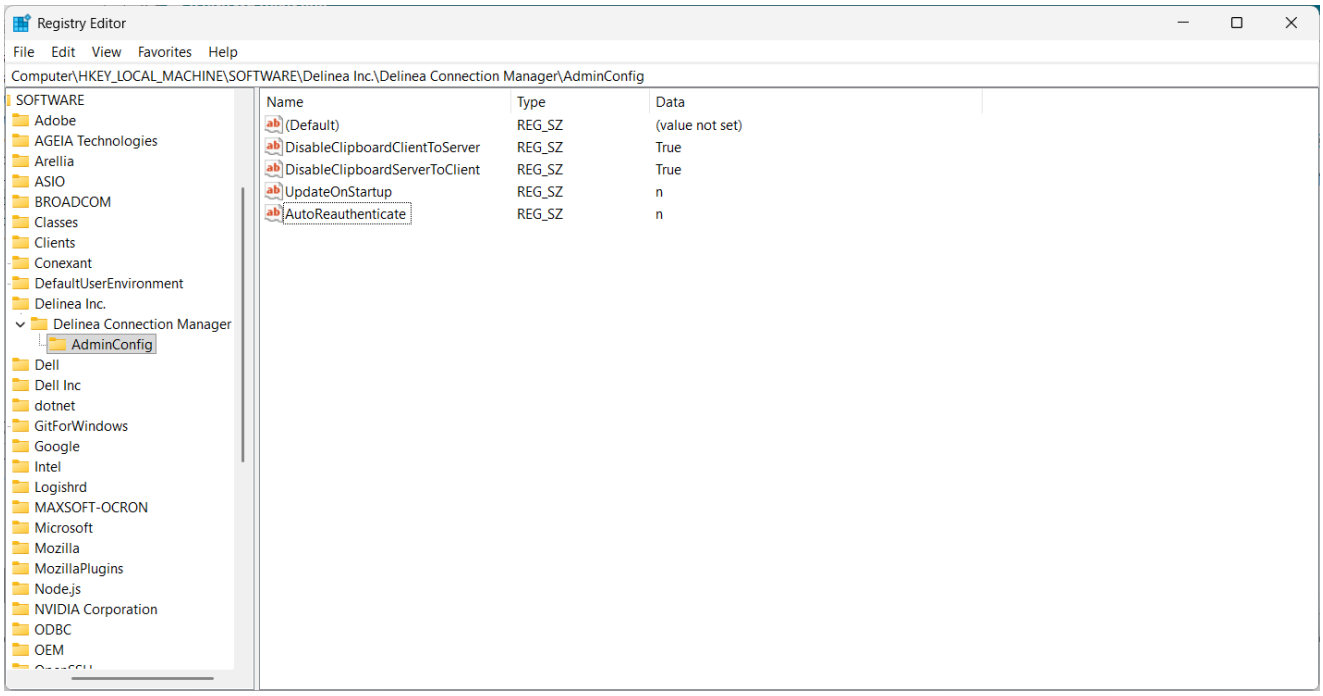


Enabling/Disabling Auto Reauthenticate

This feature provides the option to configure vault reauthentication behavior in Connection Manager. Users may keep the existing behavior that automatically restarts the authentication flow or force a fresh login when their vault session/refresh tokens have expired--mimicking the existing web API behavior.

The default value is **y** which automatically restarts the authentication flow. If the value is set to **n**, the behavior will be more similar to the web API which forces a fresh login. The **n** option is beneficial for users who use SAML configuration through an external identity provider with a longer session/refresh length and enables audit logs to correctly generate upon logout.

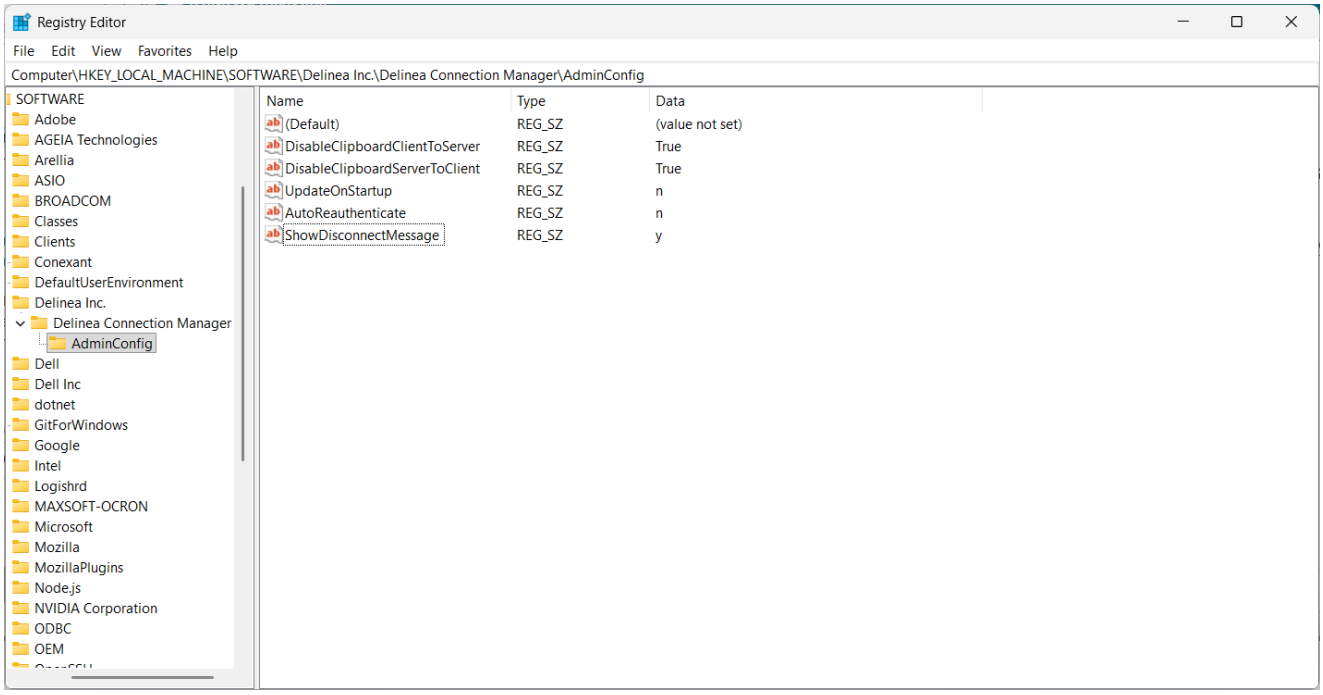
Adjust the *AutoReauthenticate* parameter with the needed value:



Enabling the Session Status Popup

The Session Status popup window is disabled by default. This window would appear every time a user signed out of a session, confirming that they also signed out of the server. However, if you are experiencing memory leak issues, Delinea recommends enabling this window by updating the `ShowDisconnectMessage` value to `y`.

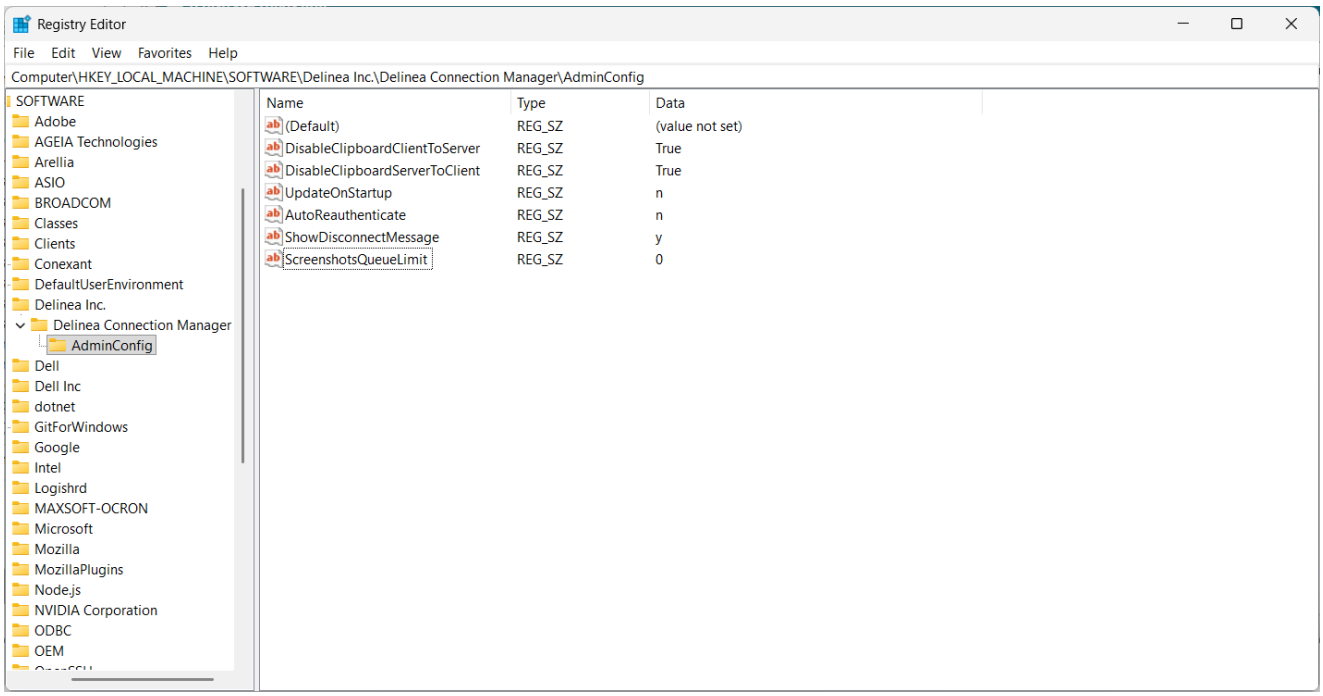
Adjust the `ShowDisconnectMessage` parameter with the needed value:



Setting the Screenshot Queue Limit

If you have session recording enabled and are experiencing unstable internet connectivity, Connection Manager may no longer be able to send screenshots to the server and your session will be terminated. If you continue to experience internet connectivity issues, you can try increasing the screenshot queue limit to allow screenshots to be temporarily saved locally until connectivity is restored. The screenshot queue limit can be increased by changing 0 to any positive value.

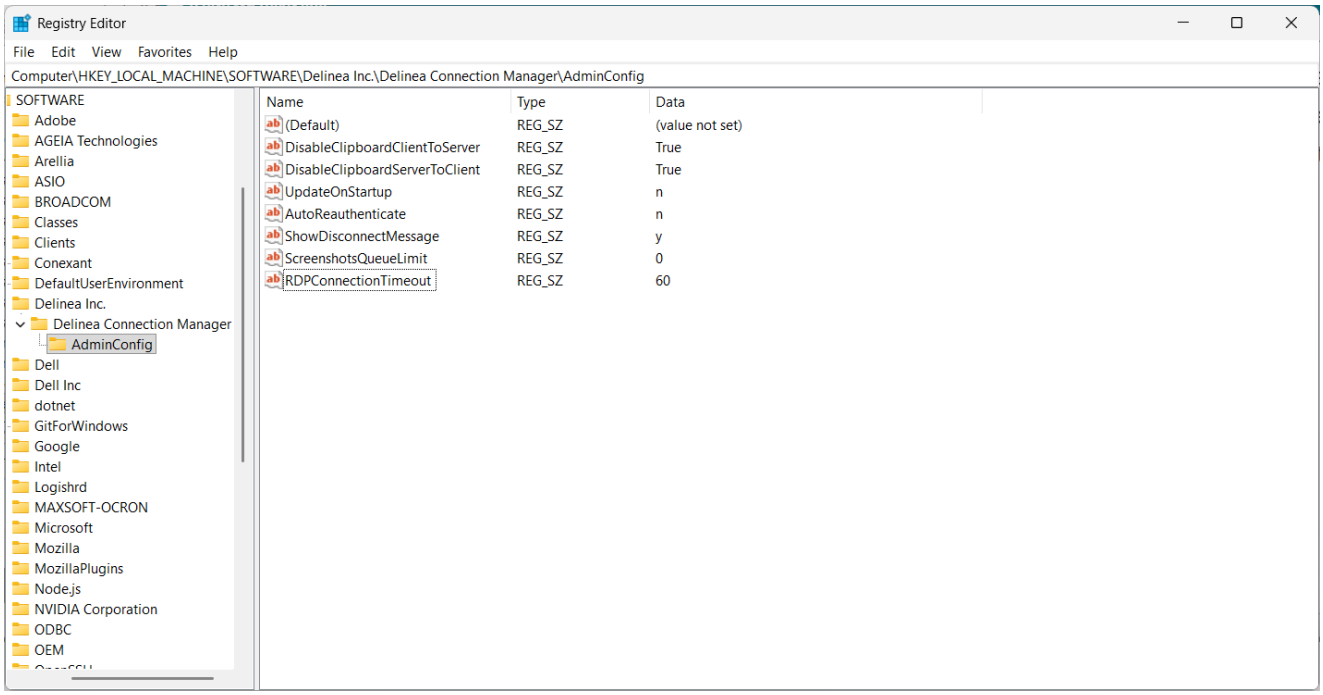
Adjust the `ScreenshotsQueueLimit` parameter with the needed value:



Configuring RDP Connection Timeout Over TCP

This configuration allows the ability to customize RDP connection timeouts in seconds. This is helpful for situations involving proxy, MFA, or other configurations that require additional time to connect before timeout due to inactivity. The timeout can be adjusted as needed, but the recommended suggestion is to start with 60 seconds as shown below.

Adjust the `RDPConnectionTimeout` parameter with the needed value:

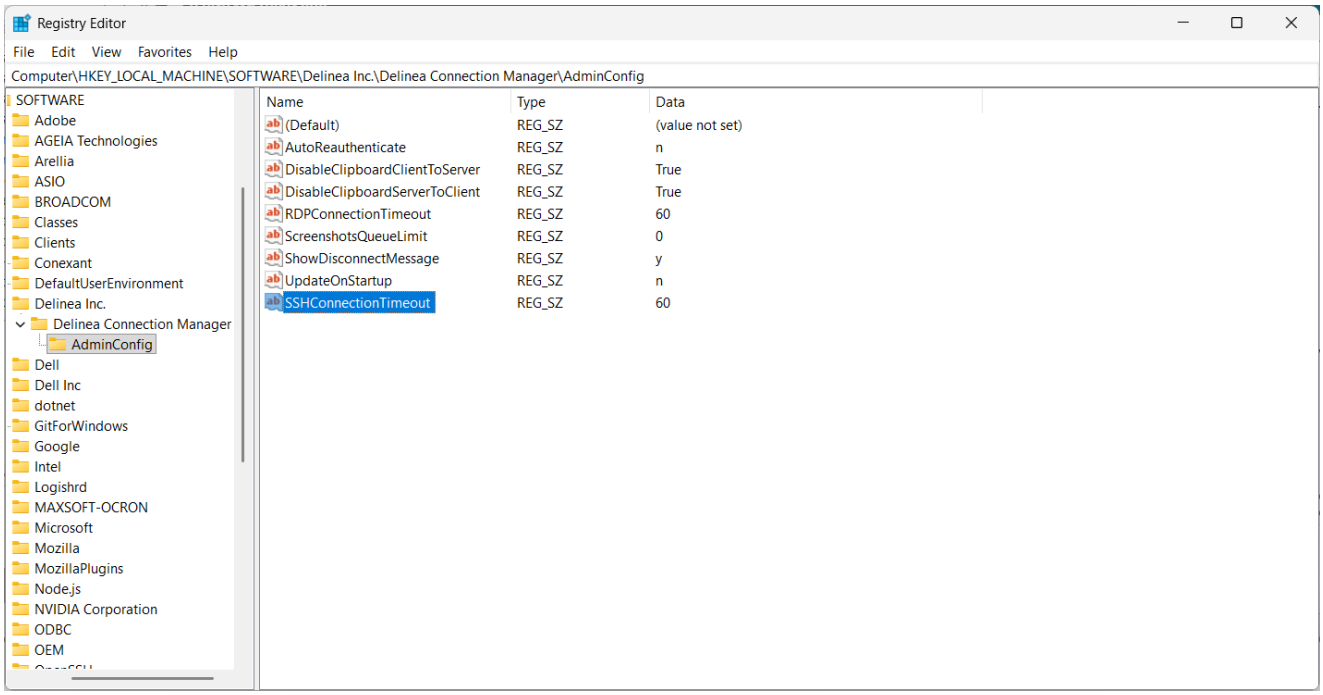


> In versions 2.5.x of Connection Manager, this value was measured in milliseconds. If users already had a value set in milliseconds, Connection Manager will preserve that value after upgrade. Otherwise, the default value will be set, which is 60 seconds.

Configuring SSH Connection Timeout Over TCP

This setting allows administrators to configure the amount of time (in seconds) during which a user can be inactive (i.e., not interacting with the system in any way) without any impact on their SSH session. After the timeout expires, the user will be disconnected from the session and session itself will be closed. The default value is set at 60 seconds, but can be adjusted as needed by changing the value shown in the example below.

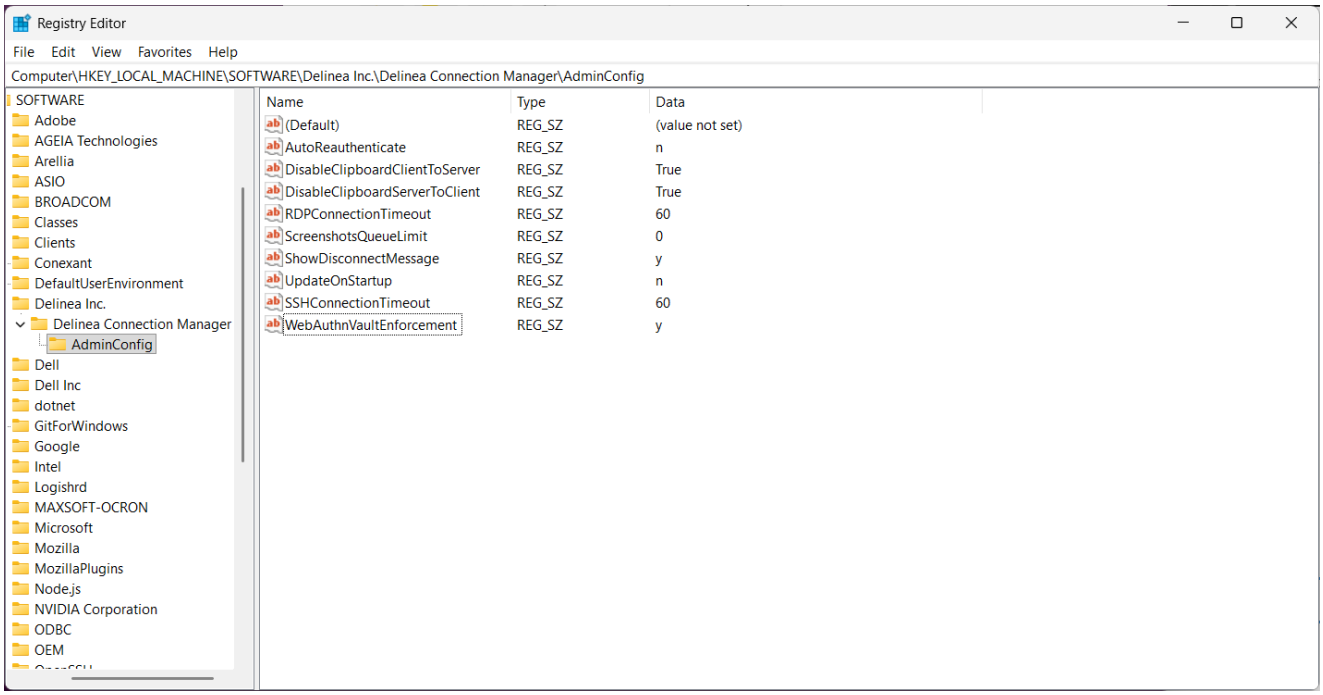
Adjust the `SSHConnectionTimeout` parameter with the needed value:



Important: In versions 2.5.x of Connection Manager, this value was measured in milliseconds. If users already had a value set in milliseconds, Connection Manager will preserve that value after upgrade. Otherwise, the default value will be set, which is 60 seconds.

Enabling WebAuthn Authentication for All Users on Windows

If you would like to enable WebAuthn authentication for all users, you will need to create a new string value called `WebAuthnVaultEnforcement` and set the value to `y` as shown below:

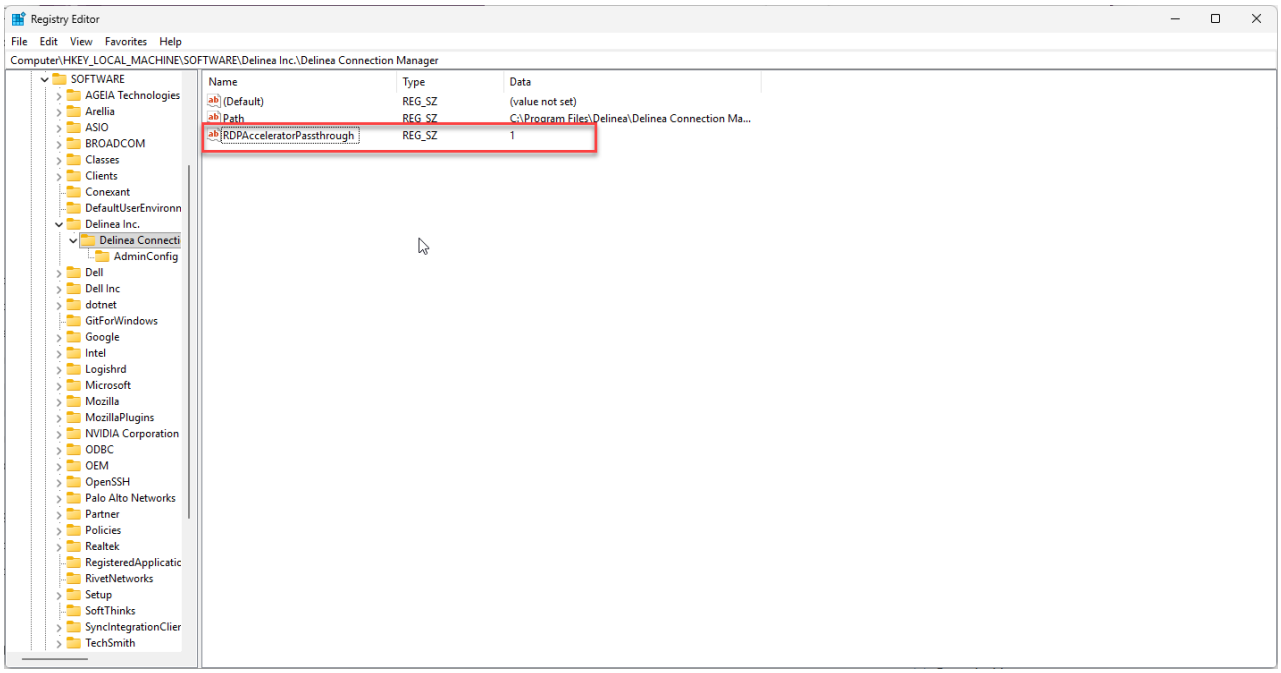


Note: WebAuthn authentication admin enforcement only enforces vault connections.

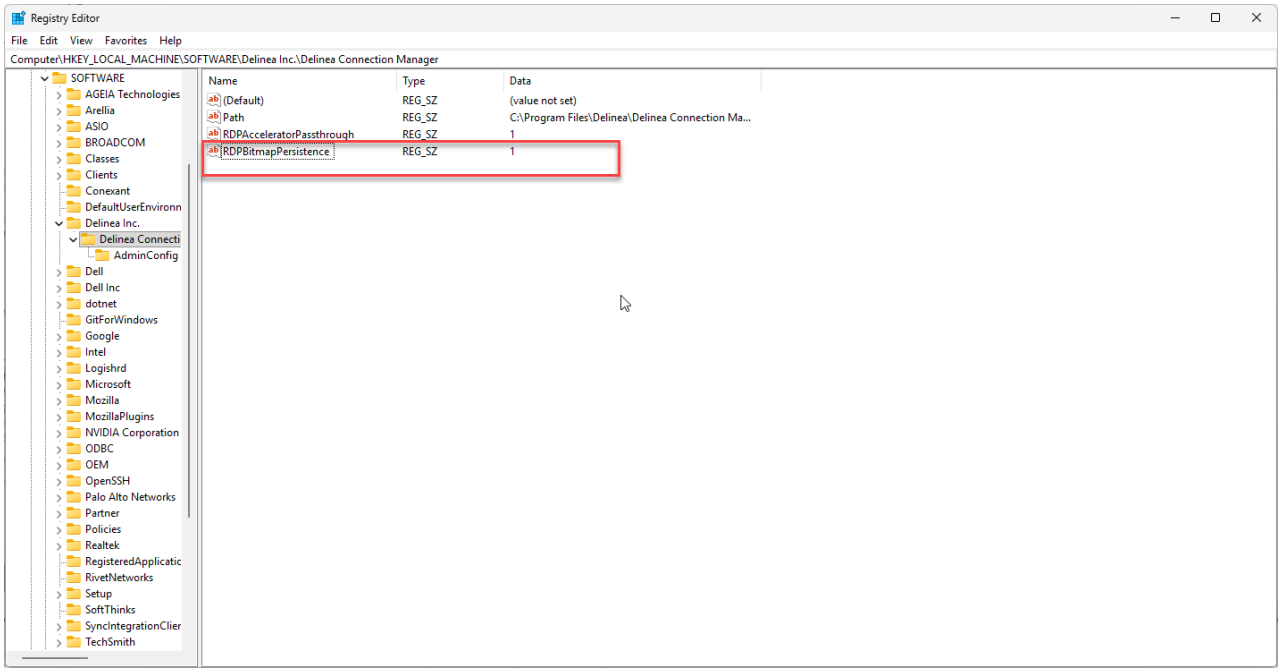
RDP Rendering Settings

If you are experiencing memory leak issues, add the following settings in the Registry Editor:

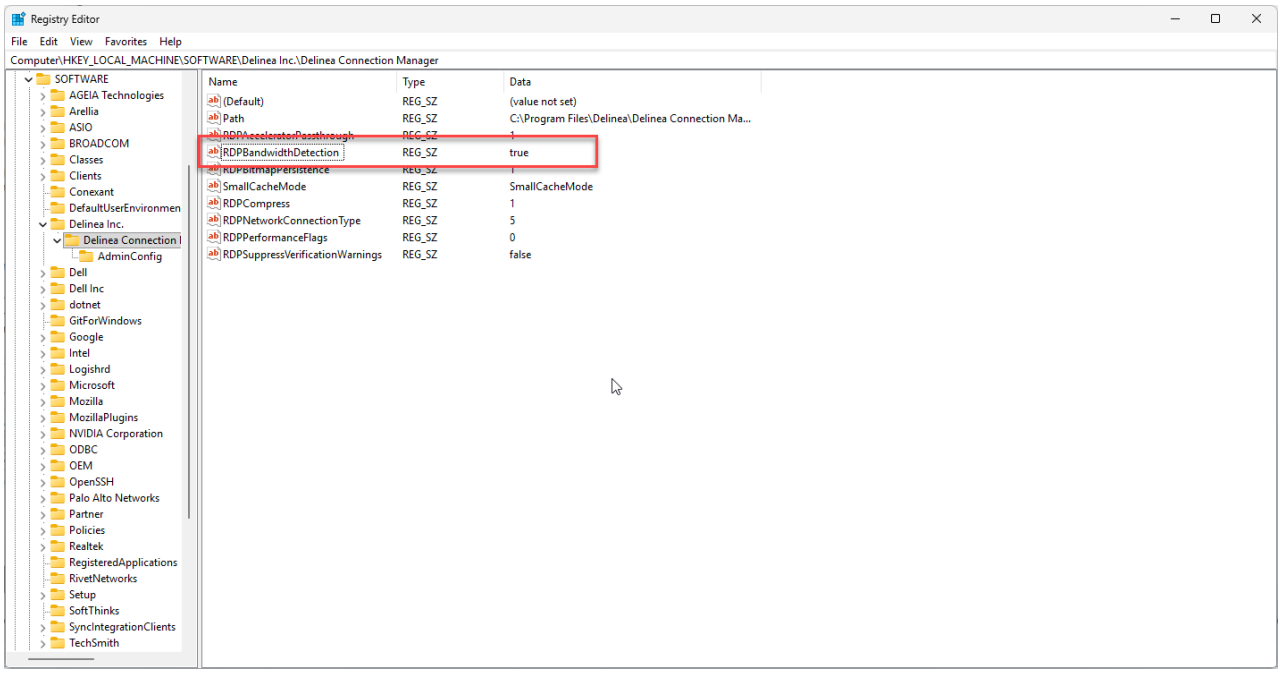
- `RDPAcceleratorPassthrough`: Specifies if keyboard accelerators should be passed to the server. Set this parameter to 0 to disable the feature or a nonzero value to enable the feature. The default is a nonzero value:



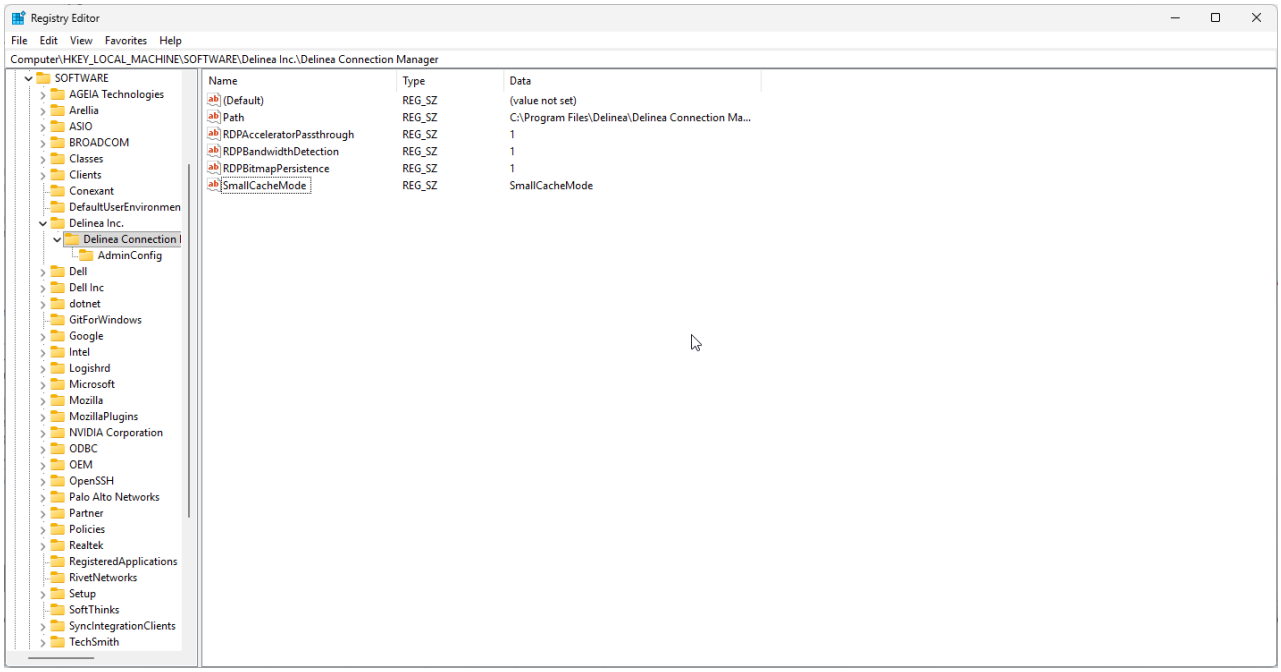
- `RDPBitmapPersistence`: Specifies if persistent bitmap caching should be used. Persistent caching can improve performance but requires additional disk space. Set this parameter to 0 to disable caching or a nonzero value to enable caching:



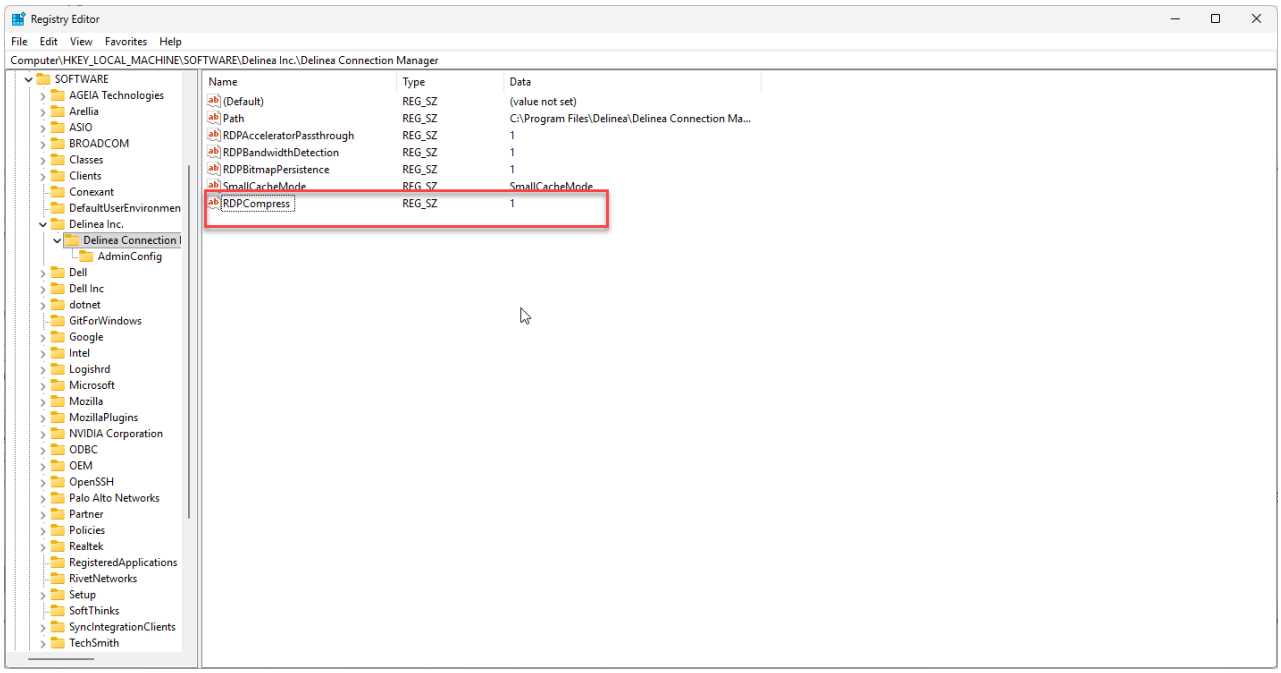
- `RDPBandwidthDetection`: Specifies if bandwidth changes are automatically detected. Set the value to `true` if bandwidth changes are automatically detected or `false` otherwise.



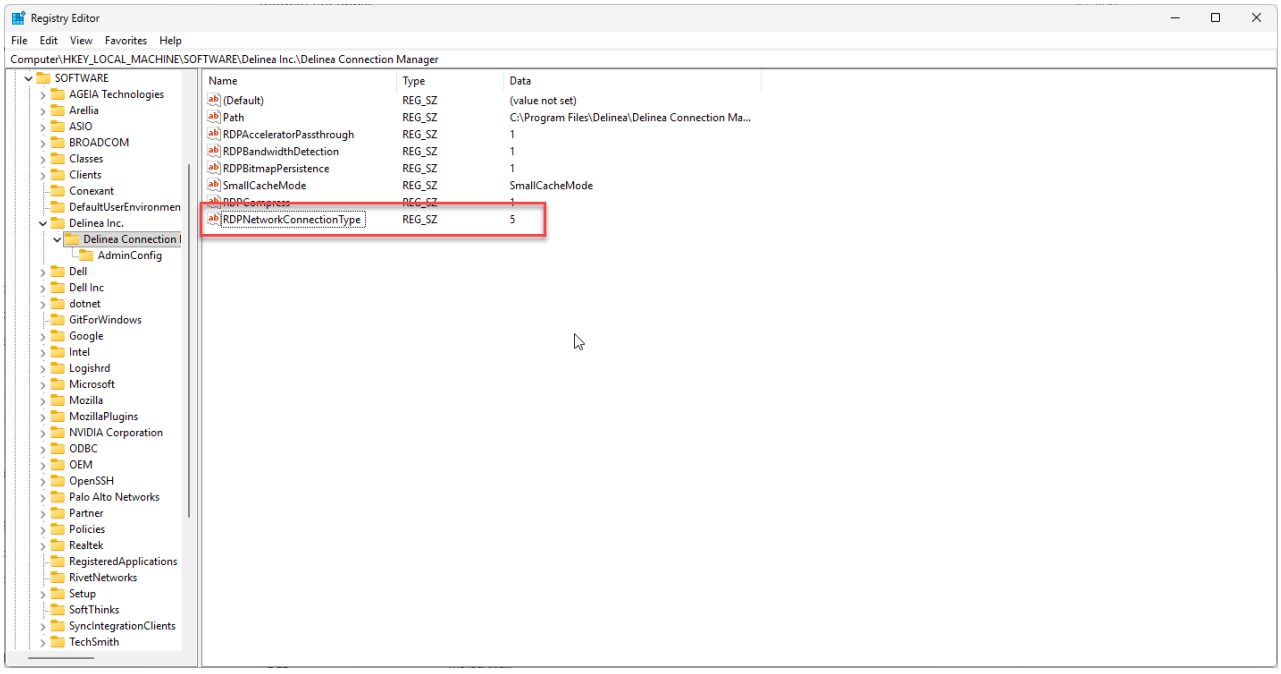
- `RDPClientProtocolSpec`: Specifies the remote desktop protocol used between the client and the server. This property is read/write: `FullMode`, `ThinClientMode`, `SmallCacheMode`:



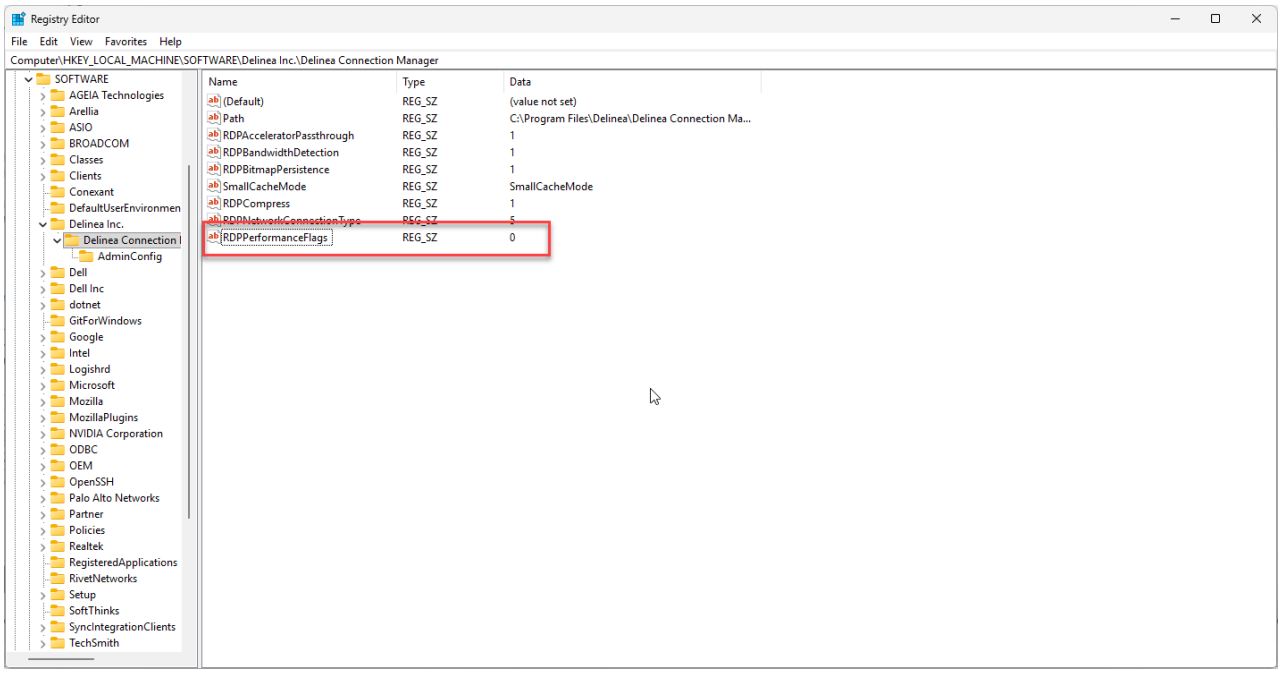
- `RDPCompress`: RDP compression settings balance memory vs. bandwidth, configured via Group Policy (gpedit.msc). Set the value to 1 to turn on RDP compression:



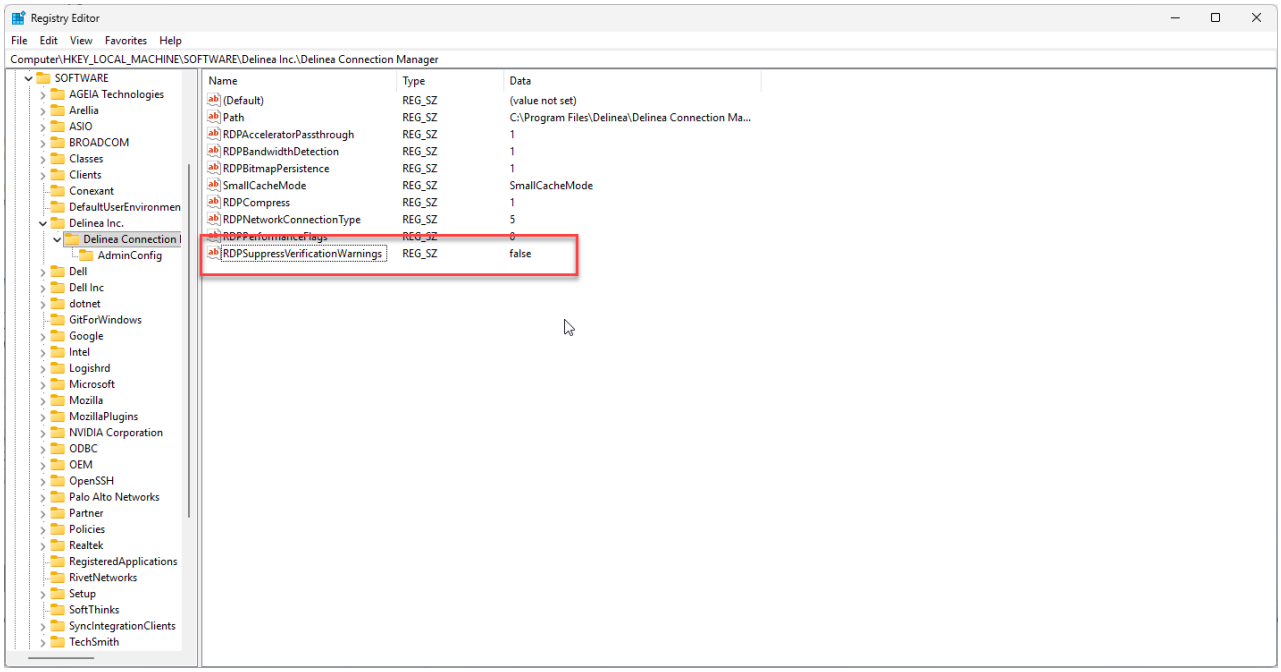
- `RDPNetworkConnectionType`: Gets or sets the type of network connection used between the client and server. The network connection type information passed on to the server helps the server tune several parameters based on the network connection type. The value of the setting will depend on the network connection type. See additional documentation from Microsoft for more information.



- `RDPPerformanceFlags`: Specifies a set of features that can be set at the server to improve performance. The default value is 0, meaning no features are disabled:



- `RDPSuppressVerificationWarnings`: Suppresses RDP certificate verification warnings. The default value is `false`:



Disabling Local Vault via Admin Enforcement

See "Disabling Local Vault via Admin Enforcement on Windows " on page 26 for more information on this setting.

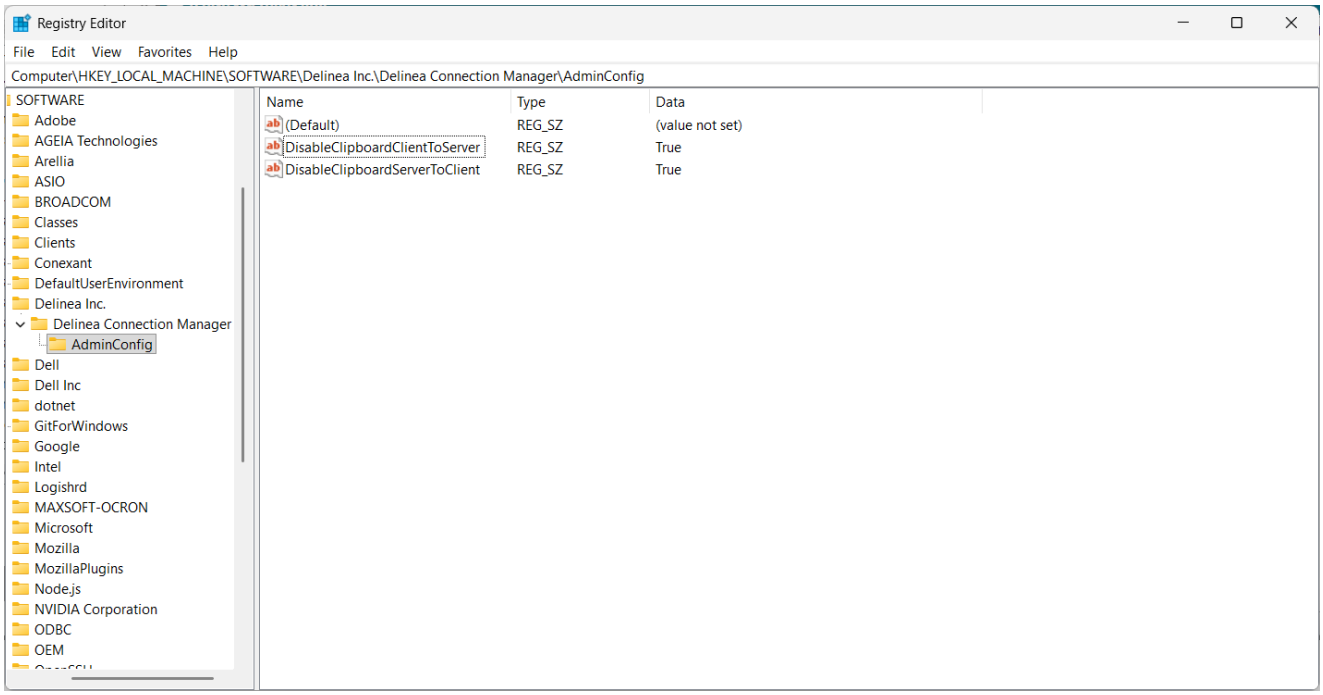
Unidirectional Clipboard Enforcement on Windows

Administrators can unidirectionally restrict clipboard access from the RDP server to the users' local machine and vice-versa in both local and vault connections. This is an administrative setting and cannot be overridden by non-admin users.

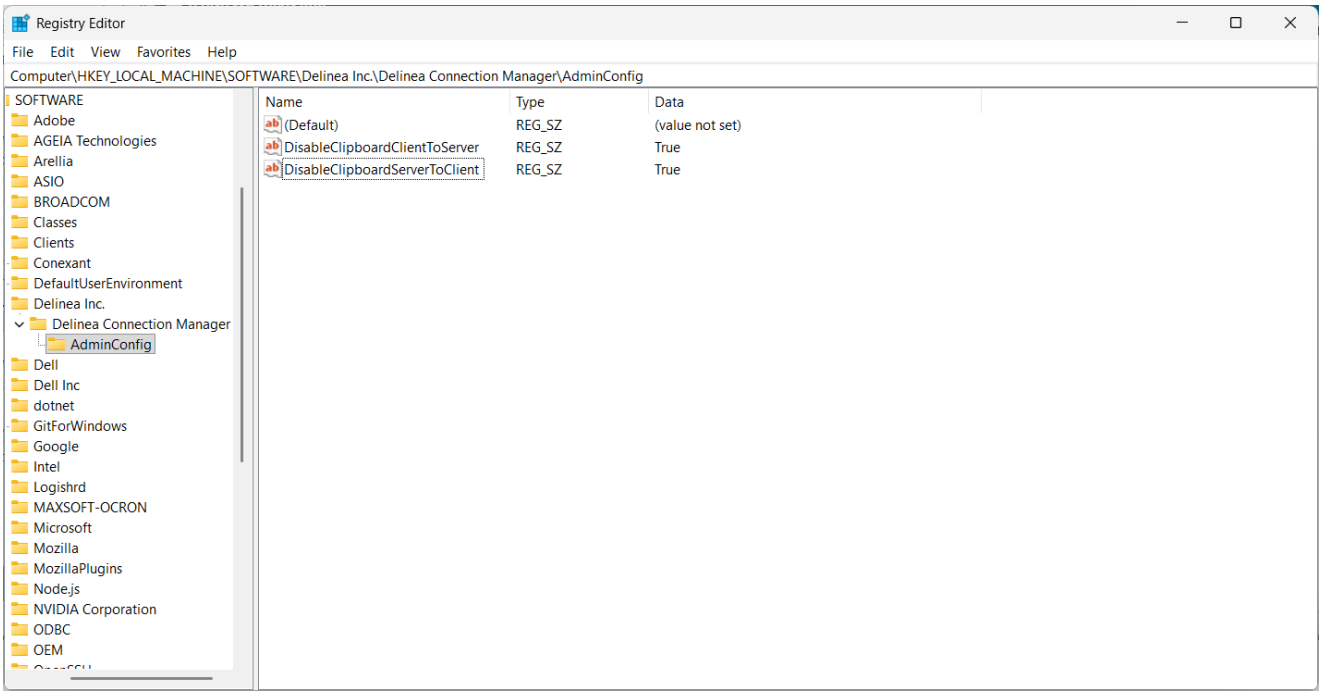
The effective clipboard redirection behavior is determined by two factors: the Secret clipboard value and the individual restrict flags for each direction (Server to Client and Client to Server):

- If the Secret clipboard value is false, all clipboard redirection is disabled regardless of restrict settings.
- If the Secret clipboard value is true, each direction is enabled unless its corresponding restrict flag is set to true.

If you would like to restrict users from copying information from the RDP server to their local machine, create a new string value called `DisableClipboardServerToClient` and set the value to `True` as shown in the example blow:



If you would like to restrict copying from the users' machine to the RDP server, create a string value called `DisableClipboardClientToServer` and set the value to `True` as shown in the example below:



For unidirectional clipboard enforcement on MacOS see "Unidirectional Clipboard Enforcement on MacOS" on page 177.

Pre-Trusting SSH Host Fingerprints

Administrators can pre-seed trusted SSH host fingerprints so that end users are not prompted to accept an unknown host key. Inside the AdminConfig registry key, create a string value (REG_SZ) named `PublicKeyFingerprintStorage` and set it to a JSON object that maps host names to their expected fingerprints.

The value must be a JSON dictionary where each key is a host name (optionally with a non-standard port appended as `host:port`) and each value is the expected fingerprint string:

```
{
    "server1.example.com": "SHA256:abc123...",
    "server2.example.com:2222": "SHA256:def456..."
}
```

Note: Admin-defined fingerprints are merged with the per-user storage at startup. Admin entries overwrite matching user entries; unrelated user entries are preserved. Restart Connection Manager after editing the registry for changes to take effect. Invalid JSON is logged and ignored. This setting is Windows-only.

Pre-Approving Secret Server URLs

Administrators can pre-approve or explicitly deny Secret Server URLs for the external launcher so that end users are not shown the URL approval dialog. Inside the AdminConfig registry key, create a string value (REG_SZ) named `ApprovedSsUrlStorage` and set it to a JSON object that maps URLs to their approval status.

The value must be a JSON dictionary where each key is a Secret Server URL and each value is `true` (approved) or `false` (explicitly denied):

```
{
    "https://ss.example.com/SecretServer": true,
    "https://untrusted.example.com": false
}
```

Note: Admin-defined URL approvals are merged with the per-user storage at startup. Admin entries overwrite matching user entries; unrelated user entries are preserved. Restart Connection Manager after editing the registry for changes to take effect. Invalid JSON is logged and ignored. This setting is Windows-only.

Deprecated Settings

The following registry settings are deprecated:

- LogFileName
- DataFileName
- SettingsFileName
- ApprovedSsUrlStorageFileName
- PublicKeyFingerprintStorageFileName
- TlsValidationBypassStorageFileName
- PreviousBrandDataFileName
- PreviousBrandAppSharedDataFolder

Application Configuration File

Note: In the 2.8 release, some of the application configuration settings were moved to the Windows Registry. See "Application Configuration via Windows Registry Editor" on page 163 for more information.

The Connection Manager configuration files can be found at the default locations indicated below.

Windows Configuration File Location

`C:\Program Files\Delinea\Connection Manager\Delinea.ConnectionManager.exe.config`

macOS Configuration File Location

`/Users/<yourusername>/Library/Preferences/com.Delinea.ConnectionManager.plist`

Unidirectional Clipboard Enforcement on MacOS

Administrators can unidirectionally restrict clipboard access from the RDP server to the users' local machine and vice-versa in both local and vault connections.

The effective clipboard redirection behavior is determined by two factors: the Secret clipboard value and the individual restrict flags for each direction (Server to Client and Client to Server):

- If the Secret clipboard value is false, all clipboard redirection is disabled regardless of restrict settings.
- If the Secret clipboard value is true, each direction is enabled unless its corresponding restrict flag is set to true.

If you would like to restrict users from copying information from the RDP server to their local machine, run the following command in the terminal:

```
sudo defaults write /Library/Preferences/com.Delinea.ConnectionManager.plist
disableclipboardservertoclient true
```

If you would like to restrict copying from the users' machine to the RDP server, run the following command:

```
sudo defaults write /Library/Preferences/com.Delinea.ConnectionManager.plist
disableclipboardclienttoserver true
```

For unidirectional clipboard enforcement on Windows see "Unidirectional Clipboard Enforcement on Windows" on page 174.

Enabling WebAuthn Authentication for All Users on MacOS

If you would like to enabling Webauthn authentication for all users, you will need to create a new parameter called `WebAuthnVaultEnforcement` and set the value to `y` as shown below:

```
sudo defaults write /Library/Preferences/com.Delinea.ConnectionManager.plist
WebAuthnVaultEnforcement y
```

Note: WebAuthn authentication admin enforcement only enforces vault connection

If you would like to enable Webauthn on Windows, see "Application Configuration via Windows Registry Editor" on page 163.

Preserving Configuration Changes During Upgrade on Windows

Starting with the 2.7 release, all manual changes in *userSettings*, *applicationSettings* and *log4net* sections of the application configuration file will be automatically saved upon upgrade. The application configuration file backup is stored at the following location: *C:\ProgramData\Delinea\Connection Manager Backup*

If you would like to replace your current application configuration file with the backup one, copy the *Delinea.ConnectionManager.exe.config.[version number].bak* file from the location mentioned above and rename it to the original application configuration file name: *Deline.ConnectionManager.exe.config*.

If you made changes to the application configuration file in Connection Manager 2.6.1 or older and you would like to save your changes when upgrading to a newer version, copy the needed values into the new configuration file. Later the modified configuration file can be shared to other environments.

Utilities like WinMerge can assist you in this process. There are important system parameters that should not be changed, such as "runtime", and this can causeConnection Manager to throw an error exception.

Disabling Update Check on Startup for Windows

To disable automatic checking for updates on startup, for Windows open the configuration file and change the value to False as depicted in the screen shot below.

```
<applicationSettings>
   <Delinea.ConnectionManager.Wpf.Properties.Settings>
     <setting name="UpdateOnStartup" serializeAs="String" >
        <value>false</value>
     </setting>
   </Delinea.ConnectionManager.Wpf.Properties.Settings>
</applicationSettings>
```

Disabling Update Check on Startup for macOS

To disable automatic checking for updates on startup for macOS, in Terminal type:

```
defaults write com.Delinea.ConnectionManager Env.CheckUpdateOnStartup -bool false
```

Enabling Software Rendering for the Internal Browser on Windows

The CEF browser is an internal browser built into Connection Manager. It has the same functionality as a regular web browser and can be useful for handling browser content redirection. It uses hardware accelerated rendering by default. If you are experiencing issues with it, you may opt to enable software rendering by running the following command.

Adjust the Application Configuration file setting with the needed value:

```
<setting name="SoftwareRenderForCEF" serializeAs="String">
   <value>True</value>
</setting>
```

Enabling/Disabling Auto Reauthenticate

This feature provides the option to configure vault reauthentication behavior in Connection Manager. Users may keep the existing behavior that automatically restarts the authentication flow or force a fresh login when their vault session/refresh tokens have expired--mimicking the existing web API behavior.

The default value is **y** which automatically restarts the authentication flow. If the value is set to **n**, the behavior will be more similar to the web API which forces a fresh login. The **n** option is beneficial for users who use SAML

configuration through an external identity provider with a longer session/refresh length and enables audit logs to correctly generate upon logout.

Important: Please see the "User Configuration File for Windows" on page 183 file for editing this parameter on Windows.

Example for Windows

Adjust the Application Configuration file setting with the needed value:

```
<setting name="AutoReauthenticate" serializeAs="String">
    <value>n</value>
</setting>
```

Example for macOS

Run the following command in the MacOS terminal:

```
defaults write com.Delinea.ConnectionManager Env.AutoReauthenticate false
```

Run the following command in the MacOS terminal:

Enabling the Session Status Popup on Windows

The Session Status popup window is disabled by default. This window would appear every time a user signed out of a session, confirming that they also signed out of the server. However, if you are experiencing memory leak issues, Delinea recommends enabling this window with the following command:

Adjust the Application Configuration file setting with the needed value:

```
<Delinea.ConnectionManager.Wpf.Properties.Settings>
      <setting name="ShowDisconnectMessage" serializeAs="String">
        <value>True</value>
      </setting>
</Delinea.ConnectionManager.Wpf.Properties.Settings>
```

Configuring Proxy Settings

Users can configure the proxy settings via the following command after *</startup>*

Adjust the Application Configuration file setting with the needed value:

```
<system.net>
    <defaultProxy enabled="True" useDefaultCredentials="True">
        <proxy proxyaddress="http://proxy.test.com:8080" />
    </defaultProxy>
</system.net>
```

Important: This parameter should only be added under the direction of your administrator. Any errors in configuration could cause errors authenticating to the Delinea Platform or Secret Server.

Setting the Screenshot Queue Limit

If you have session recording enabled and are experiencing unstable internet connectivity, Connection Manager may no longer be able to send screenshots to the server and your session will be terminated. If you continue to experience internet connectivity issues, you can try increasing the screenshot queue limit to allow screenshots to be temporarily saved locally until connectivity is restored. The screenshot queue limit can be increased by changing 0 to any positive value in the following commands:

Windows

Adjust the Application Configuration file setting with the needed value:

```
<setting name="ScreenshotsQueueLimit" serializeAs="String">
   <value>0</value>
</setting>
```

macOS

Run the following command in the MacOS terminal:

```
defaults write com.Delinea.ConnectionManager Env.ScreenshotsQueueLimit -int 0
```

Configuring RDP Connection Timeout Over TCP

This configuration allows the ability to customize RDP connection timeouts in seconds. This is helpful for situations involving proxy, MFA, or other configurations that require additional time to connect before timeout due to inactivity. The timeout can be adjusted as needed, but the recommended suggestion is to start with 60 seconds as shown below:

MacOS

Run the following command in the MacOS terminal:

```
defaults write com.Delinea.ConnectionManager Env.RDPConnectionTimeout -int 60
```

In Connection Manager versions 2.5.x, the timeout was configured using the `SSH.ConnectionTimeOut` value, which was measured in milliseconds. This value will be deprecated in the next release.
Upgrade Behavior: If you upgraded from a 2.5.x version and already had a value set for `SSH.ConnectionTimeOut` (in milliseconds), this value will be ignored if a new value is explicitly set in the `Env.SSH.ConnectionTimeOut` parameter.
Default Value: If no value was previously set in `SSH.ConnectionTimeOut`, the `Env.SSH.ConnectionTimeOut` parameter will default to 60 seconds.

Windows

Adjust the Application Configuration file setting with the needed value:

```
<setting name="RdpConnectionTimeout" serializeAs="String">
    <value>60</value>
</setting>
```

Important: In versions 2.5.x of Connection Manager, this value was measured in milliseconds. If users already had a value set in milliseconds, Connection Manager will preserve that value after upgrade. Otherwise, the default value will be set, which is 60 seconds.

Configuring SSH Connection Timeout Over TCP

This setting allows administrators to configure the amount of time (in seconds) during which a user can be inactive (i.e., not interacting with the system in any way) without any impact on their SSH session. After the timeout expires, the user will be disconnected from the session and session itself will be closed. The default value is set at 60 seconds, but can be adjusted as needed by changing the value shown in the example below:

Windows

Adjust the Application Configuration file setting with the needed value:

```
<setting name="SSHConnectionTimeout" serializeAs="String">
    <value>60</value>
</setting
```

Important: In versions 2.5.x of Connection Manager, this value was measured in milliseconds. If users already had a value set in milliseconds, Connection Manager will preserve that value after upgrade. Otherwise, the default value will be set, which is 60 seconds.

MacOS

Run the following command in the MacOS terminal:

```
defaults write com.Delinea.ConnectionManager Env.SSHConnectionTimeout -int 60
```

In Connection Manager versions 2.5.x, the timeout was configured using the `SSH.ConnectionTimeOut` value, which was measured in milliseconds.This value will be deprecated in the next release.
Upgrade Behavior: If you upgraded from a 2.5.x version and already had a value set for `SSH.ConnectionTimeOut` (in milliseconds), this value will be ignored if a new value is explicitly set in the `Env.SSH.ConnectionTimeOut` parameter.
Default Value: If no value was previously set in `SSH.ConnectionTimeOut`, the `Env.SSH.ConnectionTimeOut` parameter will default to 60 seconds.

Adjusting the SSH Scrollback Buffer Size on MacOS

Adjusting the value of the SSH scrollback buffer size allows users to update the amount of lines they can scroll back inside the terminal during the SSH session to view the session history. The default value is set at 10,000 lines, but it can be increased to as much as 100,000 lines as shown in the example below. After adjusting the scrollback buffer size you will need to restart Connection Manager for the changes to take effect.

Run the following command in the MacOS terminal:

```
defaults write com.Delinea.ConnectionManager SSH.TerminalScrollback -int 100000
```

Note: It is not recommended to set the scrollback buffer size to more than 100,000 lines since this could negatively impact the performance of the SSH terminal.

Backing Up .DAT Files and Configurations

Starting with the 2.7.0 release, Connection Manager automatically backs up as default your .dat files and application configurations. The default parameters are shown below:

Windows

```
<setting name="SettingsAutoBackup" serializeAs="String">
        <value>True</value>
      </setting>


<setting name="SettingsAutoBackupInterval" serializeAs="String">
        <value>UpgradeOnly</value>
      </setting>
```

MacOS

```
defaults write com.Delinea.ConnectionManager Env.SettingsAutoBackup - true


defaults write com.Delinea.ConnectionManager Env.SettingsAutoBackupInterval - UpgradeOnly
```

See "Automatic Back Up for .DAT Files and Configurations" on page 128 for more information.

Configuring Special Characters in SSH Connections on MacOS

The `Env.OptionAsMetaKey` setting allows you greater control over of how Connection Manager handles special characters and symbols when working in SSH connections. This setting is a preference that can be set at the user level.

- The default setting is `true`, which enables the use of the Option key as a Meta key in the terminal during SSH connections.
- When set to `false`, this setting permits the use of special symbols (e.g., @, #, ~) in certain keyboard layouts, particularly non-English keyboards, during terminal sessions over SSH connections.

  Example:

```
defaults write com.Delinea.ConnectionManager Env.OptionAsMetaKey -bool false
```

Incorrect Handling of System Keys

In the event that system keys are not handled correctly, users will need to adjust the corresponding parameters in the config file *user.config* by setting the variable "SshFunctionKeysMode". The default value is "CommonExtended" but can be set to the following values:

- CommonExtended
- Common
- Linux
- XtermR6
- VT400
- VT100Plus
- Sco
- CommonAlternative
- VT52
- LinuxAlternative
- ScoAlternative
- Wyse60
- HpUx
- Pick

Note: Strings are case sensitive

User Configuration File for Windows

This file contains parameters pertaining to individual users.

Windows Configuration File Location

C:\Users\Dell\AppData\Local\Delinea_Inc

Enabling/Disabling Auto Reauthenticate on Windows

This feature provides the option to configure vault reauthentication behavior in Connection Manager. Users may keep the existing behavior that automatically restarts the authentication flow or force a fresh login when their vault session/refresh tokens have expired--mimicking the existing web API behavior.

The default value is **y** which automatically restarts the authentication flow. If the value is set to **n**, the behavior will be more similar to the web API which forces a fresh login. The **n** option is beneficial for users who use SAML configuration through an external identity provider with a longer session/refresh length and enables audit logs to correctly generate upon logout.

Example

```
<setting name="AutoReauthenticate" serializeAs="String">
    <value>n</value>
</setting>
```

Re-enabling the Web Launcher Training Dialog

If you opted out of displaying the web launcher training dialog and would like to re-enable it, update the value of the `TrainingDialogWebLauncherHide` value to *False* or delete this setting entirely:

```
<setting name="TrainingDialogWebLauncherHide" serializeAs="String">
    <value>False</value>
</setting>
```

Re-Enabling the Browser Extension Not Found Dialog

If you opted out of displaying the *Browser extension not found* dialog and would like to re-enable it, update the value of the *DoNotShowWebBrowserError* value to *False*:

```
<setting name="DoNotShowWebBrowserError" serializeAs="String">
    <value>False</value>
</setting>
```

User Settings on MacOS

This file contains parameters pertaining to individual users.

Note: Delinea cautions against deleting user plist files via sudo as this can cause file permissions to break.

User Settings File Location

/Users/[username]/Library/Preferences/com.Delinea.ConnectionManager.plist

Re-enabling the Web Launcher Training Dialog

If you opted out of displaying the web launcher training dialog and would like to re-enable it, update the value of the `TrainingDialogWebLauncherHide` value to *False* or delete this setting entirely:

```
defaults write com.Delinea.ConnectionManager Env.TrainingDialogWebLauncherHide -bool false
```

Re-Enabling the Browser Extension Not Found Dialog

If you opted out of displaying the *Browser extension not found* dialog and would like to re-enable it, update the value of the *DoNotShowWebBrowserError* value to *False*:

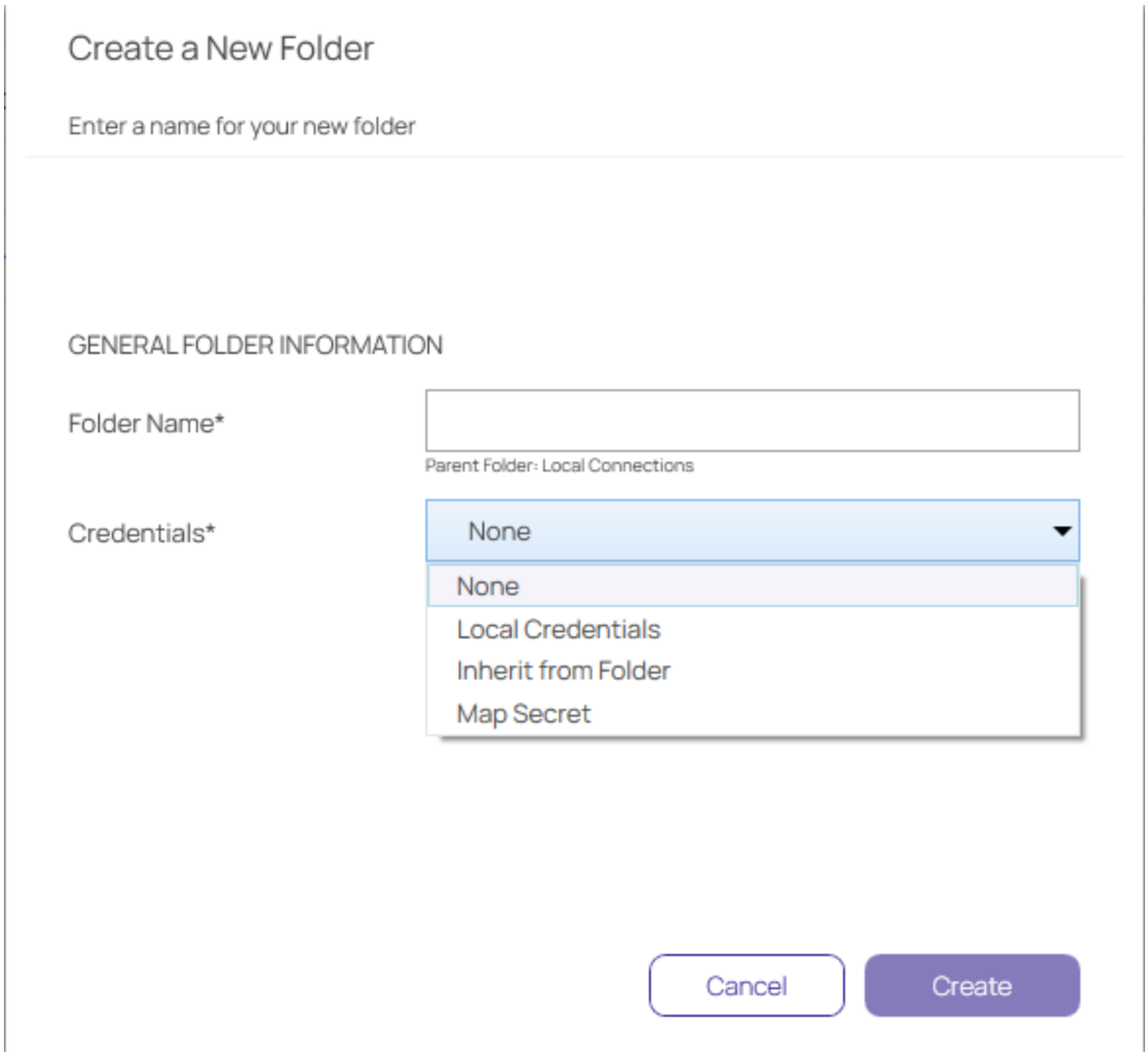
```
defaults write com.Delinea.ConnectionManager Env.DoNotShowWebBrowserError -bool false
```

Folder: Creating, Editing, Moving, Deleting

Creating a New Folder

Connection Manager uses folders to help organize local connections.

1. Navigate to the location where a new folder should be created.
2. Right-click and select **New Folder**.

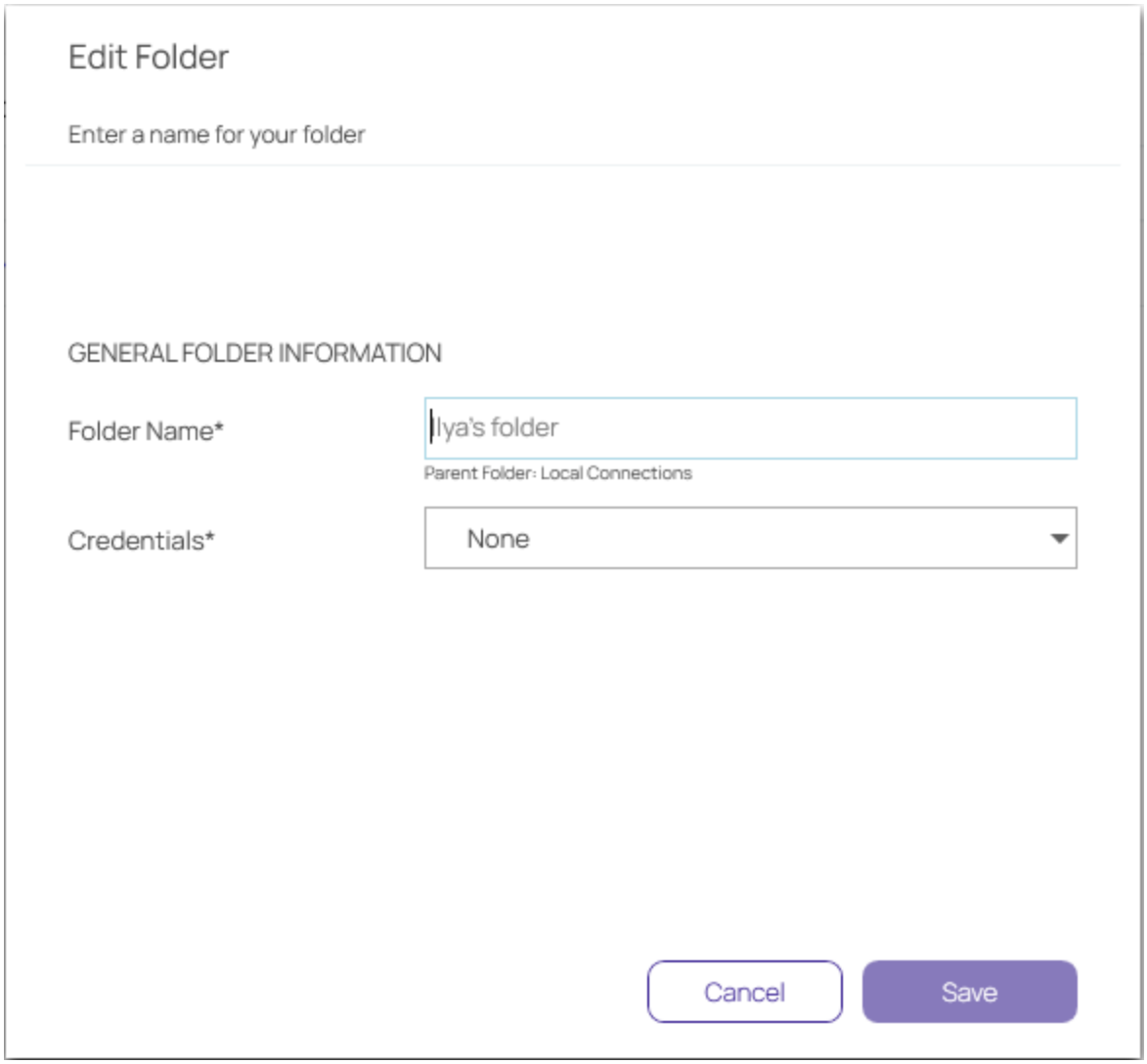


3. Enter the **Folder Name** and click **Create**.
4. Choose the appropriate **credential option** from the list:
   - **None**: No credential values will be set or required for the new folder.
   - **Local Credentials**: Allows a user to create the credentials for the new folder.
   - **Inherit from Folder**: Allows a user to set credentials for a sub-folder to imitate the folder in which it will reside.
   - **Map Secret**: Allows a user to apply secrets to the new folder.

View Integrated Connections for additional information on credentials.

Editing a Folder

1. Navigate to the folder to be edited and right-click. The Edit Folder dialog box opens.



2. Make any desired change to the folder and click **Save**.

View the Integrated Connections section for additional information on credentials.

Moving a Folder

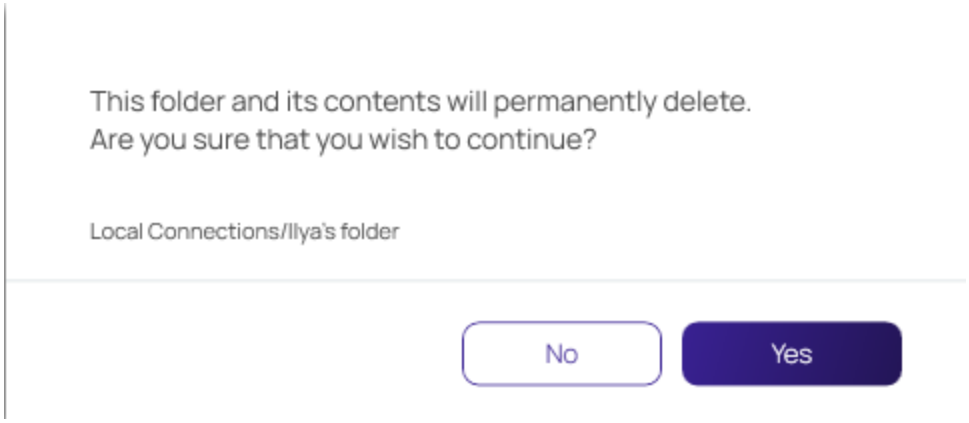
Move folders to organize them by dragging and dropping them in the Local Connections view.

Deleting a Folder

When a folder is deleted, the folder and its contents (Local connections and other folders) are deleted.

Important: This action is **NOT** reversible. Once a connection is deleted it cannot be recovered.

1. Navigate to the folder to be deleted.
2. Right-click the **folder name** and select **Delete**. A confirmation modal opens.

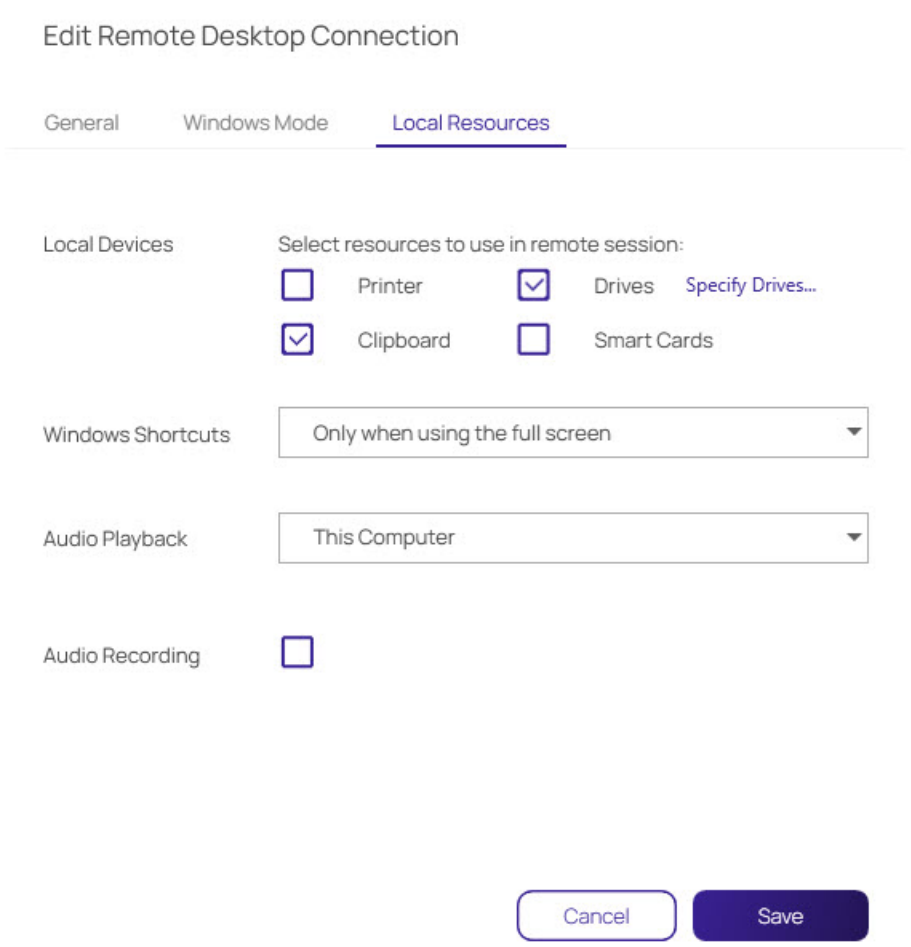


3. Select **Yes** to confirm.

Transferring Files Using Local Drives

Customers can copy files from their local machine to remote targets, and vice versa, by mapping local drives to remote targets via RDP when using Connection Manager.

1. Right click on a local connection and click **Edit**.
2. Click the Local Resources tab.
3. In the Local Devices section, check the Drives box.



4. Specify the drives to use in the remote session and click **OK**.

Note: You can also set this as the global configuration default in the global RDP settings.

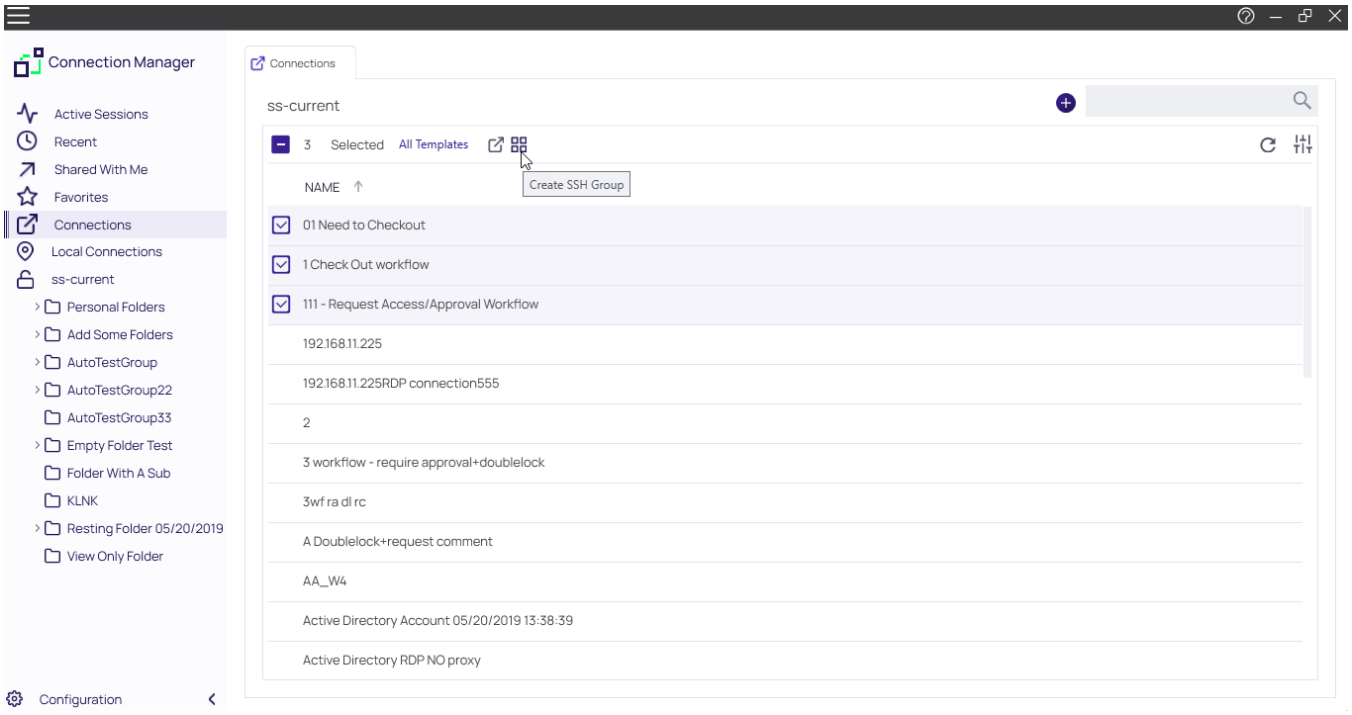
Using SSH Session Groups

Users can now create one or more groups of active SSH sessions, then send a command or a series of commands in bulk to all active sessions in the group.

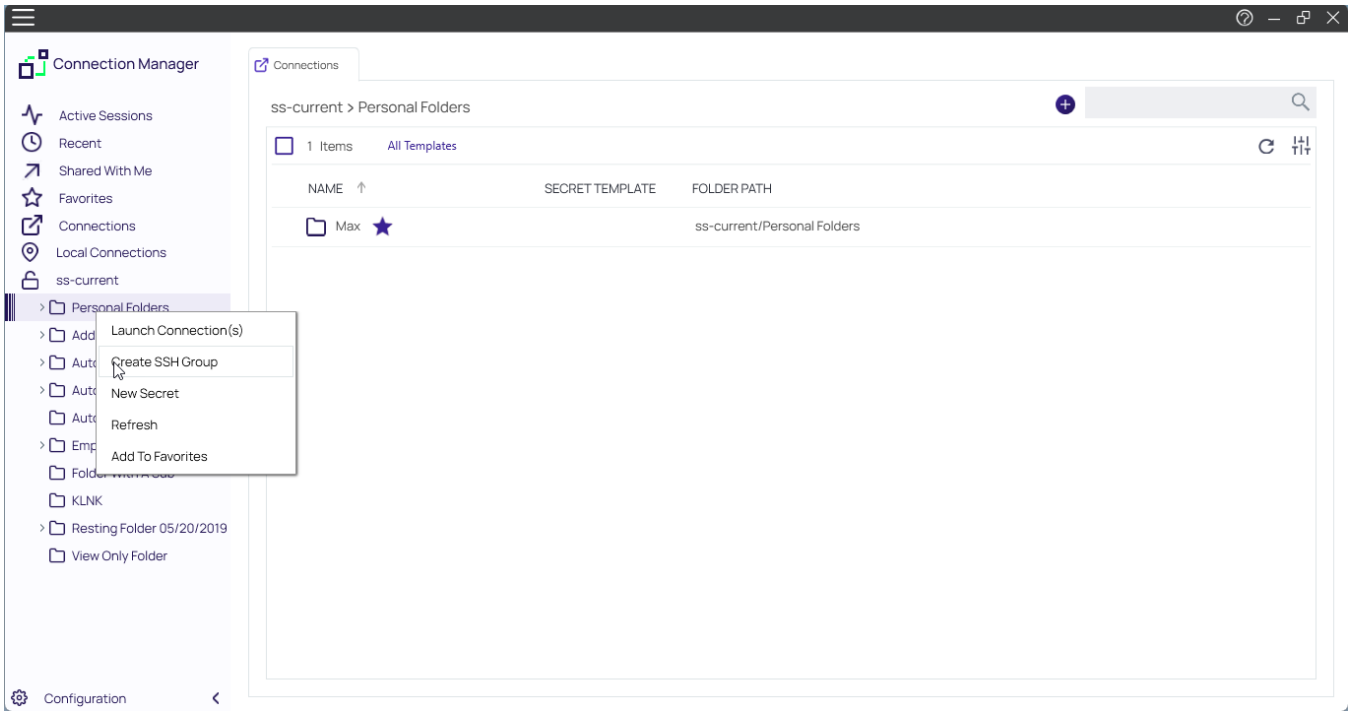
Creating and Naming an SSH Group

You can create a new SSH Group two ways. The first is this way:

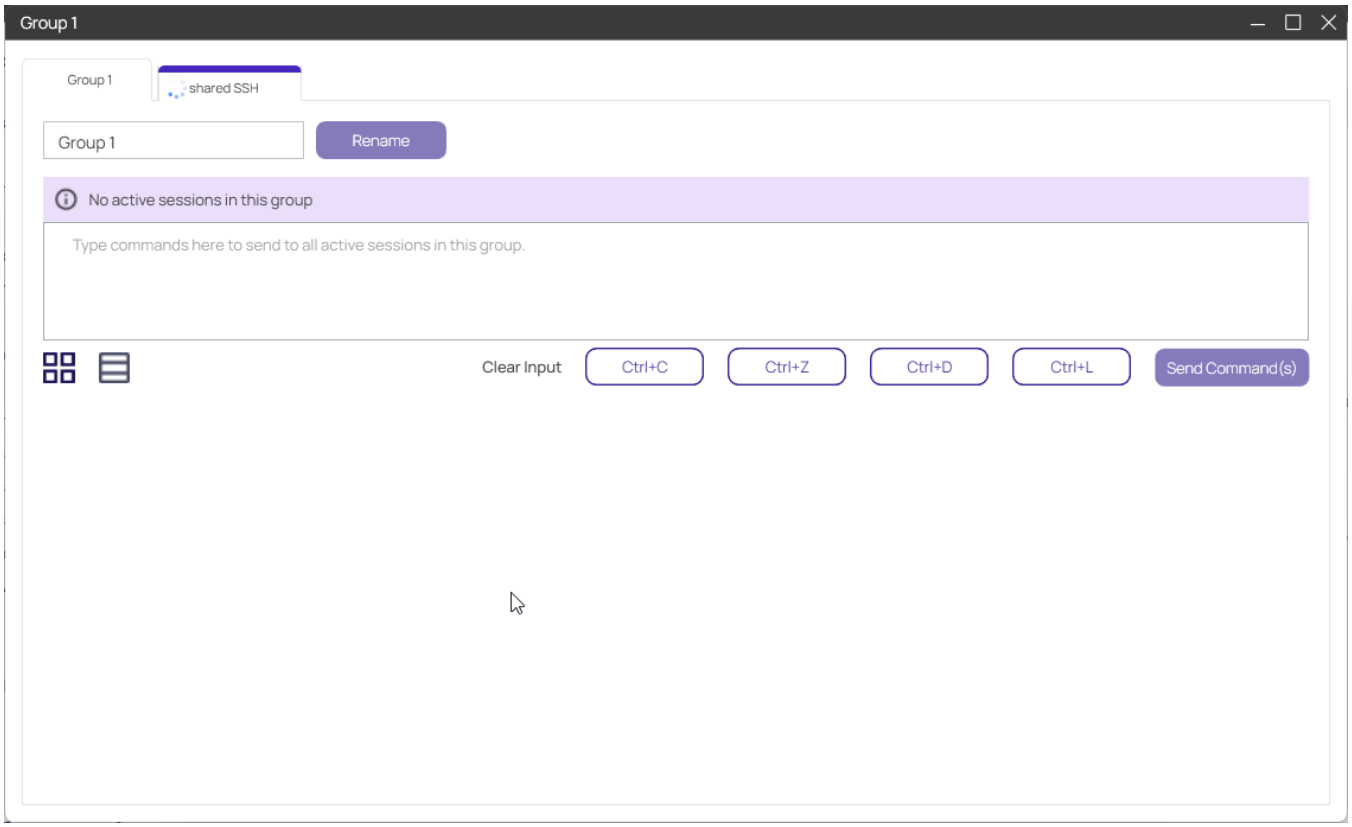
1. Select the sessions you want to include in the group
2. Click the **Create a Group** toolbar icon.



The second is to use the **Create SSH Group** option in right-click context menus.



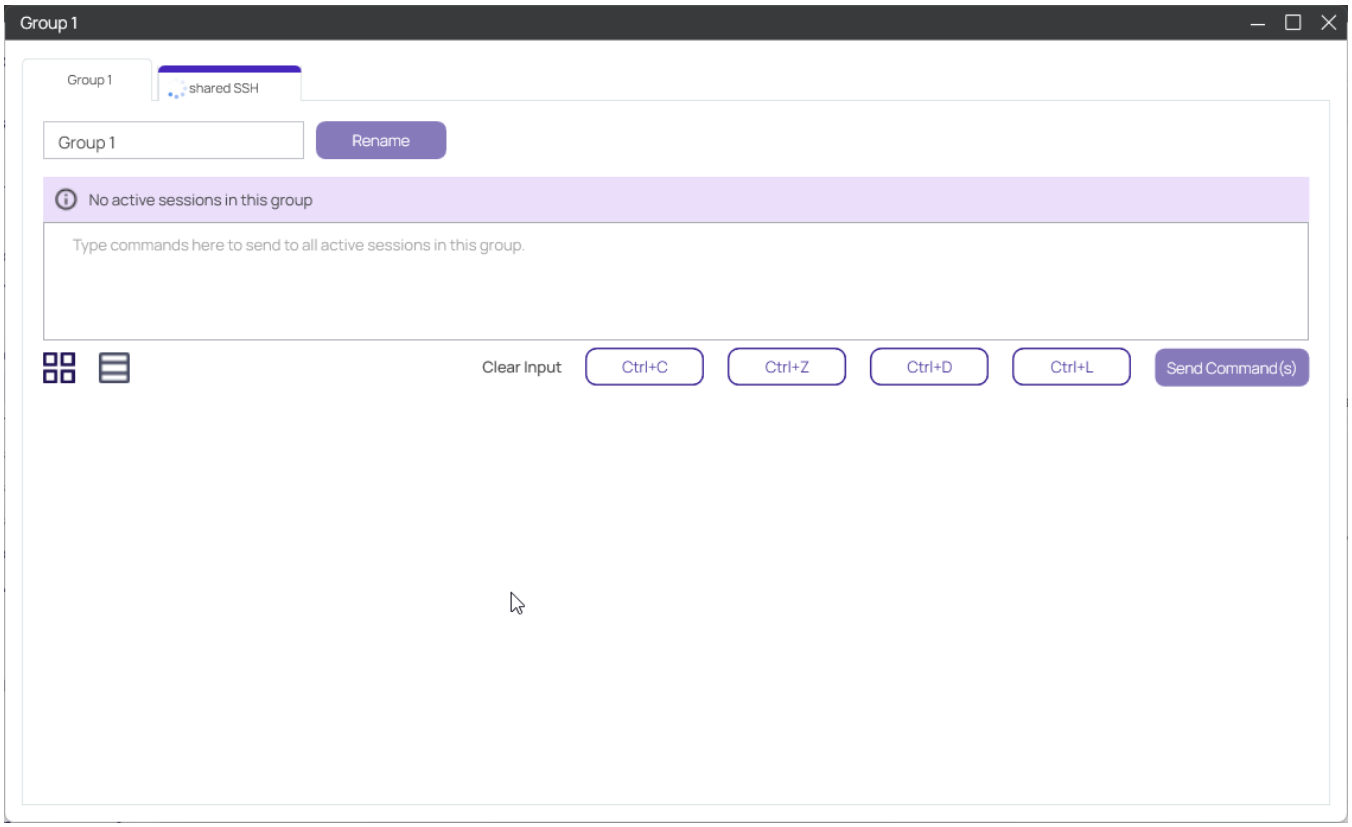
When the SSH Group is created, it opens in its own window with a special Group tab followed by the individual tabs for each SSH session in the group.



If the user has generated the SSH Group from sessions occupying a single folder, the group tab will be labeled with the name of the original folder. If the user has generated the SSH Group from sessions that did not occupy a single folder, the group tab will be labeled with a generated sequential name such as Group 1, Group 2, etc. The user can always change any group name from the name it was assigned initially.

Sending Commands to the SSH Group

At the top of the Group tab is a command window, where users can input one or more commands to send to all sessions in the group. To send a single command, the user simply enters the command and presses the Enter key or clicks the **Send Command(s)** button. To send a series of commands as a group, the user enters each command followed by Ctrl+Enter. When the user has entered the last command in the series, pressing the Enter key or clicking the **Send Command(s)** button sends all of the commands to all SSH sessions in the group, following the sequence in which they were entered.



The four commands listed below are built into the user interface as individual buttons:

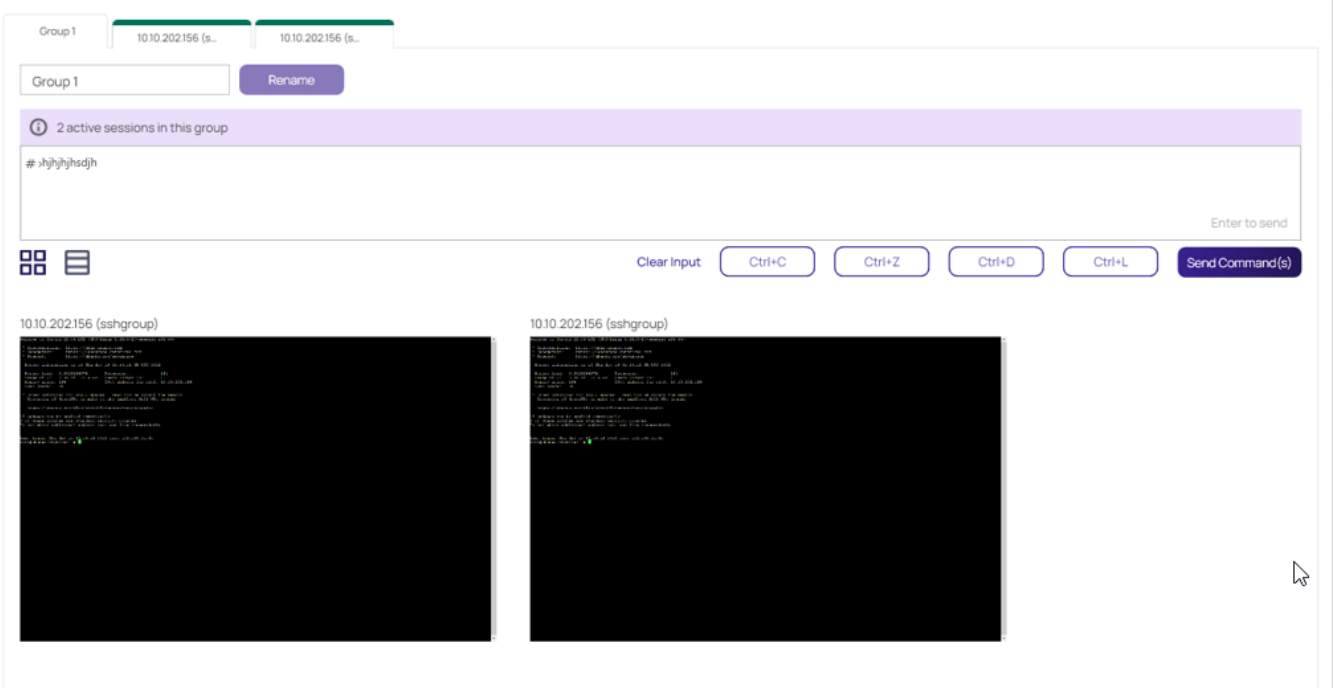
- **Ctrl+C** Kill whatever you are running. The confirmation alert should be displayed, the command should be broadcast to all sessions, and the top command should be stopped.
- **Ctrl+D** Exit the current shell. The "exit" should be displayed on all SSH sessions in the group; all sessions in the group should be closed, and the Group window should be closed.
- **Ctrl+L** Clear the screen, similar to the Clear command.
- **Ctrl+Z** Send whatever you are running into a suspended background process. fg restores it. The top command should be sent into the background.

Options for Displaying SSH Sessions on the Group Tab

The main SSH Group tab displays the SSH sessions in a grid by default. In this grid view the session panels do not change size, but as the user makes the Group window larger or smaller, the panels rearrange themselves in the window for optimal fit and display.

The user can change the display of SSH sessions from a grid to a stack (single column) layout, which leaves more horizontal space across the window, allowing each session to be enlarged for better visibility. The two views can be toggled back and forth using the grid and stack icons shown below.





Building an SSH Group

An SSH session cannot belong to more than one group at a time, so you cannot add an SSH session that already belongs to an SSH Group into a second SSH Group. But if an SSH session does not belong to any group, you can add it to an existing SSH Group by detaching the session tab from a window and dragging and dropping the tab into the Group window. Once a session has been added to a Group, you cannot remove the session from the group by detaching its tab and dragging it elsewhere.

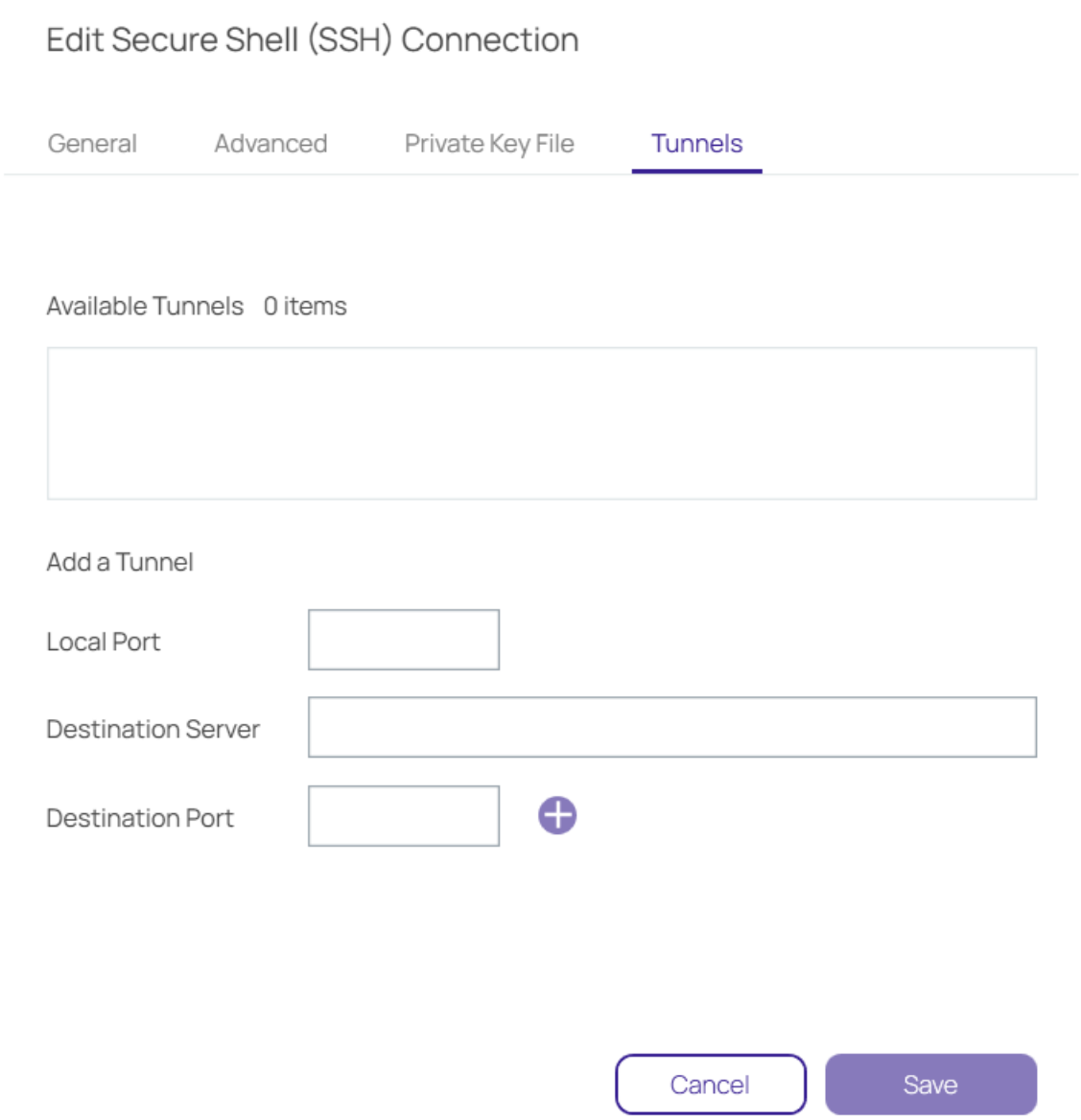
Closing an SSH Group

You cannot close an SSH Group by closing the Group tab or by removing the active sessions. The only way to close an SSH Group is to close the Group window.

SSH Tunneling

SSH tunneling is a method to transport additional data streams within an existing SSH session. To create an SSH tunnel, left click on an SSH connection. The **Edit SSH Connection** window appears.

In the Tunnels tab, you will see available tunnels, if any, as well as the ability to add a new tunnel.



Secrets with Workflows

Connection Manager supports a variety of Delinea Platform and Secret Server workflows associated with remote connections and the workflows functions are very similar to Secret Server such as:

- Multi-factor authentication
- Require Comment
- Check in or Check out (Able to check-in a secret if it was checked-out by the same user)
- Change Password on Check-in

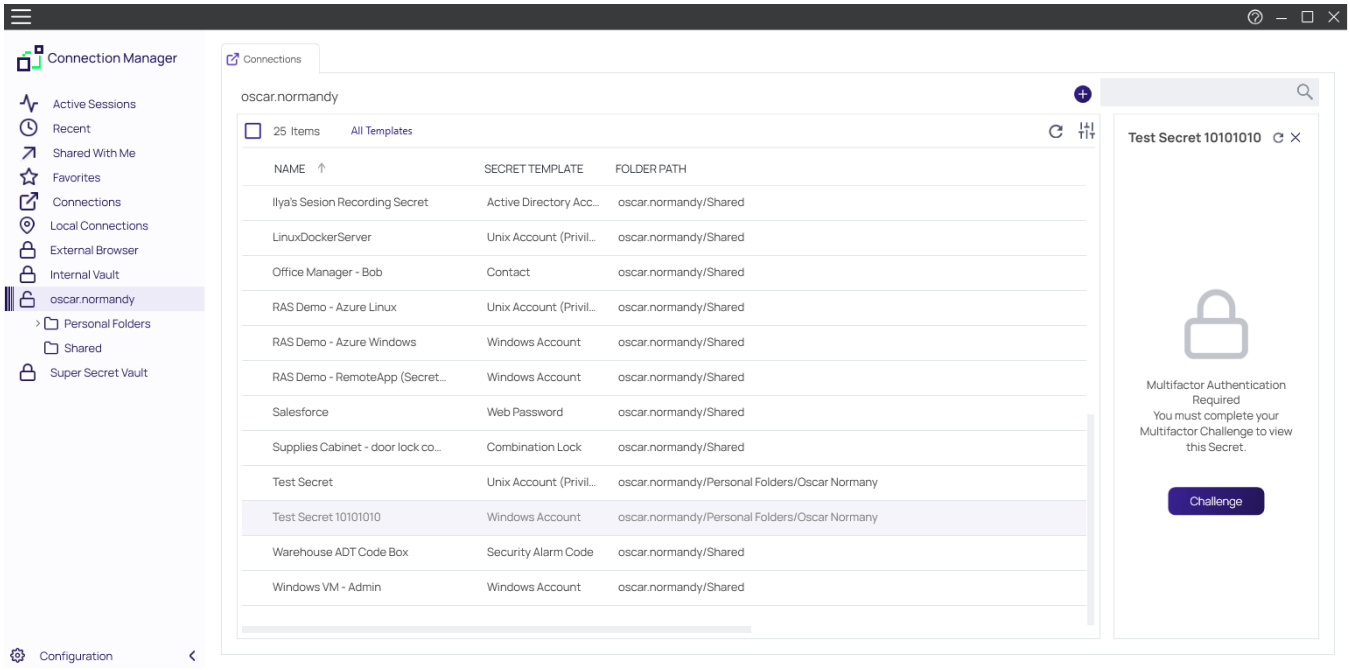
- Prompt for Reason or Ticket System
- Request Access
- QuantumLock

Users will see a notification in the secret properties pane and if a Secret has a workflow associated with it, Connection Manager will prompt you for the appropriate workflow options in the Properties pane. Please see the Secret Server Secret Workflows.

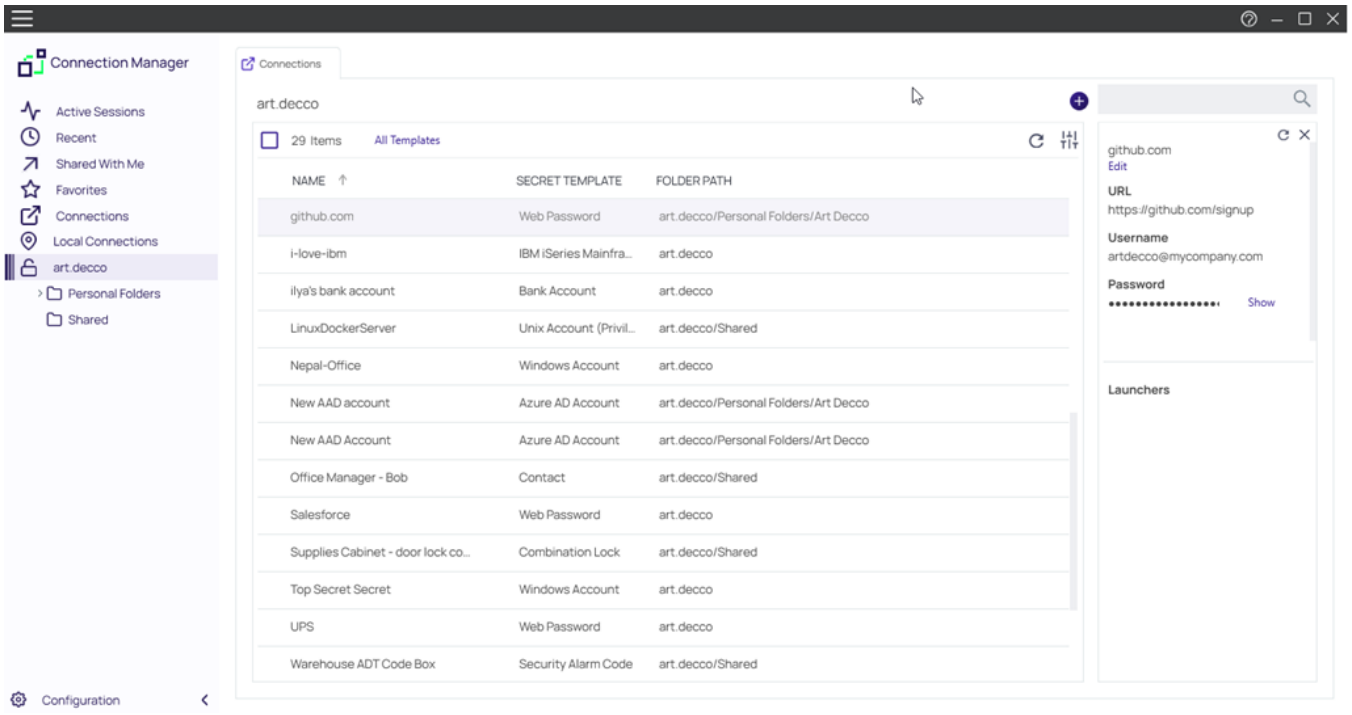
Once the workflow is successful, the connection is established.

Accessing Secrets Guarded by Multi-Factor Authentication

Delinea Platform users can access secrets guarded by MFA through Connection Manager. The authentication challenge can be completed via external or internal browser. When a user attempts to access a secret guarded by MFA, they will see a message that they must complete an additional MFA challenge:



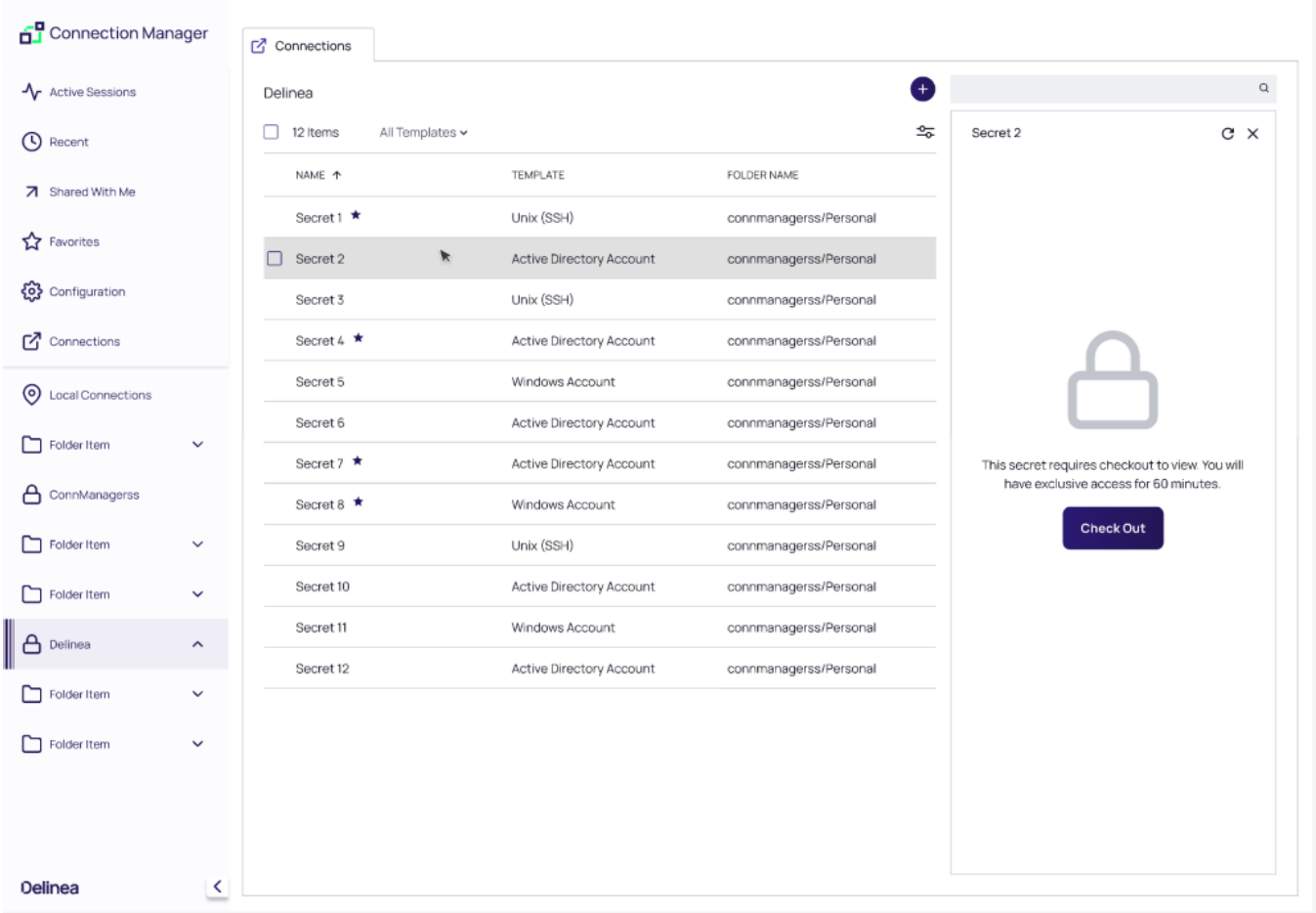
After clicking **Challenge**, users will be prompted to complete the MFA challenge in a separate Connection Manager window. When the MFA challenge has been successfully completed, users can return back to Connection Manager to view or launch the secret.



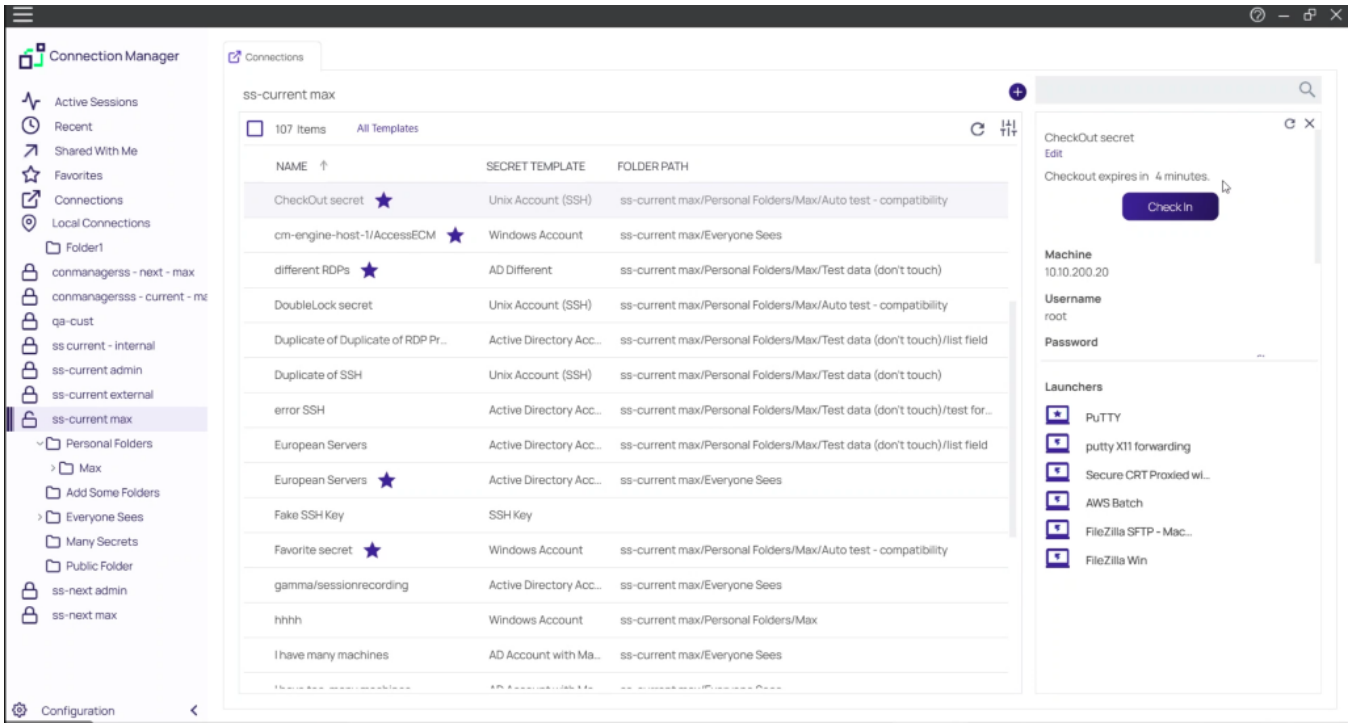
Secret Check Out Timer

As part of the secret workflow, Connection Manager offers a secret check out timer which informs users how much time they have remaining to access a secret. The workflow for the secret checkout timer is described below:

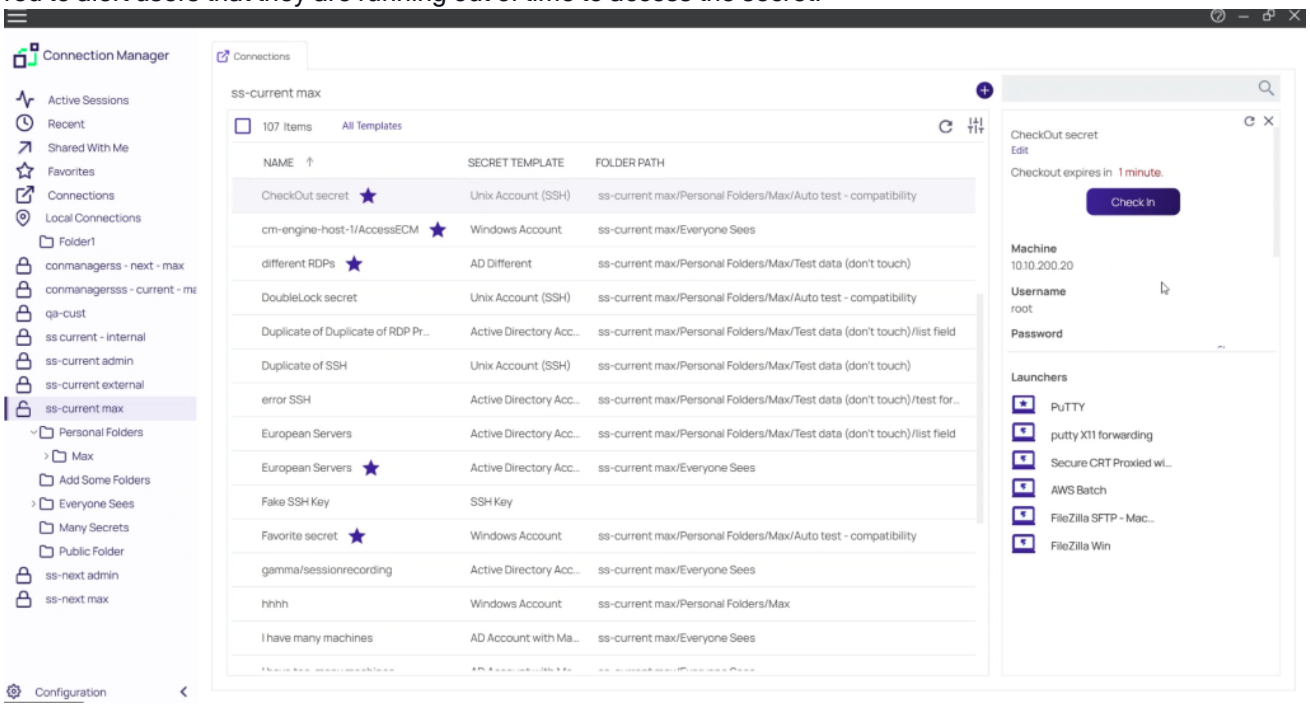
1. Simply click on any secret and in the right pane you will see information on whether or not the secret requires check out and how much time you will have to access the secret.



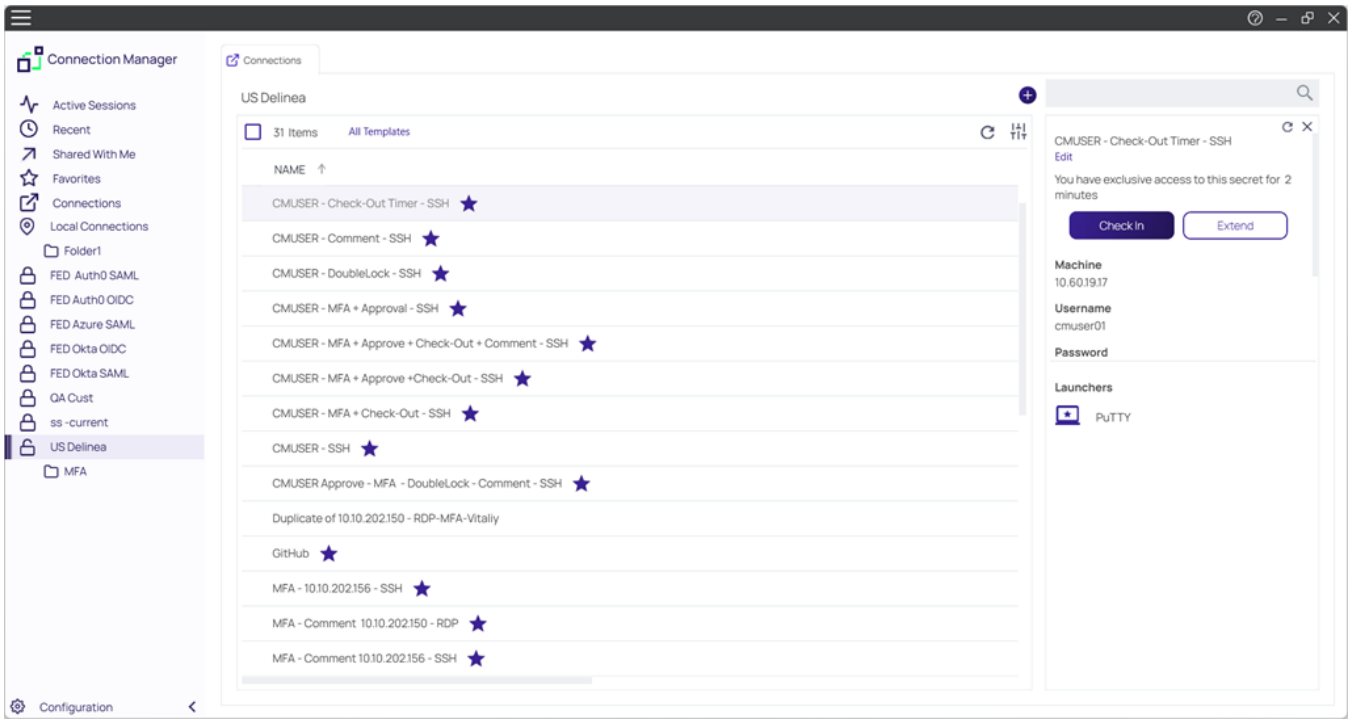
2. If the secret requires check out, click **Check Out**
3. Once you have been granted access to the secret, you will see a timer in the right pane, along with all of the needed information about the secret.



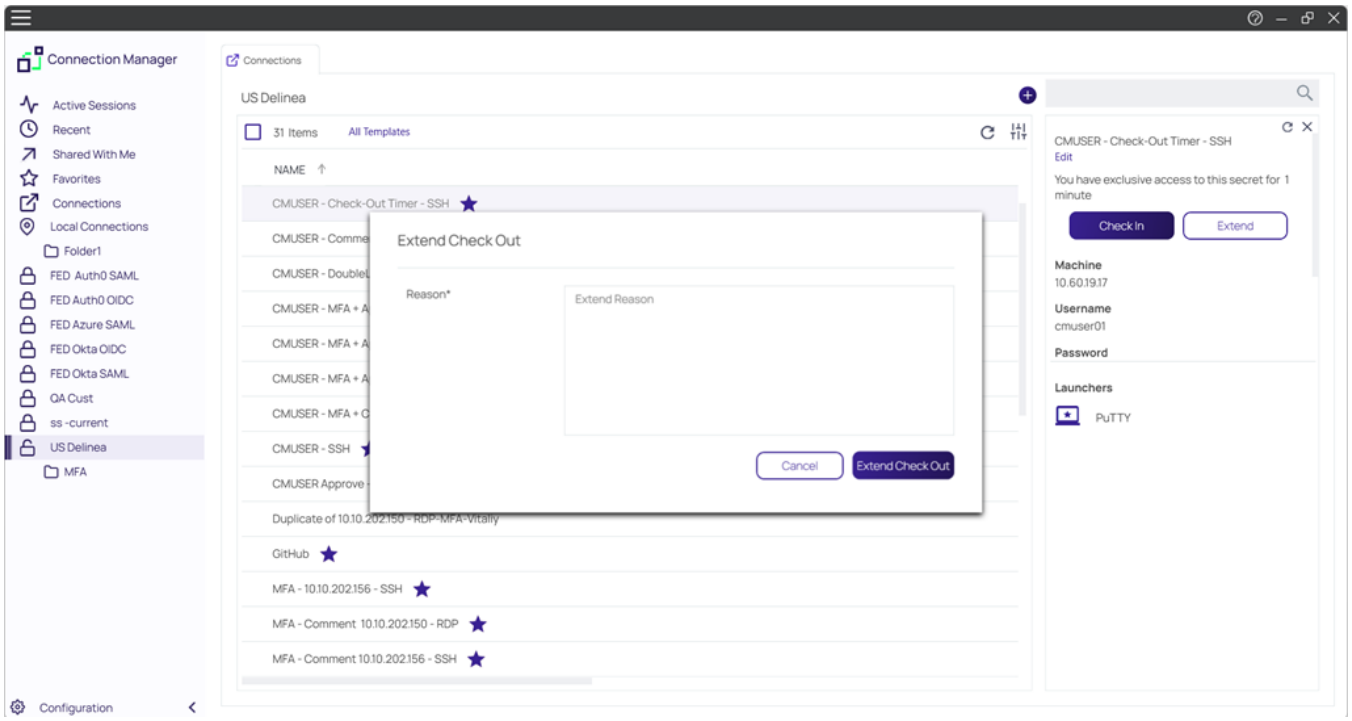
4. When the time remaining with the secret falls below the threshold set in Secret Server, the timer color will turn red to alert users that they are running out of time to access the secret.



5. Users can extend the secret check out timer by clicking **Extend**. (Optional)

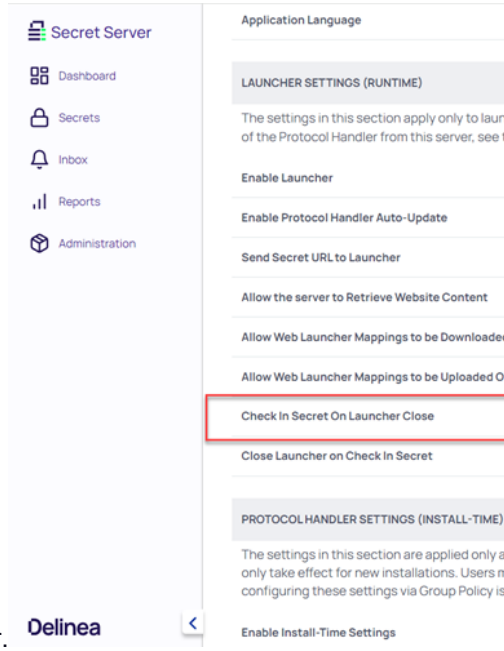


Users must enter a reason for extending the secret check out time



Important: The extend check out functionality needs to be configured in Secret Server.

Note: Connection Manager automatically checks in secrets after the user logs off the endpoint server. To prevent this from occurring, please adjust the relevant setting in Secret Server.



Troubleshooting

This section provides helpful troubleshooting tips and answer to frequently asked questions.

- General
- "CM Crashing When Offline and Checking Certificates" on page 219
- AVBlock Error with Session Recording
- Host Names
- Encryption
- Licensing
- Generate Additional Log Entries

Log Files

The Connection Manager log files can be found at the following default locations:

Windows Log File Location

```
C:\Users\{username}\AppData\Roaming\Delinea\Connection Manager\ConnectionManager.log
```

CEF Browser Log File Locations

- `C:\Users\{username}\AppData\Local\CEF\User Data`
- `C:\Users\{username}\AppData\Roaming\Delinea\Connection Manager\CefBrowser.log`

MacOS Log File Location

```
~/Users/{username}/Library/Application Support/Delinea/Connection
Manager/ConnectionManager.log
```

> **Note:** If a user installs Connection Manager for all users on the machine, the log files will be located in: `~/Users/{username}/Library/Application Support/Delinea/Connection Manager/ConnectionManager.log`

Installer Log File Locations

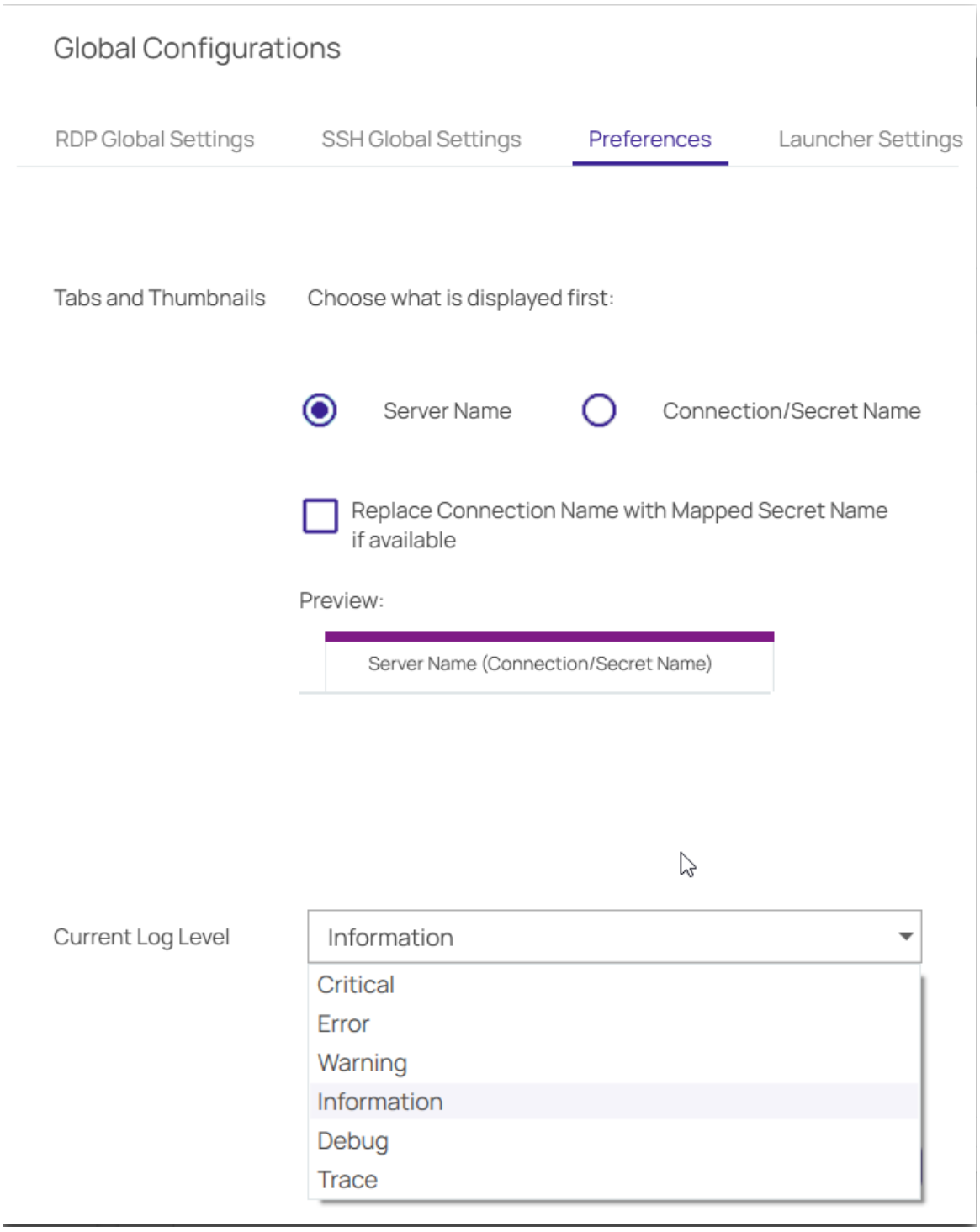
On Windows, the install log files will be located in the same location as the installation file. For example, if the installer is in Downloads, the installer log file will be there as well.

On MacOS, the install log can be found at the following location:

```
~/Library/Logs/Delinea/Delinea Connection Manager/install.log
```

Changing the Log Level

On Windows system the default log level can be changed in the Preferences tab in the Global Configuration settings. This can be done without admin rights:



On macOS you change the logging level of Connection Manager's logs to DEBUG mode by opening **Terminal** and typing:

```
defaults write com.Delinea.ConnectionManager Log.FileLevel Debug
```

Note: For Connection Manager versions 1.7 and older, the directory names will use *Thycotic* instead of *Delinea*

Generating Additional Log Entries

Should you need to generate more detailed logging to help troubleshoot Connection Manager issues, you can set the log level to DEBUG per the steps below. Setting the log level to DEBUG will generate larger log files so it is recommended that you return the setting back to INFO when you are done troubleshooting.

1. Open the Application Configuration File:
   - **Windows default location:**C:\Program Files\Delinea\Delinea Connection Manager\Delinea.ConnectionManager.exe.config
   - **macOS default location:** /Users/<yourusername>/Library/Preferences/com.Delinea.ConnectionManager.plist
2. Find the snippet below and change `INFO` to `DEBUG`.

Note: For Connection Manager versions 1.7 and older, the directory names will use *Thycotic* instead of *Delinea*

Before:

```
<root>
  <level value="INFO" />
  <appender-ref ref="LogFileAppender" />
  <appender-ref ref="TraceAppender" />
</root>
```

After:

```
<root>
  <level value="DEBUG" />
  <appender-ref ref="LogFileAppender" />
  <appender-ref ref="TraceAppender" />
</root>
```

Advanced Log Entries

Setting the log level to TRACE will enabled more advanced debugging scenarios as needed. Remember to turn off TRACE once debugging is complete as this can significantly impact log file size over an extended period of time.

```
<root>
  <level value="TRACE" />
```

```
    <appender-ref ref="LogFileAppender" />
    <appender-ref ref="TraceAppender" />
  </root>
```

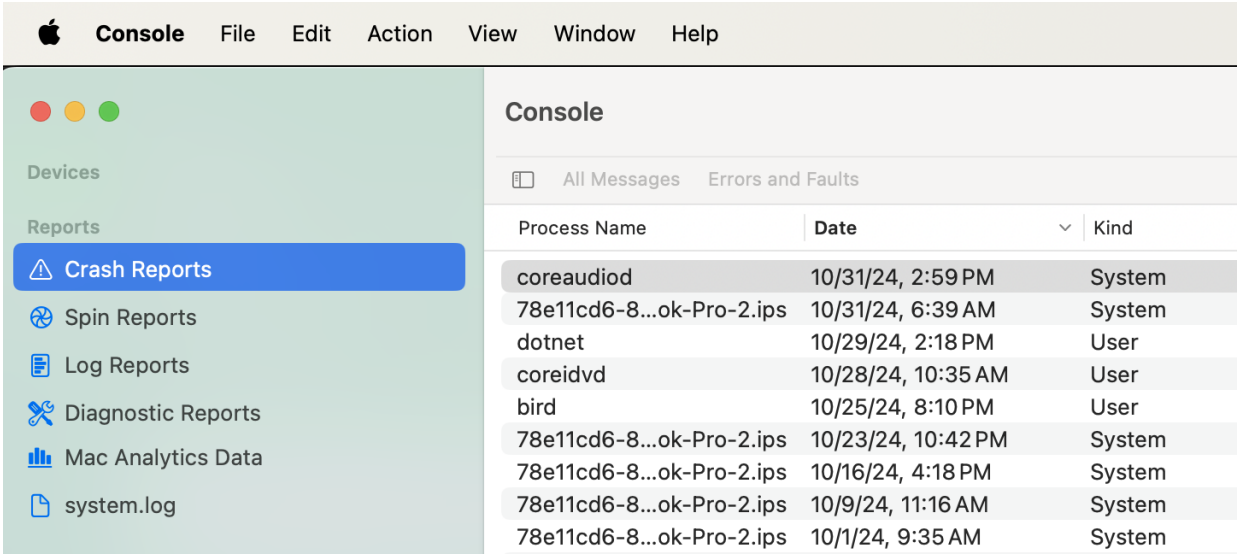
MacOS Installer Log Entries

To generate MacOS installer log entries:

1. Check the crash reports from installer app:
   a. Open the Console app
   b. Select *Crash Reports* on the right
   c. Check if there are any crash reports for the installer process

   If there are installer crash reports:

   a. Right click on the report
   b. Reveal in Finder
   c. Send as a crash report file



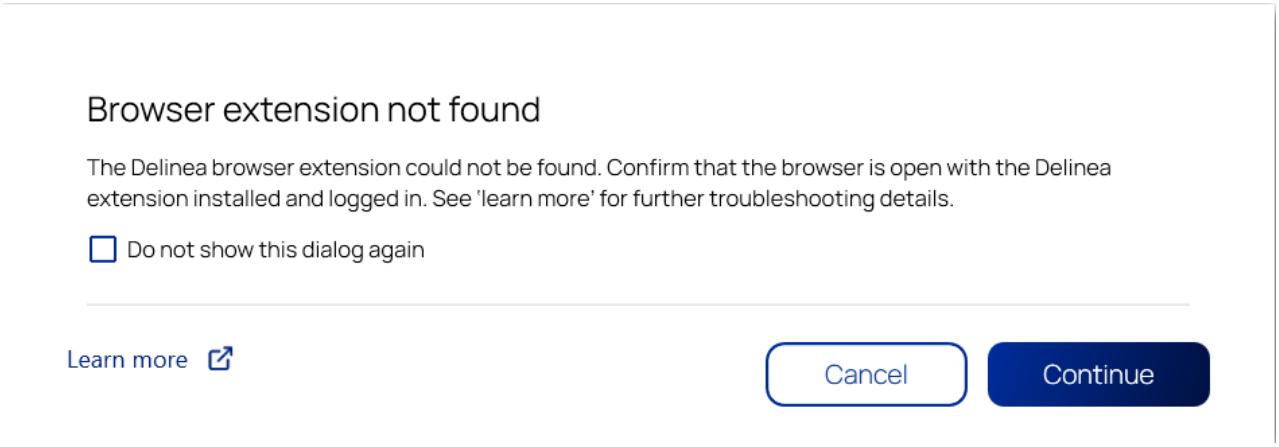
2. Check the */var/log/install.log* file.
3. Check the `/Library/Logs/Delinea/Delinea\ Connection\ Manager` folder and locate the *installer.log* file.

   Send these files to the Delinea Support team, if you have permission to do so.

Troubleshooting Website Launcher Issues

The following are common issues you may encounter when launching websites and auto-filling credentials with the Web Password template.

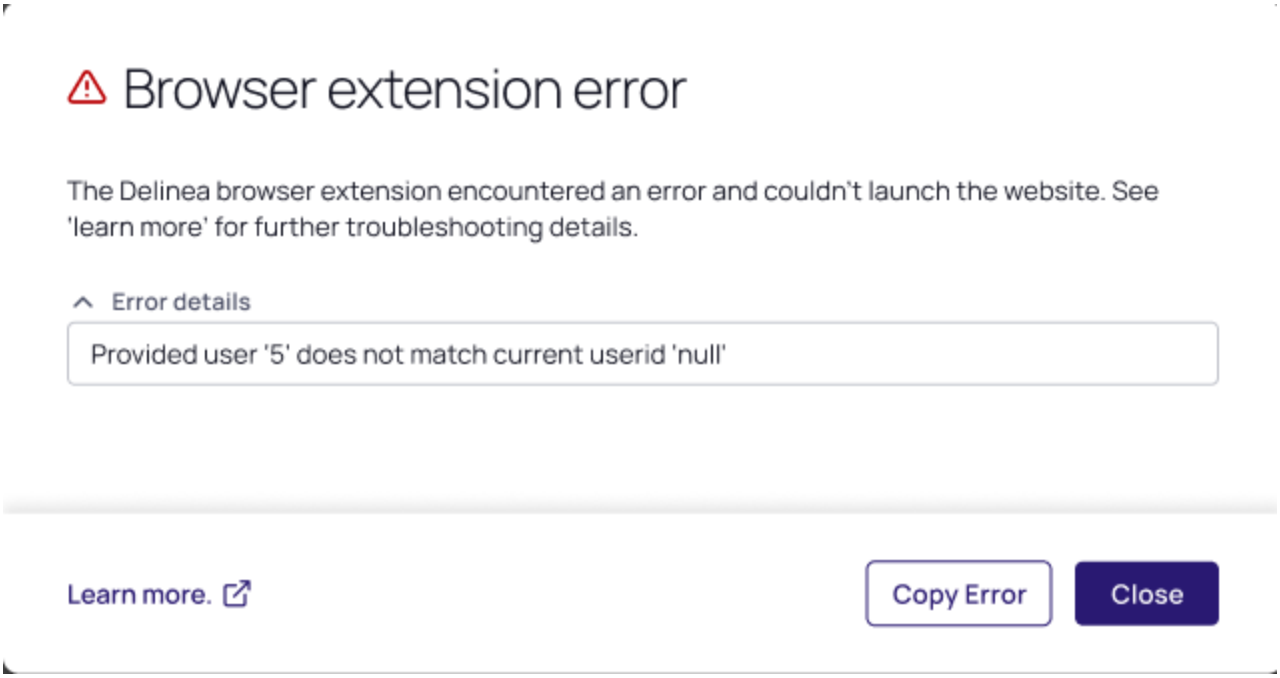
1. **Error msg:** Browser extension not found



Solution: Connection Manager was not able to identify a browser with the Delinea browser extension installed and active. Make sure that the first browser you open after activating the web launcher has the Delinea browser extension installed and you are signed in.

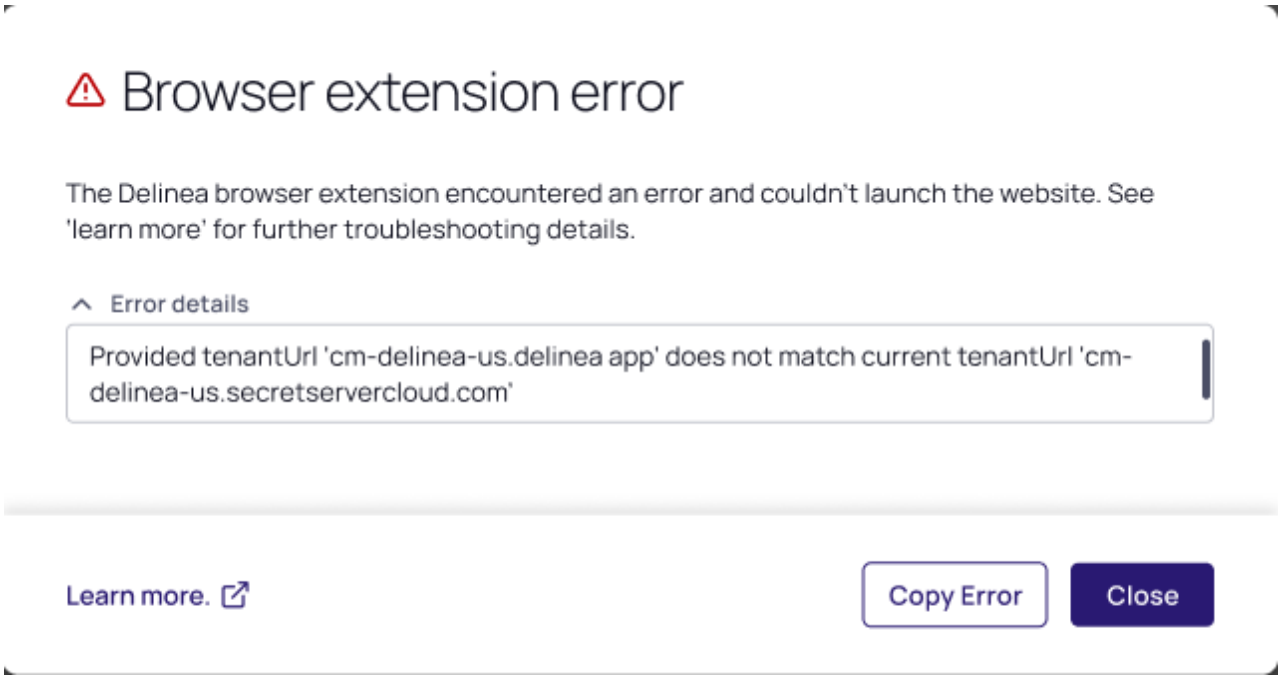
> **Note:** If you implemented a Native Messaging block list, you need to create an exception within the allow list specifically for Connection Manager [com.delinea.cm.message_host].

2. **Error msg:** Browser extension error



Solution: Check to make you are logged into the Delinea browser extension with the same username as you used to connect to a Delinea vault.

3. **Error msg:** Browser extension error



Solution: Check to make sure that you are logged into both the Delinea browser extension and Connection Manager with the same tenant URL.

4. No connection between Connection Manager and the Delinea browser extension.

   Make sure that the `Delinea.ConnectionManager.WebPasswords.Win` process is in the Task Manager on Windows or Activity Monitor on MacOS. If this process is active:

   a. Reload/ Reactivate the Delinea browser extension.

   b. Relaunch the browser.

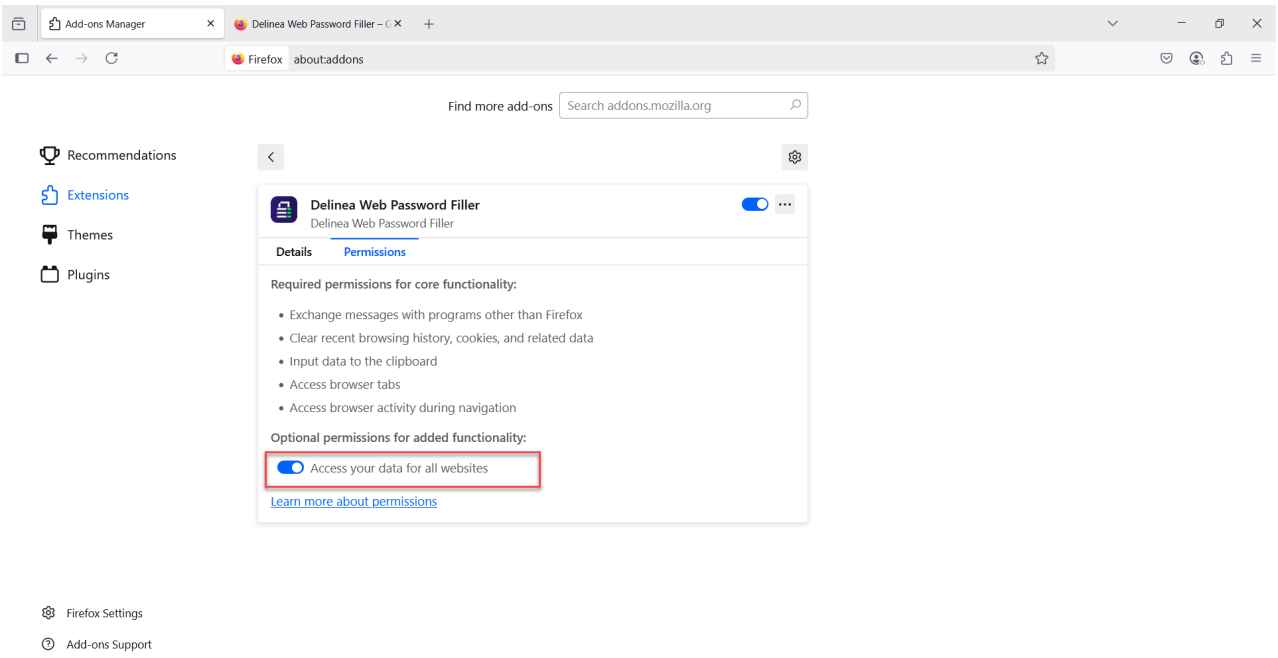
   If the process is not active, relaunch the Connection Manager installer and reinstall or repair Connection Manager.

5. The Delinea browser extension status is displayed incorrectly on Microsoft Edge.

   Due to Microsoft specifications, the `Delinea.ConnectionManager.WebPasswords.Win` process may continue to run on Edge after the browser was closed. If this is the case, open Task Manager and terminate the Edge browser process.

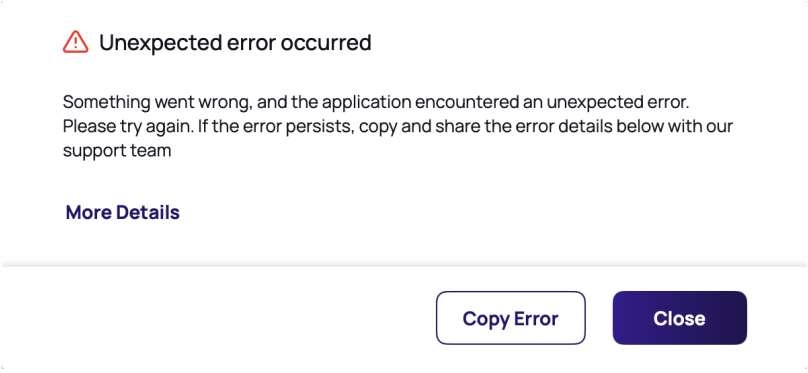
6. The Delinea browser extension fails to launch valid vault URL

   Check to make sure that the *Access your data for all websites* toggle is enabled in the Delinea browser extension permission settings.

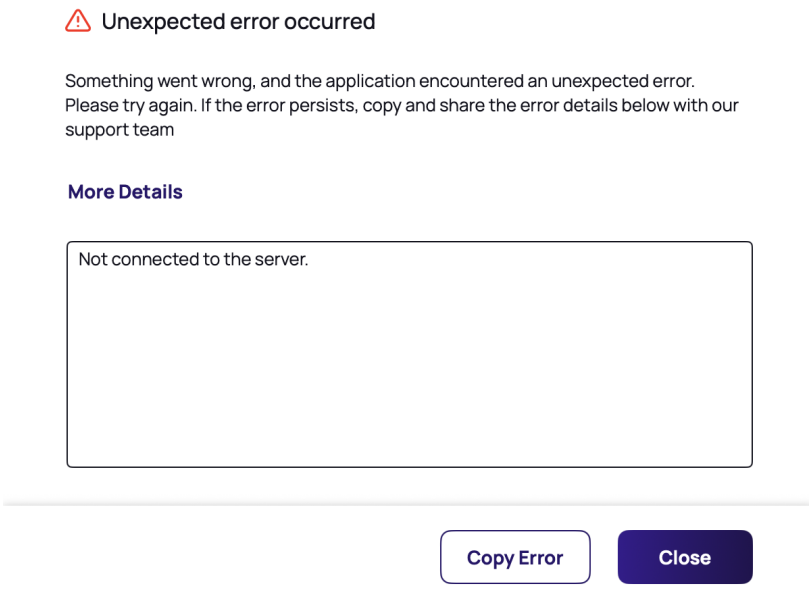


Troubleshooting Unhandled Errors

In the event that Connection Manager encounters an unhandled error, Connection Manager will display the following error message:



You can view additional information about the error by clicking More Details:



You will be able to copy this information and share it with Delinea support, if needed.

Downgrading to an Older Version of Connection Manager

Older versions of the Connection Manager installer are unable to downgrade through the installer UI. As such, users wishing to downgrade need to manually uninstall the application prior to installing the new application version.

In addition, users using Delinea Vault Connections, Local Connections, and Custom Settings require additional steps to ensure a smoother downgrade experience.

Delinea Vault Connections

When downgrading to an older version of Connection Manager with connections from a Delinea Vault, please authenticate to the vault to retrieve the connections.

Note: Delinea Vault credentials will need to be readded to access these connections.

Local Connections

When downgrading with local connections, first export the local connections as JSON using the steps included in "Exporting Connections" on page 96.

Important: Please ensure to keep this file in a secure location as credentials are not encrypted.

Next, implement the Connection Manager downgrade and reimport the local connections using the steps from "Importing JSON Files" on page 96.

Custom Settings

While the "Application Configuration File" on page 176 must be readjusted for each version change, "User Configuration File for Windows" on page 183 can be manually copied and work as expected.

Fixing the .DAT File Location After Upgrading on macOS

These instructions explain how to fix the .DAT file location after upgrading Delinea Connection Manager on macOS. This resolves an issue where Connection Manager occasionally saves session files in the incorrect folder, resulting in the loss of local connections.

Expected File Location

After upgrading Connection Manager, local connection files may occasionally save in an **incorrect** location, such as:

/Users/$USER/Documents/Library/Application Support/Delinea/Connection Manager/ConnectionManager.dat

The **expected** location for local connections is:

/Users/$USER/Library/Application Support/Delinea/Connection Manager/ConnectionManager.dat

Possible Solutions

Solution 1: Move the File Manually to the Correct Location (Recommended)

1. Close Connection Manager.
2. Move all files stored in incorrect local connection file directory by the executing the following command in the terminal:

```
rsync -r “/Users/$USER/Documents/Library/Application Support/Delinea/Connection
Manager/“ “Users/$USER/Library/Application Support/Delinea/”
```

3. Execute the following command in the terminal to change the local connection file directory:

```
defaults write com.Delinea.ConnectionManager Env.DataLocation
“/Users/$USER/Library/Application Support/Delinea/Connection Manager”
```

Solution 2: Reinstalling Connection Manager (Not Recommended)

Note: This solution is not recommended as all local connections, Delinea vaults, and custom configurations will be lost.

1. Uninstall Connection Manager.
2. Remove preferences file by running the following command:

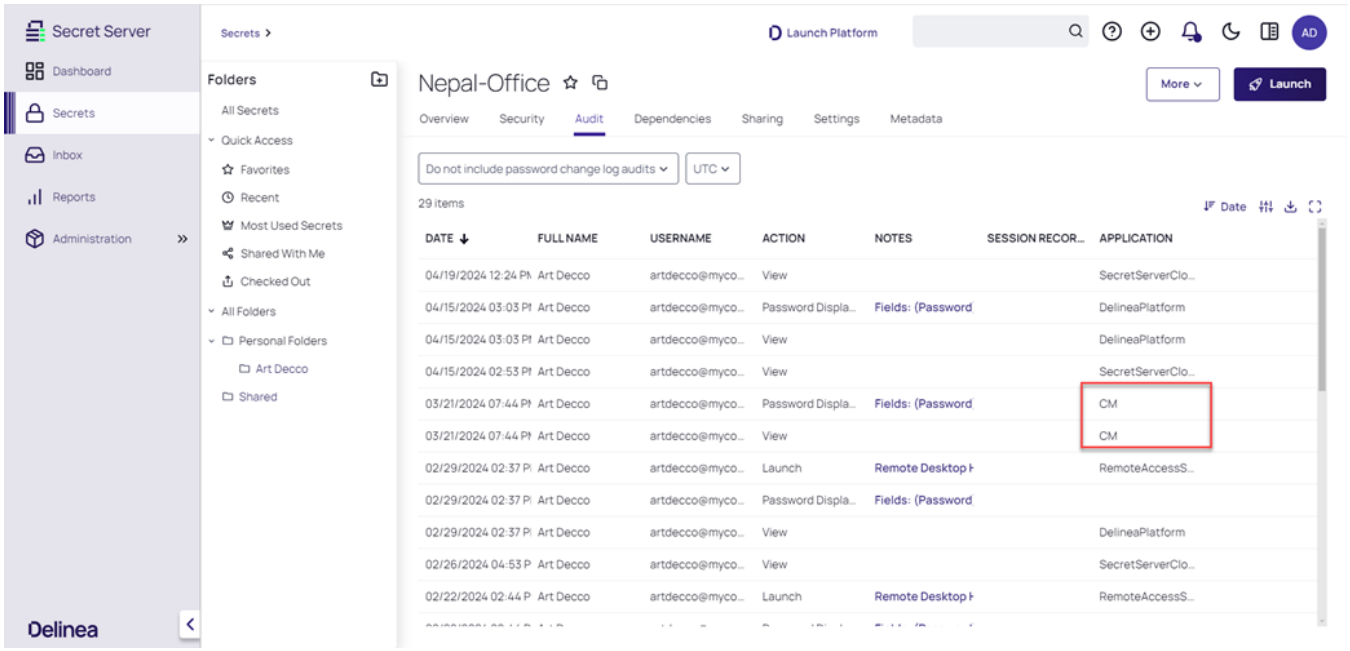
```
plist '/Users/$USER/Library/Preferences/com.Delinea.ConnectionManager.plist'
```

3. Remove the incorrect local connection file directory located at:
   /Users/$USER/Documents/Library/Application Support/Delinea/Connection Manager/
4. Reinstall Connection Manager.
5. Launch Connection Manager and choose the correct local connection file directory location at:
   /Users/$USER/Library/Application Support/Delinea/Connection Manager/ConnectionManager.dat

Troubleshooting Auditing Issues

Password Displayed Events Occurring in the Audit Log or System Log

If a user accesses a secret or launches a session via Connection Manager, a password displayed event may be triggered in the audit log or system log even if the password was not displayed. To prevent this from occurring, administrators need to filter their report by the *Application* column and remove all rows that contain "CM" or "Connection Manager".

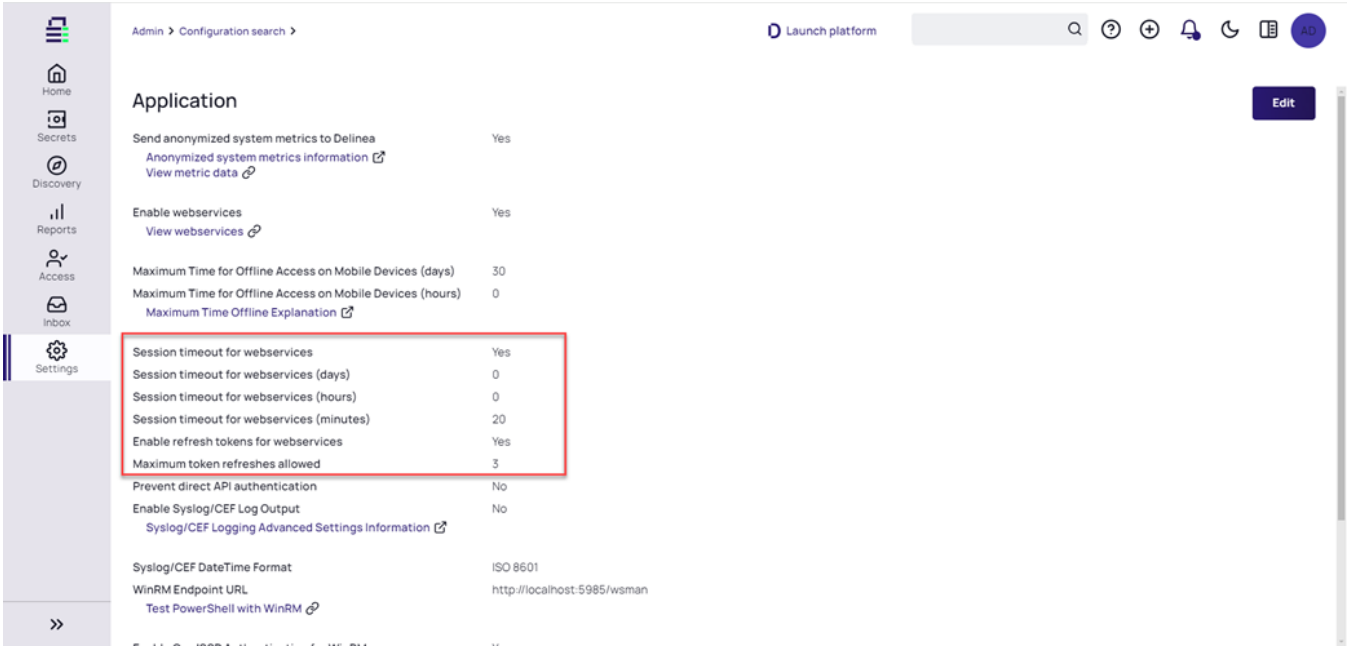


Vault Authentication Issues

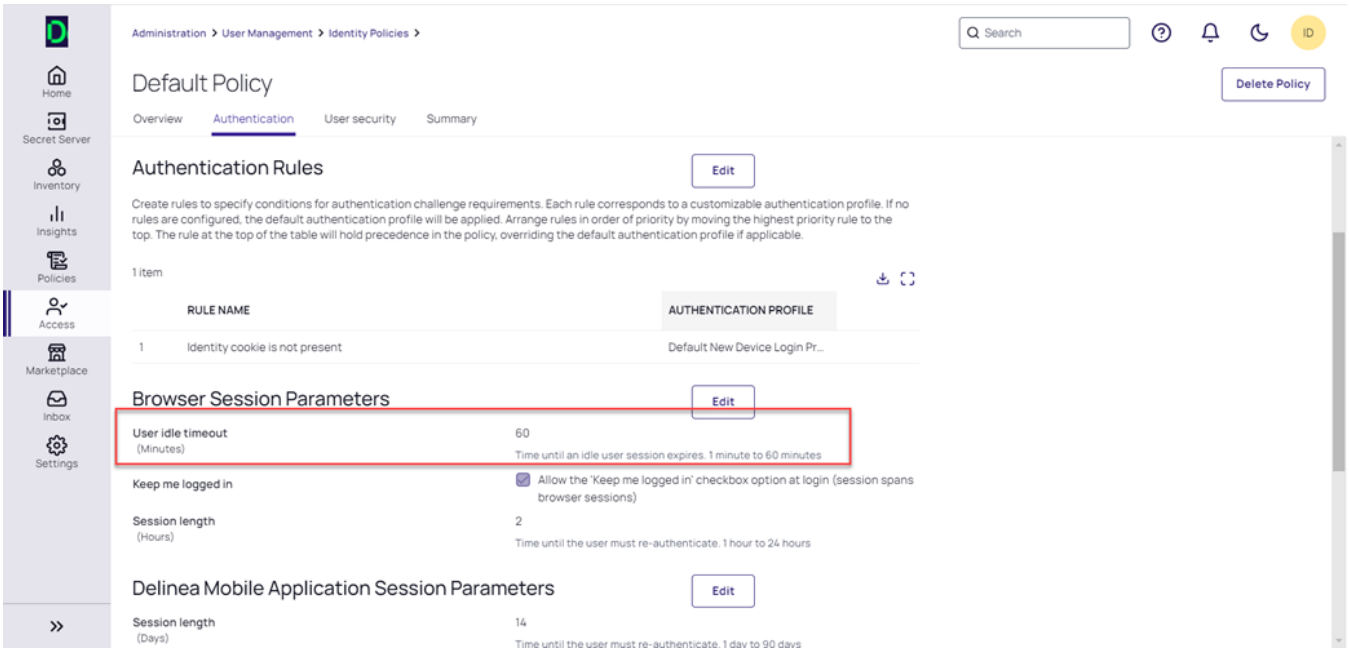
Troubleshooting Vault Authentication Timeout

If your session times out prematurely, be sure to check the corresponding settings in both Secret Server and the Delinea Platform.In Secret Server, you need to check the following settings:

- **Session Timeout for Webservices** - Set a Session time limit on Webservices API. Once Webservices expires, the user must log in again with their username and password.
- **Enable Refresh Tokens for Webservices** - Tell OAuth2 to send back a refresh token during Authentication. This token will allow the user to get a new access token without having to enter credentials.
- **Maximum token refreshes allowed** - Set the maximum amount of times a user can refresh an access token.



Inside the Delinea Platform, **Administration > User Management > Identity Policies** and check the **User Idle Timeout** setting:



To learn more about Connection Manager's Auto Reauthenticate parameter, please see "Enabling/Disabling Auto Reauthenticate " on page 178.

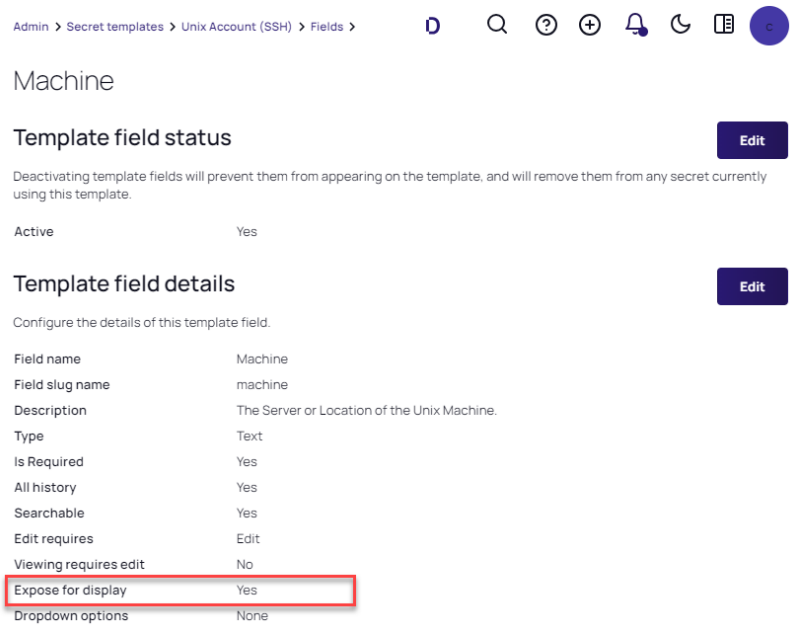
DPI Scaling Issues

Delinea recommends using a maximum of 125% scaling when running Connection Manager on full HD (1920x1080) monitors. If this scaling limit is exceeded, the Connection Manager application window size will exceed the display resolution size of your monitor.

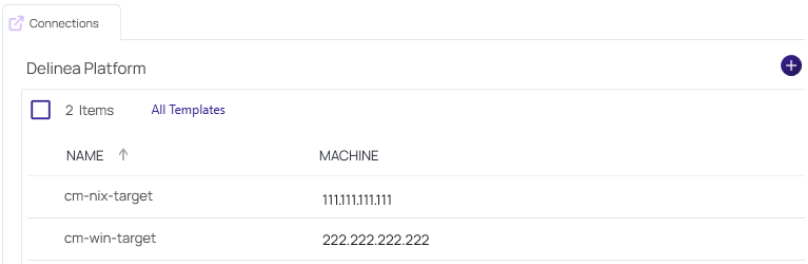
Display Column Issues

The *Machine* Field is Not Visible in the Connection Manager Grid View

Out of the box, all Machine fields are encrypted and, therefore, can only be seen in a grid if customers adjust the Field on the Secret Server template to "Exposed for display." This unencrypts the field and allows it to show in grids without a permission check.



The Machine field is now visible:



Note: When you change *Expose for display* to **Yes**, there could be a short delay from background processing before all data populates.

Troubleshooting SSH Connections

If you are having issues connecting to the target host via SSH, the issue could be incorrect authentication method setup on the target host. This can be fixed by changing the "PreferredAuthentications" key in the Application Configuration file, which contains a list of preferred authentication methods.

The default values are "gssapi-with-mic,hostbased,keyboard-interactive,publickey,password" (gssapi-with-mic and hostbased are not currently supported and are included for future updates). Removing or reordering methods in this list can resolve connection issue. Possible solutions include:

- Placing the password before other methods such as: "gssapi-with-mic,hostbased,password,keyboard-interactive,publickey"
- Removing other methods completely such as: "gssapi-with-mic,hostbased,password"

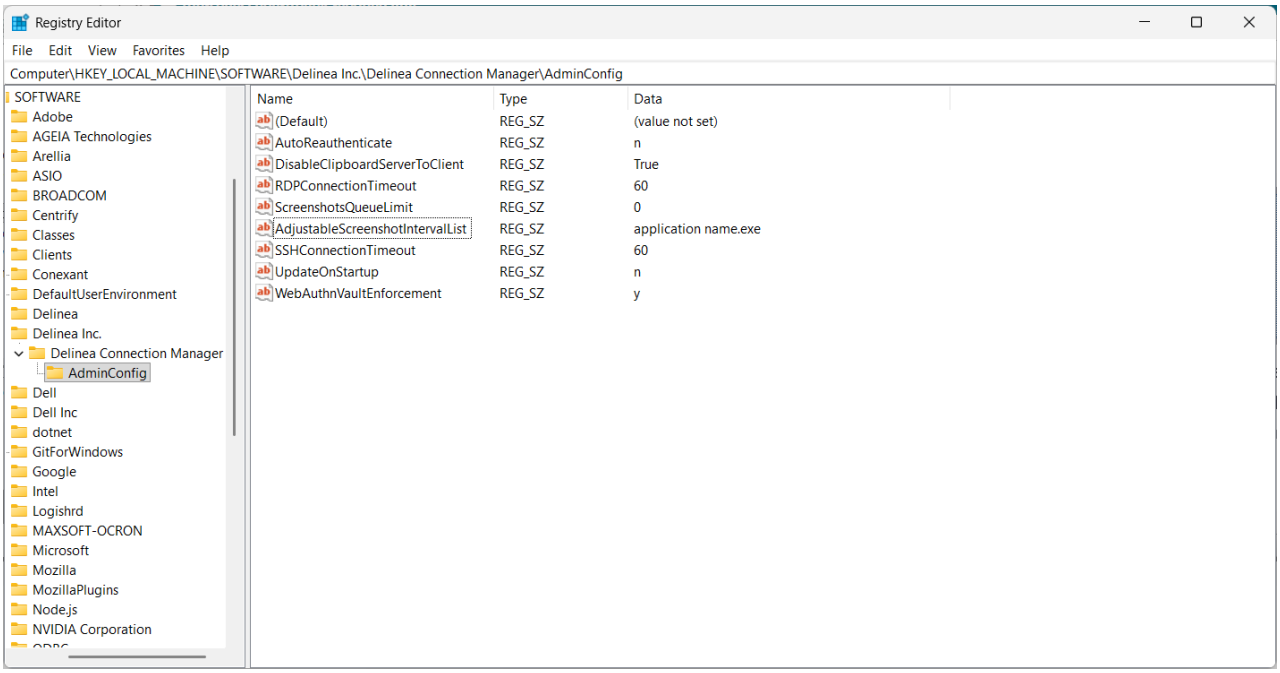
Please note that these settings affect all the SSH hosts connected through Connection Manager. Therefore, removing an authentication method (for example "publickey") will make all hosts with the "publickey" access-only method unreachable.

Troubleshooting RDP Connections

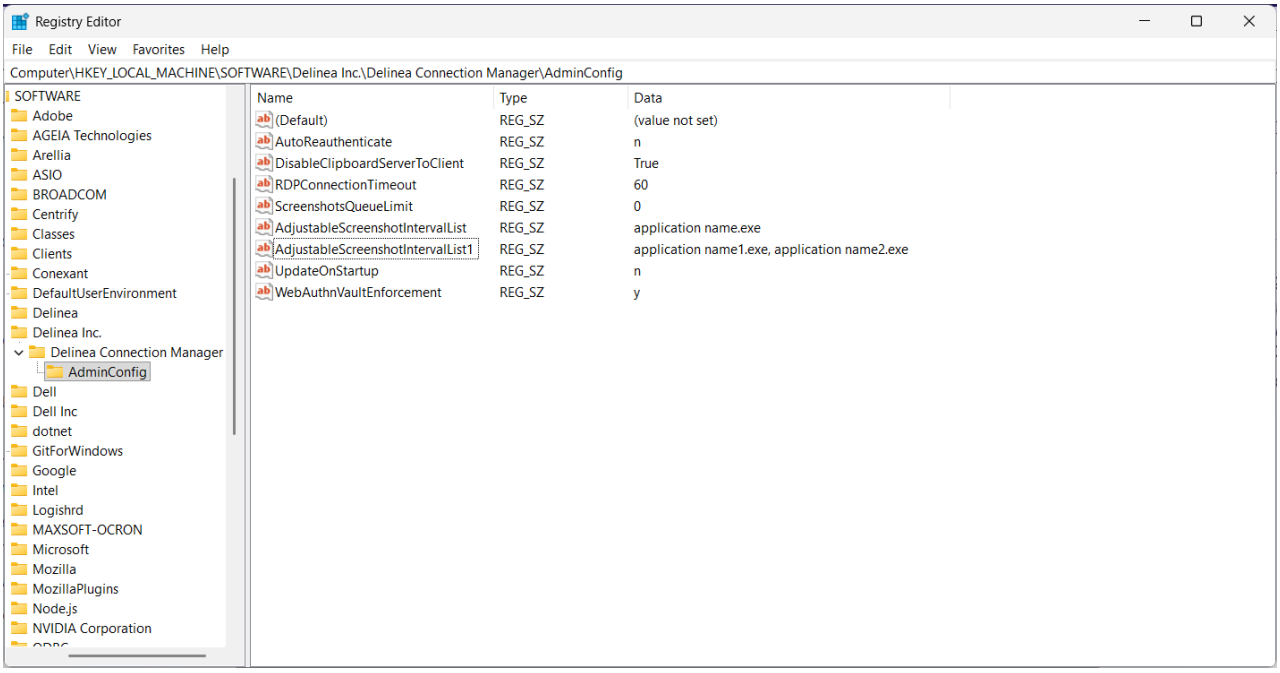
Resolving Flickering Issues in MECM and SCVMM Consoles Launched via Connection Manager

If you notice flickering in the Configuration Manager Console and Virtual Machine Manager Console (MECM or SCVMM), you can resolve the issue by the following the steps below:

1. Open the Registry Editor.
2. Add the following parameter after the *ScreenShotQueueLimit* parameter:



Note: The application name needs to be the same as in the MECM or SCVMM launcher. If you are using two or more applications, you need to write the application names separated by commas, as shown in the example below:



3. Open the application(s) to see if the flickering still exists.

Dragging Credentials from an External Password Manager

Dragging credentials from an external password manager into Connection Manager is not supported and may close the session unexpectedly. Instead, copy and paste or type the credentials directly into Connection Manager.

RDP Connection Timeout Issues

If you are experiencing connection timeout issues when using a VPN, firewall or any other software that negatively impacts the network speed, try increasing the SSH Inactivity Timeout setting in the Application Configuration File. See "Configuring RDP Connection Timeout Over TCP" on page 166 for more information.

Troubleshooting Proxies

To troubleshoot issues with proxies, start by Enabling Debug Mode in the DE Log Files inside Secret Server. In addition to the DE logs, users can see the IP address of the distributed engine they have connected to in order to help troubleshoot issues.

Issues With the Clipboard Functionality

Access to clipboard allows a user to copy and paste to/from the client machine's clipboard to the remote machine during launched RDP sessions. It may be set on three different locations:

- User Preferences

  This will be applicable to the logged in user only and all secrets that the user has access to.

  1. Log in to Secret Server.
  2. Click the profile icon, then select User Preferences.
  3. On the Settings tab, toggle the button to the right of Allow Access to Clipboard.

- Secret

  This will be applicable to the logged in user only and the secret that it was configured on.

  1. Access the secret.
  2. On the Settings tab, click Edit next to RDP Launcher.
  3. Enable the Allow Access to Clipboard setting.
  4. Click Save.

     Note: Secret Owners have an additional option to enforce the Secret level RDP settings for all users.

- Secret Policy

  This will be applicable to all the users that have access to the secret, as well as the secret/s and folder/s that the policy is assigned to.

  1. Access the secret policy.
  2. On the Policy page, click on the Launcher tab.

3. Click Edit.
4. Set Enforce RDP Settings for All Users to Yes.
5. Enable the Allow Access to Clipboard setting.
6. Click Save.

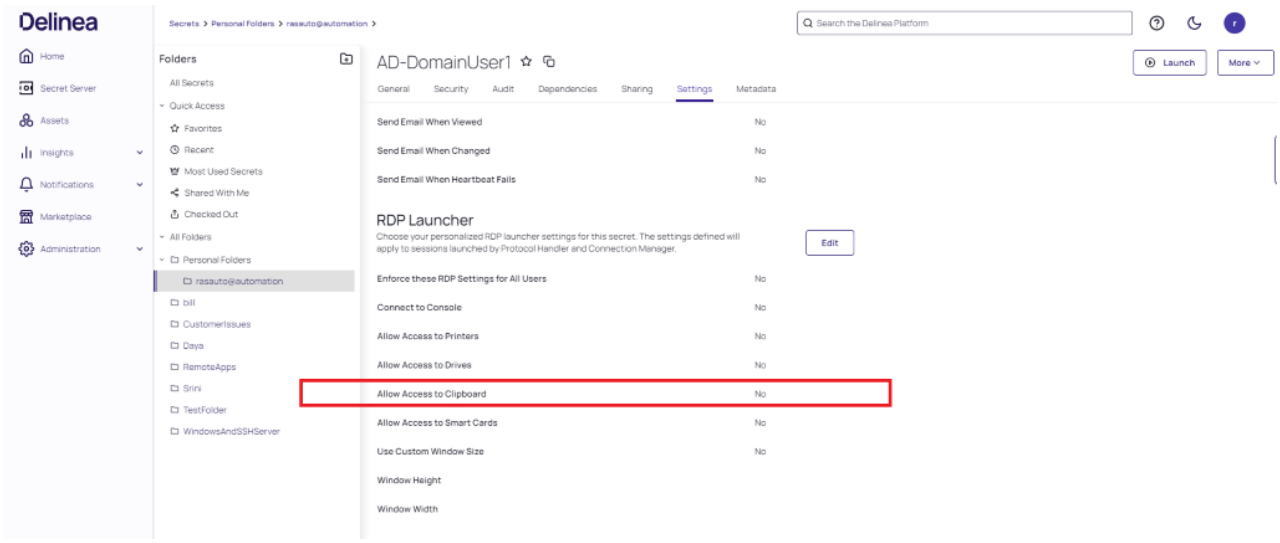
Important: Access to the clipboard must also be allowed in the machine's security policy. The above instructions also apply to the following RDP settings:

- Connect to console
- Allow access to printers
- Allow access to drives
- Allow access to smart cards
- Use custom Window Size

Troubleshooting

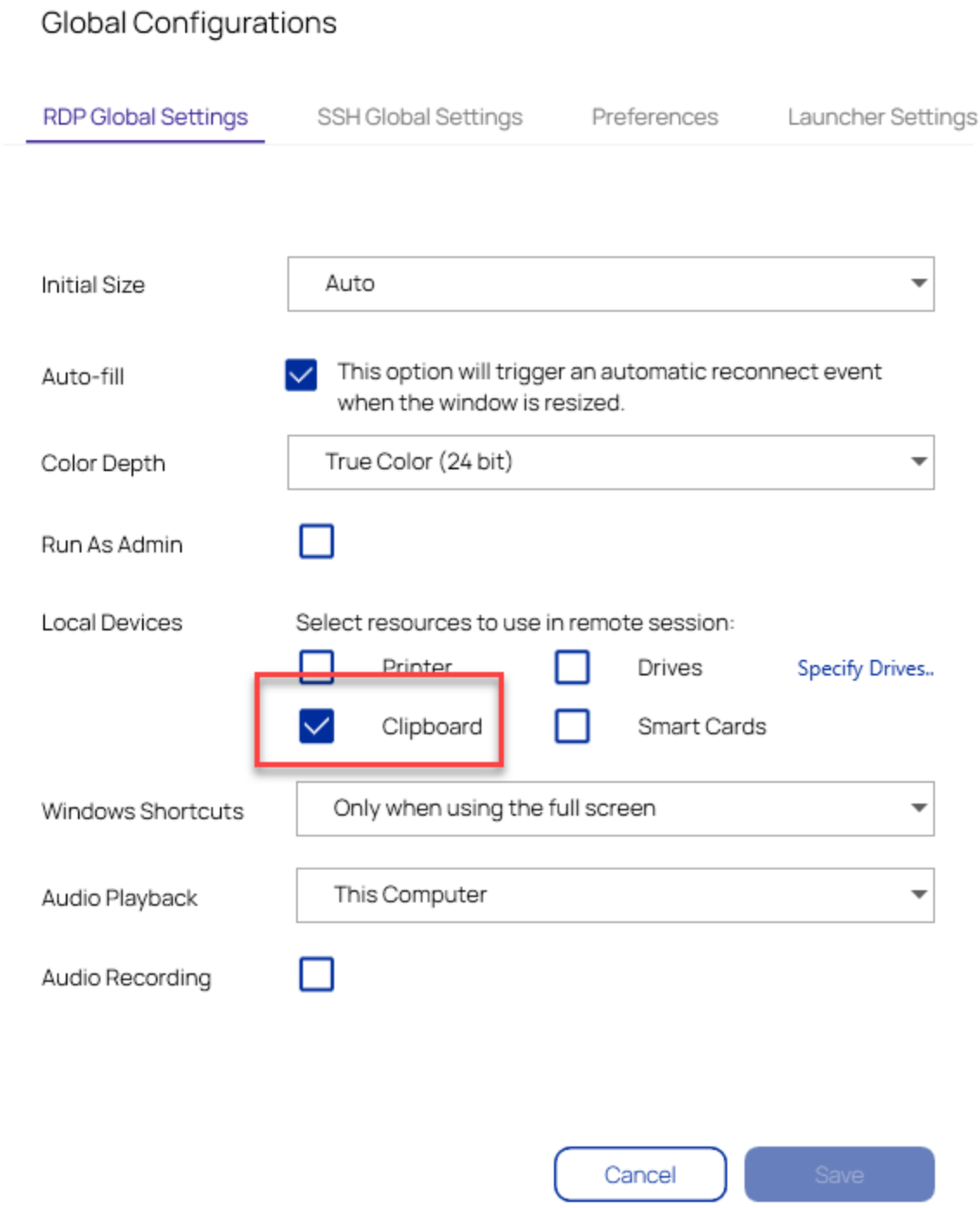
If you are experiencing issues with the clipboard functionality (copy/paste), please try the following:

1. Check if clipboad access is enabled on the secret



Note: If you are mapping a local connection to a secret, make sure the clipboard functionality is also enabled on the secret.

2. Make sure the clipboard functionality is enabled for RDP.



AVBlock Error with Session Recording

Connection Manager utilizes a third-party library for video encoding known as AVBlocks. This library performs a license check through the URL `lms.primosoftware.com`.

Note: This is a third-party check for licensing.

The license is checked infrequently and cached in the `username\local\temp\primosoftware.lm.cache` folder on Windows. If the license check fails, Connection Manager will be unable to record a session and provide an error message, although all other functionalities will continue to operate normally.

Note: Connection Manager's AVBlock license was recently extended.

`Thycotic.Video.AVBlocks.Common.AvBlocksException`

To facilitate this process, we recommend open network access via port 80 (HTTP) and 443 (HTTPS). If it is not possible to keep the ports open continuously, please use allow port 80 and 443 access to primosoftware.com and its subdomains through DNS filtering or other appropriate mechanism depending on your company policies for client machines.

In some cases, Connection Manager may cache and invalid license on the client machine. In this case, we recommend deleting the contents of the cache folder for all affected users.

In Connection Manager when attempting to launch a Secret Server Secret that has session recording enabled, the session may fail to launch and return an exception error in the logs.

Examples of these error exceptions:

- ERROR Delinea.ConnectionManager.Core.ViewModels.ExplorerViewModel: Unhandled exception in Connect: Autofac.Core.DependencyResolutionException: An exception was thrown while activating Delinea.ConnectionManager.SecretServer.SecretServerSessionBackgroundWork.
- ERROR Delinea.ConnectionManager.Core.Managers.ErrorProcessingManager: Show error to user: An exception was thrown while activating Delinea.ConnectionManager.SecretServer.SecretServerSessionBackgroundWork.

Problem

This is caused when a component that Connection Manager uses for session recording starts caching an invalid license for that component on the client machine. The invalid license causes an rdpwin.exe error for the recorded session when it launches, resulting in the error messages as shown in the examples above.

AVBlocks can call home to a licensing server, here `https://lms.primosoftware.com/`, from the client endpoint where the Protocol Handler is installed and it creates a local cache of the licence in `%temp%\primosoftware.lm.cache`.

If the access to the license server is then blocked, the cached license will eventually expire and cause a PH recording error:

```
Failed to open transcoder: Error=Unlicensed feature Facility=AVBlocks, Code=9, Hint=vp8-
enc;
```

This can be seen in 6.0.0.13 and newer logs with verbose logging enabled in `C:\Program Files\Thycotic Software Ltd\Secret Server Protocol Handler\log4net-rdp.xml`.

Workaround

1. Re-enable access to https://lms.primosoftware.com/.
2. Delete the contents of `%temp%\primosoftware.lm.cache` for all affected users.

CM Crashing When Offline and Checking Certificates

Issue

If a Connection Manager end user is using untrusted certificates in their environment while they are offline, CM will try to reach out to an MS DNS to confirm the certificate. This happens even after a DNS sinkhole is set on that domain through the host file. But because there is no outbound internet connection, CM pauses while waiting indefinitely for a confirmation that will never come, eventually freezing and crashing.

Resolution

To resolve this issue, edit the local group policy using the information in the article, An Automatic Updater of Untrusted Certificates for Windows.

Encryption

- Encryption for CM login:
  - 256-bit encryption > AES 256. To check its integrity, we use HMAC + AES 256

General

What are the default locations for the Connection Manager application and log files?

Windows, application file: `C:\Program Files\Delinea Software Ltd\Delinea Connection Manager on Windows`

Windows, log file: `C:\Users\Appdata\Roaming\Delinea\Connection Manager`

macOS, application file: `Applications/delinea/Connection Manager.app`

macOS, log file: `users/<username>/library/application support/delinea/Connection Manager`

Is there a local session timeout for sessions within Connection Manager (CM)?

Yes. - For Local Connections, the Windows default socket connect timeout applies (e.g. standard RDP/SSH remote session timeout). The session timeouts on secrets can be set in Secret Server (SS).

I'm seeing a Connection failed error message while trying to connect to SS

`Connection failed reason: Request to Secret Server failed. Internal server error. An error has occurred.` Seeing this error upon connection to SS means the currently installed version of SS is lower than 10.7.

Is there a way to refresh the SS connections?

Yes. - The Secret Server connection got a refresh button with the 1.2.0 version update.

Where and how is the data for Connection Manager stored?

A Connection Manager data file containing the list of connections is stored in `C:\Users\\AppData\Roaming\Delinea\Connection Manager`. The file is stored using AES 256 (256-bit) encryption.

Is there a way to push scripted code out to multiple SSH sessions at one time for updates or commands?

Is there a way to send a scripted file out to multiple PuTTY sessions at once using commands?

There is currently no support to run this type of action from Connection Manager. This is sometimes done with X11, but we do not currently support that connection type. There is a Feature Request in the backlog to add support.

What happens if the SS Heartbeat fails?

Connection Manager does monitor Secret Server heartbeat. If an active RDP/SSH session detects a heartbeat failure the session will be closed automatically.

Is there any current performance data for Connection Manager? Including: general memory, amount of space needed, number of open connections that can be made at one tie, etc.

We are getting more information. Currently we have tested with up to 30 open connections. Some of the performance numbers will depend on the system hardware for the machine that is running Connection Manager.

While recording a session, if a user isn't on tab, what's the behavior? Do we reduce what we record and send? Or does it stay the same? How can we tell if it's the "focus"?

We follow the same behavior as the Secret Server session recording. If a user is not on the Tab, then we record and send less information.

Note: For Connection Manager versions 1.7 and older, the directory names will use *Thycotic* instead of *Delinea*

Host Names

We follow these general naming conventions and constraints:

https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

An underscore "_" in the host name is not currently supported. The underscore has a special role, as it is permitted for the first character in SRV records by RFC definition, but newer DNS servers may also allow it anywhere in a name. For more details, see: http://technet.microsoft.com/en-us/library/cc959336.aspx

Licenses

Does a Current Customer Drop in the Platinum Trial License Key Into Their Current Secret Server Instance to Receive the Connection Manager Feature?

Yes, if the platinum trial license was created recently.

Does it Matter, if Connection Manager is Working With a Different Secret Server Instance Than the One Aligned With the Trial Key?

Connection Manager can connect to any Secret Server instance that is licensed with the Connection Manager Add-on license for Secret Server.

Is it Okay to Add a Trial License to a Production Server? Will it Overwrite or Add to the Current License?

It should add and run alongside the current license. While the Trial is active, they will have access to Secret Server Platinum level features, but once the trial expires, they will revert to their existing license.

Are There Any License Restrictions to connection-manager?

If users do not have a license, they may see the following message when connecting - "connection-manager is currently not licensed for secret-server. You may still download it to test with locally stored connections.

Manually Cleaning the Connection Manager File System

> Use the following procedures only after you have uninstalled connection-manager according your operating system's procedures.

To manually clean up the Connection Manager file system, you need to remove files and folders specified below, and then clear Registry entries specified below.

Instructions for Windows Users

Remove files and folders

Remove the specified files and folders at the following paths:

- C:\Users\UserName\AppData\Roaming\Delinea

  (folder **Delinea** must be deleted)
- C:\Users\UserName\AppData\Local\Delinea_Inc

  (folder **Delinea_Inc** must be deleted)
- C:\Program Files\Delinea

  (folder **Delinea Software Ltd** must be deleted)

- C:\ProgramData\Delinea\

  (Delete this folder entirely)

Clear entries from the Registry

Clear entries from the registry as specified below:

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\sslauncher
- HKEY_CURRENT_USER\Software\Delinea
- HKEY_LOCAL_MACHINE\SOFTWARE\Delinea Inc
- HKEY_CURRENT_USER\Software\Classes\sslauncher
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version Vector
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version Vector

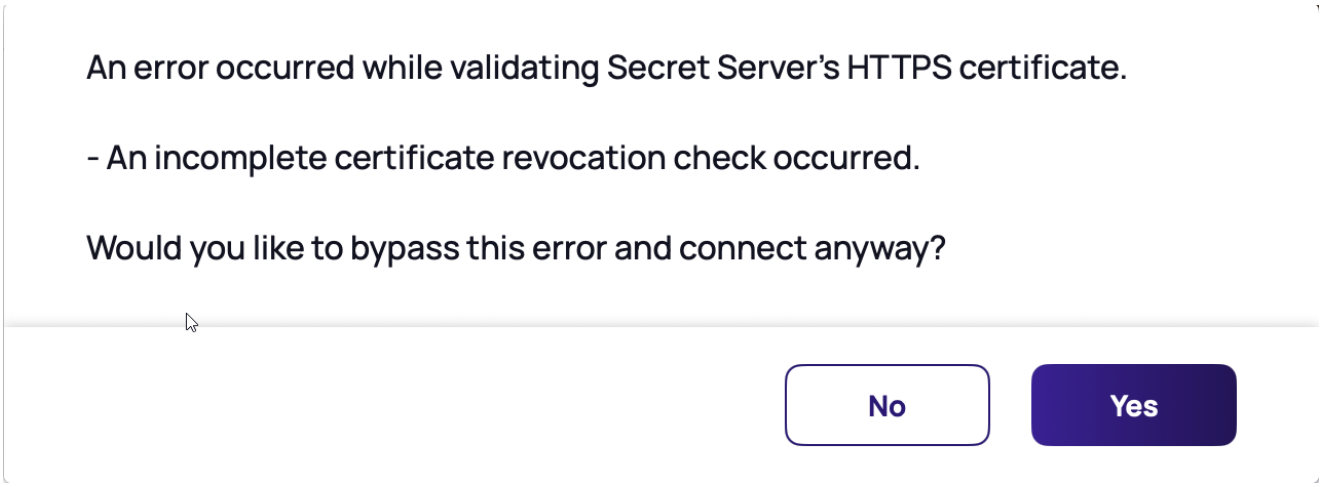
In addition, run regedit, search for and remove all registry keys that contain "delinea" as part of a key name.

Instructions for macOS Users

- Delete /Applications/Delinea/ directory (which holds the Delinea Connection Manager and ProtocolHandler apps)
- Delete /Users/<userID>/Library/Application Support/Delinea/ directory (which holds user settings.dat, logs, and ConnectionManger.dat)
- If you want to save your Local Connections, you will want to copy the ConnectionManager.dat elsewhere before deleting the directory above
- If you want to save your Global Configuration settings, you will want to copy the Settings.dat elsewhere before deleting the directory above
- Open Terminal and run the command (this should delete install receipts, typically MDM's check against install receipts before they push a required package. If that is the case, as it is here, the MDM will see the application still installed and won't push):
- sudo pkgutil --forget com.Delinea.ConnectionManager
- Delete /Users/<userID>/Library/Preferences/com.Delinea.ConnectionManager.plist

Troubleshooting MacOS Certificate Errors

If Connection Manager is displaying a MacOS the following "Incomplete certificate revocation check occurred" error, it means that Connection Manager was not able to validate the Secret Server SSL certificate by a certificate authority.



This issue might have multiple root causes. Consider all of the possible causes below and follow the troubleshooting steps in each section.

Disable Certificate Revocation Check

Run the following command in the terminal:

```
defaults write com.Delinea.ConnectionManager Url.CertificateRevocationListCheck -bool
false
```

Note: Since MacOS does not always properly handle certificate revocation checks after OSCP deprecation, disabling CRL checks is the best workaround. Learn more about OSCP deprecation.

Secret Server Certificate Validation Fails When Using OCSP

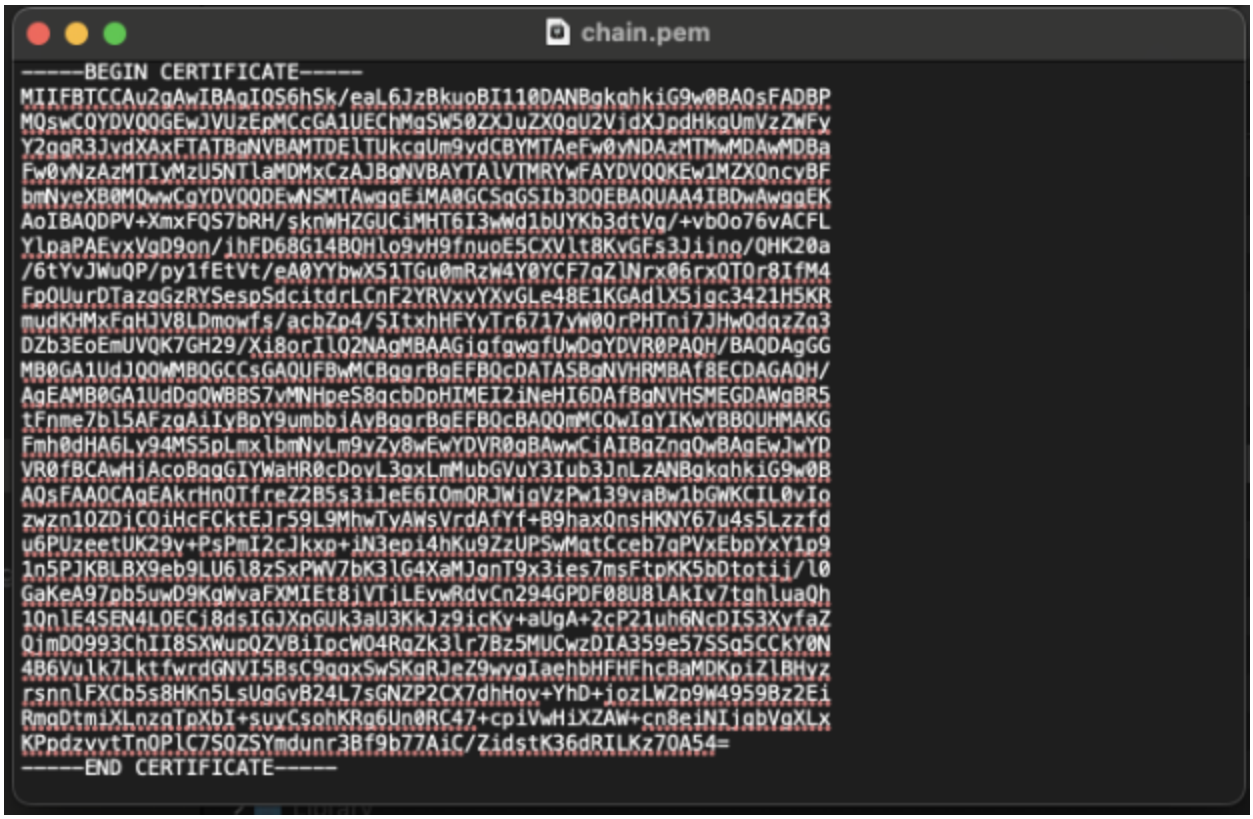
Note: Only check this if the OCSP Responder URI is present in the certificate.

1. Open in this Terminal app and cd to folder that contain `certificate.pem` from previous step.
2. Assign SSURL variable to Secret Server Host.
3. Get an Intermediate Certificate. To view the list of intermediate certs, use the following command:

   ```
   openssl s_client -showcerts -connect $SSURL:443 < /dev/null 2>&1 |  sed -n '/-----
   BEGIN/,/-----END/p'
   ```

   The very first certificate is the server certificate you saved in previous step. For all the certificates below, they will be copied and saved to a file called `chain.pem`.

   Example `chain.pem` file (Can be opened with the Text Edit application):



4. Get the OCSP Responder URL for the server certificate:

   ```
   OCSPURL=$(openssl x509 -noout -ocsp_uri -in certificate.pem)

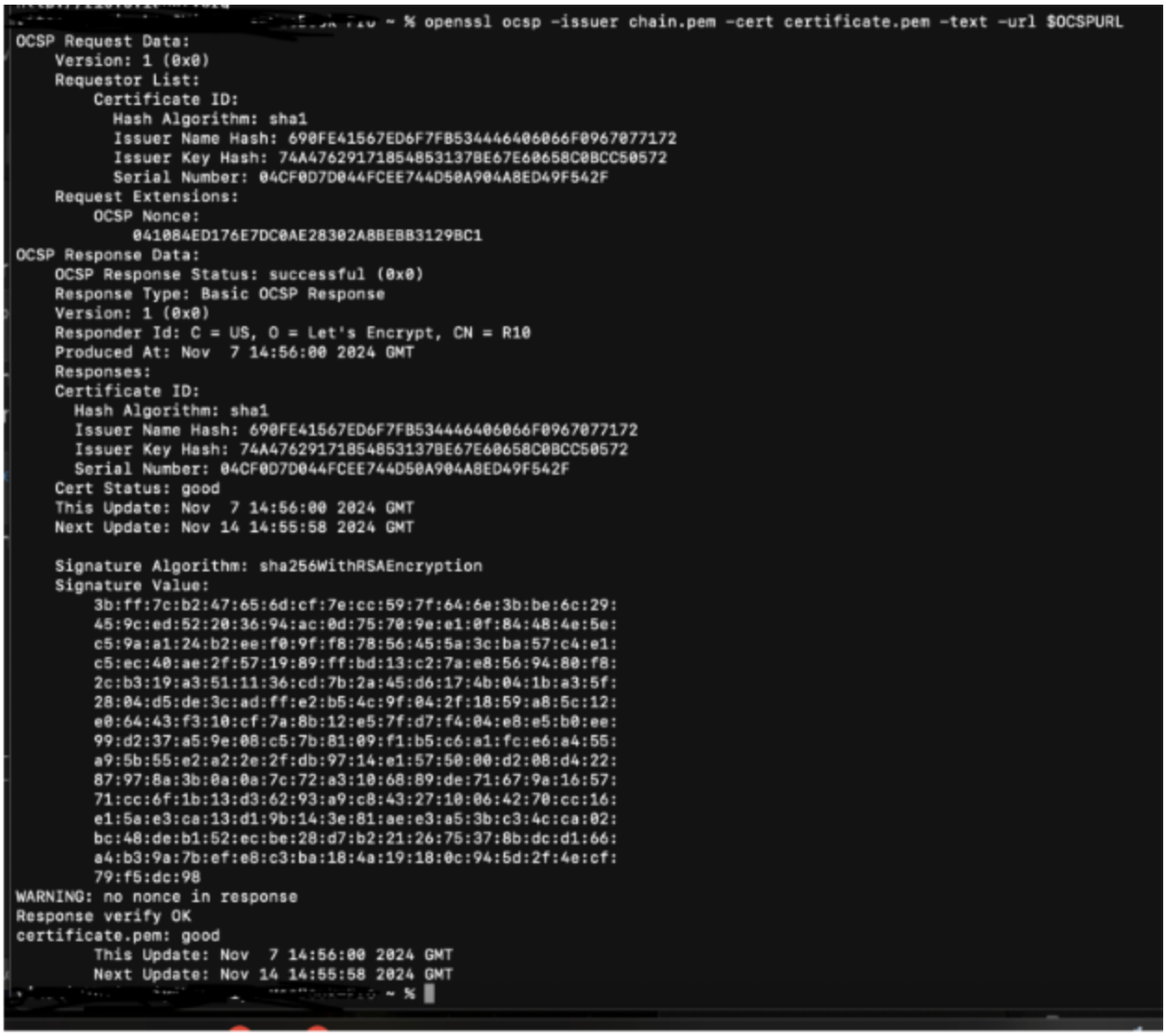
   echo $OCSPURL
   ```

   Make sure the SSURL displays the OCSP URL.

5. Make an OCSP validation request:

   ```
   openssl ocsp -issuer chain.pem -cert certificate.pem -text -url $OCSPURL
   ```

   Example output:



Make sure that **Cert Status: good** is displayed.

6. Save and provide output of previous command to DelineaSupport.

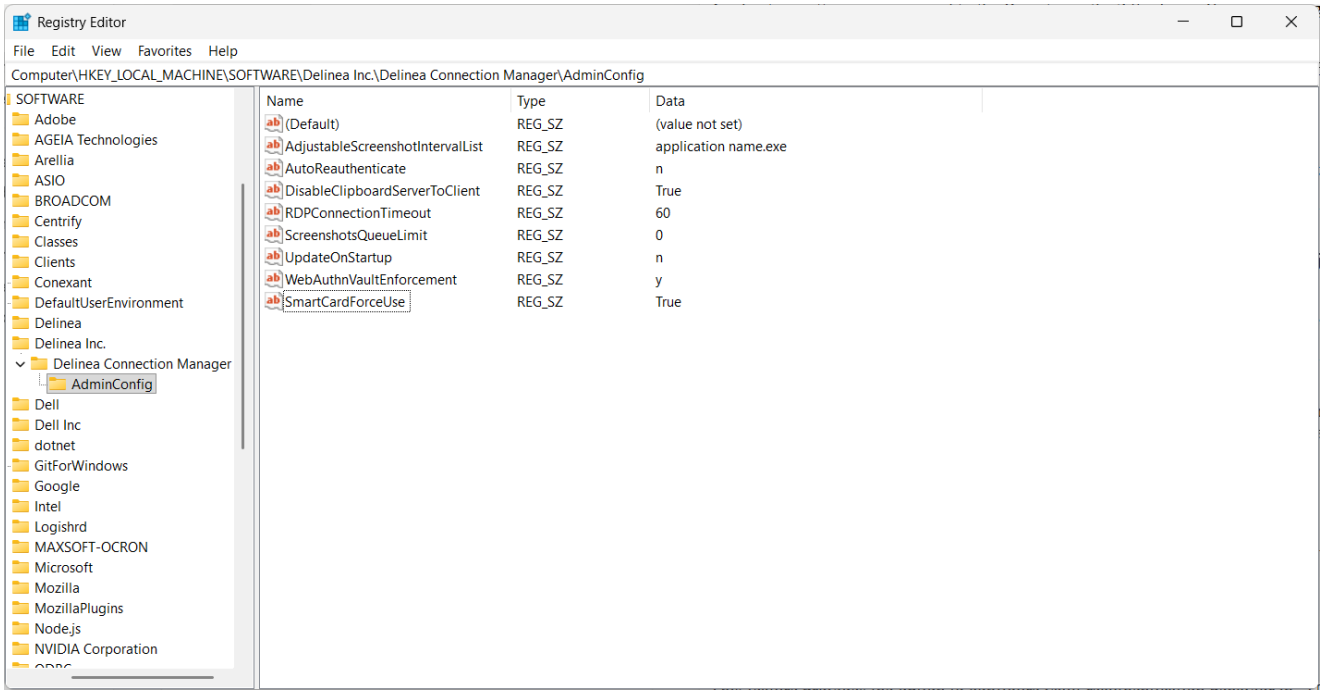
Incorrect Trust Policy in Root Certificate Authority

1. Open **Keychain Access -> Certificate**.
2. Find company Root Certificate issued by Markants. It will be either in Login or System Keychain.
3. If there is one, do a *Cmd+click* and go to **Get Info >Trust**.

Troubleshooting Issues With Smart Cards

Smart Card Force Use

If Connection Manager crashes when launching an RDP session for a user whose Active Directory account has **Smart card is required for interactive logon** enabled, create a new string value called `SmartCardForceUse` in the `AdminConfig` or `UserConfig` registry key and set the value to `True`.



Note: This setting applies to Windows only. Restart Connection Manager after editing the registry for the change to take effect.

Release Notes

Connection Manager Version Compatibility with Secret Server

Your Connection Manager version is compatible with any Secret Server version released within the 12 months preceding the Connection Manager release.

Release Notes History

The following Connection Manager release notes are available:

- "2.8.3 Release Notes" on page 229
- "2.8.0 Release Notes " on page 230

- "2.7.1 Release Notes " on page 232
- "2.7.0 Release Notes" on page 232
- "2.6.1 Release Notes " on page 233
- "2.6.0 Release Notes" on page 233
- "2.5.4 Release Notes" on page 235
- "2.5.3 Release Notes" on page 236
- "2.5.2 Release Notes " on page 237
- "2.5.1 Release Notes (Windows Only)" on page 238
- "2.5.0 Release Notes" on page 239
- "2.4.0 Release Notes " on page 240
- "2.3.1 Release Notes " on page 241
- "2.3.0 Release Notes " on page 242
- "2.2.0 Release Notes" on page 242
- "2.1.0 Release Notes" on page 243
- "2.0.1 Release Notes" on page 244
- 2.0.0 - Release Notes
- 1.9.7 - Release Notes
- 1.9.6 - Release Notes
- 1.9.5 - Release Notes
- 1.9.2 - Release Notes
- 1.8.0 - Release Notes
- 1.7.1 - Release Notes
- 1.7.0 - Release Notes

2.9.0 EA Release Notes

Date: July 9, 2026

Features

- Connection Manager now supports Session Connector-based launchers on MacOS.
- Connection Manager now supports Kerberos authentication.
- Connection Manager now supports Arm64 processors on MacOS.

Improvements

- Improved the bulk launch experience for secrets that require ticket-based approval. Bulk launch of MFA-protected secrets is not yet supported. [696555]
- Users are now notified with a "Vault access token expired" dialog when their RDP session is disconnected due to a web services session timeout. [669403]
- Connection Manager now hardens credential security by ensuring passwords and sensitive data are no longer exposed as plain text in memory dumps.

Windows Specific

- Improved the RDP Proxy Site dialog window selection for Proxy Site on Windows. [689490]
- Improved INFO level event logging. Sessions cancelled by the user are not logged as errors with full stack trace. [687701]
- Administrators can pre-seed trusted SSH host fingerprints so that end users are not prompted to accept an unknown host key. See "Pre-Trusting SSH Host Fingerprints" on page 175 for more information. [723914]
- Administrators can pre-approve or explicitly deny Secret Server URLs for the external launcher so that end users are not shown the URL approval dialog. See "Pre-Approving Secret Server URLs" on page 175 for more information.

MacOS Specific

- Customer can launch non-proxied RDP sessions on MacOS using AD accounts. [633747]
- Connection Manager now supports copying and pasting files within RDP sessions on MacOS. [684814]

Fixed Issues

- Fixed an issue where Connection Manager versions 2.8.0 and 2.8.3 would fail to launch and freeze after authentication. [730606]

Windows Specific

- Fixed an issue where Connection Manager would display a "Invalid Window handle" error message. [704230]
- Fixed an issue where session recording produced a blank/black screen when launching complex batch file launchers through Connection Manager. [707153]
- Fixed an issue where Connection Manager displayed a "The method or operation is not implemented" error when launching an RDP session using a "Map Secret" credential. [717855]
- Fixed an issue where session recording would fail with a "Process is not suitable for session recording" error. [721144]
- Fixed an issue where Connection Manager displayed a "Not enough quota is available to process this command" error when reconnecting an RDP session. [722872]

MacOS Specific

- Fixed instability issues when connecting with RDP on Connection Manager versions 2.8.0 and 2.8.3. [729266]
- Fixed an issue where mapped proxy RDP connections would close when pressing Ctrl + C & Command + C multiple times. [702256]
- Fixed an issue where Connection Manager would not connect to an AD user with an email for Windows Account secret. [705840]
- Fixed an issue where Connection Manager would display an XML error instead of updated prompt. [666279]
- Fixed an issue where Connection Manager exhibited unintended behavior when the system language was set to Latvian. [709409]
- Fixed an issue where Connection Manager would crash after performing a file transfer in an RDP session. [709814]
- Fixed an issue where Connection Manager versions 2.8.0 and 2.8.3 failed to connect via proxy when using an SSH tunnel with Secret Server Cloud. [729845]
- Fixed an issue that caused Connection Manager to malfunction after upgrading to version 2.8.3. [730077]
- Fixed an issue where session recording failed for certain customers due to an outdated media processing library. [668260]
- Fixed an issue where Connection Manager could become stuck with lost focus and remain unusable until a force restart. [687033]

2.8.3 Release Notes

Date: April 29, 2026

Features

- Administrators can now unidirectionally restrict clipboard operations from the RDP server to the users' local machines and vice versa. See "Unidirectional Clipboard Enforcement on Windows" on page 174 and "Unidirectional Clipboard Enforcement on MacOS" on page 177 for more information.

Fixed Issues

- Fixed an issue where the session monitoring page in Secret Server was not showing that the session has ended displaying and error message. [718158]
- Fixed an issue where the duration of sessions did not match the session or the video content length. [723851]

Windows Specific

- Fixed an issue where the IWA would not allow refresh tokens for Connection Manager. [701833]
- Fixed an issue where sessions with session monitoring launched via Connection Manager were displaying a "Launcher did not start" error. [649218]

MacOS Specific

- Fixed an issue where Connection Manager would launch a secret with an incorrect launcher. [704562]
- Fixed an issue where Connection Manager failed to launch connections with certain username formats. [704582]
- Fixed an issue where Connection Manager would display an error after signing out from an RDP session guarded by MFA. [698144]
- Fixed an issue where Connection Manager could not connect via RDP proxy after a distributed engine upgrade.

Note: For your application settings to be automatically migrated from the configuration file to the Registry, you need to run Connection Manager as an administrator. [699913]

2.8.0 Release Notes

Date: *January 20, 2026*

Internal browser authentication is deprecated as of the 2.8 release.

Features

Windows Specific

- Users can now launch Secret Server Session Connector launchers directly from Connection Manager. See "Launchers" on page 137 for more information.
- Users can now update the Debug configuration without admin rights. See "Log Files" on page 200 for more information.
- Users can now install Connection Manager without admin rights on Windows. See "Installing on Windows" on page 7 for more information.

MacOS Specific

- FIDO2 WebAuthn authentication is now available on MacOS, which enables secure passwordless authentication using hardware security keys, biometrics or platform authenticators during remote RDP sessions. See "Authenticating With WebAuthn " on page 130 for more information.
- The RDP experience on MacOS was upgraded for improved usability and convenience including the ability to

resize without initiating a reconnect flow. The updated FreeRDP version now supports auto-resize. See "Desktop Size and Auto Expand" on page 126 for more information.

Improvements

- Users now have more consistency between application configuration and CLI installation settings with the ability to insert command line arguments during installation. See "Command Line Arguments" on page 17 for more information.
- User configuration settings are now preserved between upgrades.
- Added connection failed reason for INFO log level.
- Updated the password copy notification for property panel.
- Connection Manager now offers unicode clipboard support.

Windows Specific

- Users may now modify RDP rendering settings in order to reduce memory. See "RDP Rendering Settings" on page 169 for more information.
- Application configuration settings along with their values were moved from the Application Configuration file to the Registry on Windows. See "Application Configuration via Windows Registry Editor" on page 163 for more information.
- Users now have configuration options for external browser authentication including incognito mode so users can automatically close authentication tabs, authenticate with multiple accounts, adjust authentication window location, etc. See "Customizing External Browser Authentication" on page 23 and " Authenticating to Secret Server via External Browser " on page 56 for more information.

MacOS Specific

- Connection Manager now supports MacOS 26 (Tahoe).
- Addressed scaling issues with MacOS icons.

Fixed Issues

Windows Specific

- Fixed an issue where the AVBlocks library was using the *http* protocol instead of *https*. [636930]
- Fixed an issue where sessions launched with the SAP launcher were not recorded correctly. [668994]
- Fixed an issue where token refresh after expiry was causing an error to occur. [652745]

MacOS Specific

- Fixed and issue where copy-paste from remote to local device caused instability issues on Connection Manager. [648913]

Known Issues

- Connection Manager does not preserve collapsed state after upgrade from 1.9.2 to the latest version. [674591]

2.7.1 Release Notes

September 4, 2025

Features

- [Beta] FIDO2 WebAuthn authentication enables secure passwordless authentication using hardware security keys, biometrics or platform authenticators during remote RDP sessions. See "Authenticating With WebAuthn " on page 130 for more information.

Improvements

- Improved error messaging around the Prevent Direct API Authentication functionality in Secret Server.
- Improved the pop-up login and pincode windows to automatically receive focus when they appear, allowing users to immediately enter their credentials without needing to click on the window first.
- Updated the checked out message for mapped secrets.

Fixed Issues

- Fixed an issue where remote sessions were being closed when the connection to Secret Server was ended. [638740]
- Fixed an issue where users would experience flickering when attempting to use VMM applications and MECM consoles launched via Connection Manager. [663653]

2.7.0 Release Notes

July 1, 2025

> Starting with the 2.7 release, external browser authentication is now the default authentication method. While it is possible for administrators to enable internal browser authentication, it will be fully deprecated in the 2.8 release.

Features

- Connection Manager now offers the ability to launch websites and auto-fill credentials with the Web Password template through external vault connections. See "Launching Websites and Auto-Filling Credentials with the Web Password Template" on page 154 for more information.

Improvements

- Internal browser authentication is now disabled by default. This is part of our effort to fully deprecate internal browser authentication in the next release. However, administrators can re-enable internal browser authentication if needed. See "Enabling Internal Browser Authentication" on page 55 for more information.
- Connection Manager now backs up application.*dat* files and local storage files. See "Automatic Back Up for .DAT Files and Configurations" on page 128 for more information.
- Made multiple error message improvements. See "Troubleshooting Unhandled Errors " on page 207 for more information.
- Connection Manager now upgrades to the latest version without requiring application restart. See "Updates" on page 16 for more information.

Fixed Issues

MacOS Specific

- Fixed an issue where Connection Manager would display an "Unable to cast object" error when attempting to complete an MFA on secret challenge. [647850]

2.6.1 Release Notes

Release Date: April 24, 2025

Improvements

- Added a new *Env.OptionAsMetaKey* configuration setting on MacOS to allow for better handling of special characters and symbols when working with SSH connections. See "Configuring Special Characters in SSH Connections on MacOS" on page 182 for more information.

Fixed Issues

- Fixed an issue where RDP connections using mapped secrets would reconnect to the distributed engine server when proxy is enabled. [643314]

MacOS Specific

- Resolved an issue where the pipe symbol would not work for RDP connections with German keyboard layouts. [638935]

2.6.0 Release Notes

Release Date: March 31, 2025

> As of the 2.6 release, MacOS 12 (Monterey) is no longer supported. See "System Requirements" on page 7 for more information on supported operating systems.

In the 2.6 release, the CEF browser was updated to the latest version. This can cause additional files to appear in the `C:\Users\[username]\AppData\Roaming\Delinea\Connection Manager` folder.

For mapped secrets with a proxy enabled, Connection Manager selects the target host from the local secret. In previous versions, the target hosts were selected from the secret on the server

Features

- Users can now complete challenges to secrets guarded by MFA via external browser. See "Accessing Secrets Guarded by Multi-Factor Authentication" on page 195 for more information.
- Connection Manager now offers MacOS users a fullscreen display for a more native experience.
- The SSH terminal on MacOS was upgraded for improved performance, usability, and convenience. See "Using SSH Session Groups" on page 189 for more information.

Improvements

- Administrators can now centrally disable local vault for all users both during and after installation. See "Disabling Local Vault via Admin Enforcement" on page 26 for more information.
- Users can now launch files attached to secrets using Connection Manager. See "Attaching Files to Secret Launchers" on page 149 for more information.
- Users can now adjust the scrollback buffer size on MacOS to update the amount of lines they can scroll back inside the SSH terminal. See "Adjusting the SSH Scrollback Buffer Size on MacOS" on page 182 for more information.
- **Important:** The configuring SSH and RDP connection timeout over TCP parameters are now measured in seconds, as opposed to milliseconds. For more information on how this change will effect Windows and MacOS users, see "Configuring SSH Connection Timeout Over TCP" on page 181 and "Configuring RDP Connection Timeout Over TCP" on page 180.
- Users can now filter secrets by template when searching for a secret. See "Template Search " on page 36 for more information.
- After upgrading to version 2.6, Connection Manager will now relaunch automatically after upgrade. See "Updates" on page 16 for more information about this and other upgrade improvements.

Fixed Issues

- Fixed an issue where Connection Manager was not honoring the Browser Session Parameters. [562777]
- Fixed an issue where Connection Manager was not preserving the search results secrets in sub folders after a launching session. [570749]
- Fixed an issue where Connection Manager would ignore the machine name on mapped secrets for local SSH connections. [567590]
- Fixed an issue where users were not able to launch secrets from Secret Server when using Connection Manager as the protocol handler. [588139]

- Fixed an issue where Connection Manager would display an access denied message when attempting to convert a mapped secret to another template. [419431]
- Fixed an issue where access tokens were visible in the debug log in certain situations. [636093]

Windows Specific

- Fixed an issue where Connection Manager would display an error when clicking the RDP launcher after upgrading to version 2.5. [567956]
- Fixed an issue where no action was concurring after clicking Next in the Edit Vault window. [563159]
- Fixed an issue where the Connection Manager pin to start icon was no longer functional after upgrade. [604588]
- Fixed an issue where Connection Manager would display an error message when attempting to add a vault connection on 2.5.x. [608438]
- Fixed an issue where RDP sessions would close unexpectedly in Connection Manager version 2.5.3. [625811]
- Fixed an issue where Connection Manager was intermittently displaying a "Value cannot be null. Parameter name: rgb" error message when connecting to Windows servers. [628737]

MacOS Specific

- Fixed instability issues in Connection Manager when attempting to print documents from RDP secrets with shared printers. [584126]
- Fixed an issue where Connection Manager would display an incorrect default path for .DAT file after install. [596858]

2.5.4 Release Notes

Release Date: December 5, 2024

Improvements

- Connection Manager now offers a simplified authentication flow when authenticating to Secret Server via external browser. Users no longer need to click on a Secret Server page to launch Connection Manager. See " Authenticating to Secret Server via External Browser " on page 56 for more information.
- Connection Manager now makes it easier for users to troubleshoot distributed engine connection issues. See "Troubleshooting Proxies" on page 215 for more information.
- The Screenshot Queue Limit error message has been updated for improved clarity. See "Setting the Screenshot Queue Limit" on page 180 for more information.
- Administrators can now preconfigure multiple vaults so that users do not have to create connections themselves when opening Connection Manager for the first time. See "Pre-Configuring Vault Connections on Install " on page 20 for more information.
- Connection Manager now allows users to customize the RDP connection timeout over TCP (Windows). See "Configuring RDP Connection Timeout Over TCP" on page 180 for more information.

- When a new version of Connection Manager is available, users will see the version number of the latest version and a link to the release notes.
- The *About* page was updated with new icon and text styling.

Fixed Issue

- Fixed an issues where Connection Manager would display an "Unable to Connect" error message when disconnecting from a VPN. [603286]

Windows-Specific

- Fixed an issue where users would see flickering on the Virtual Machine Manager console and Configuration Manager Console when launching a secret from Connection Manager. [560833]
- Fixed an issues where Connection Manager was displaying an error when accessing servers. [596337]

MacOS-Specific

- Fixed an issue where Connection Manager was displaying an error after encountering an error with SSH connections. [574276]
- Fixed stability issues when authenticating to Connection Manager or connecting to an RDP session. [592726]
- Fixed stability issues when upgrading to version 2.5.3 from a previous version of Connection Manager. [607181]

2.5.3 Release Notes

Release Date: October 1, 2024

Improvements

- Connection Manager now displays release candidate installer versions, making it easier to update from an older release candidate to a newer one.
- Connection Manager now supports macOS 15 (Sequoia).
- All instances of *DoubleLock* were renamed to *QuantumLock* .
- Connection Manager now allows users to customize the RDP connection timeout over TCP (MacOS). See "Configuring RDP Connection Timeout Over TCP" on page 180 for more information.

Fixed Issues

- Fixed an issue where Connection Manager was not saving the color settings for the terminal under Advanced Settings.
- Fixed an issue where Connection Manager was displaying an error when selecting a secret with an SSH Proxy.

Windows

- Fixed an issue where the Connection Manager display was not adapting to the resolution of user monitors.

macOS

- Fixed an issue where users were not able to change the font family or font sizes.
- Adjusted the default value for the Screenshot Queue Limit.

Note: Prior to launching Connection Manager 2.5.3 for the first time, MacOS users will see a new password request. See "Delinea Encryption Key" on page 17 for more details

2.5.2 Release Notes

July 18, 2024

Customers who installed a prior Early Access build, should uninstall this build and do a clean reinstallation of the 2.5.2 version of Connection Manager.

Important notice for customers upgrading from 2.5.x. The Application Configuration file in the 2.5.2 release will be moved from *C:\Program Files\Delinea\Delinea Connection Manager\Delinea.ConnectionManager.dll.config* to *C:\Program Files\Delinea\Delinea Connection Manager\Delinea.ConnectionManager.exe.config*. This means you will need to manually transfer all data from the old location to the new one.

Bug Fixes

- Fixed an issue where users were not able to import RDP connections in RDG format.
- Fixed an issue where authentication from Connection Manager toSecret Server Cloud and Secret Server OnPrem 11.7.000016 resulted in 40x error codes.
- Fixed an issue where Connection Manager would terminate Secret Server sessions without reauthenticating.

Windows Specific

- Fixed a .NET memory leak related to opening and closing RDP sessions.
- Fixed a .NET memory leak related to reconnecting to RDP sessions.
- Fixed an issue regarding closing invisible tabs.
- Fixed an issue where Connection Manager fails to start after adding proxy configuration to the configuration file.
- Fixed an issue where Connection Manager would freeze when running RDP connections with session recording.

- Fixed an issue where Connection Manager displayed a reconnect dialog window for an extended period of time.
- Fixed an issue where Connection Manager would crash with a "Cannot access disposed object" error.

macOS Specific

- Fixed an issue where Connection Manager periodically crashes
- Fixed an issue where Connection Manager quit unexpectedly after opening and closing a number of RDP sessions.
- Fixed an issue where Connection Manager periodically crashes.

Known Issues

- A memory leak can occur when disconnecting RDP sessions via the "Disconnect" button on Windows. This leak can be addressed by "Enabling the Session Status Popup on Windows " on page 179 message.
- A minor memory leak in the UI can occur when opening and closing RDP sessions. This will be addressed in a future release.
- In the event of a slow internet connection or internet connection interruption, users may encounter an "OutOfMemory" exception (or noticeably slow performance from Connection Manager) for sessions with recording enabled. The workaround for this is to increase the *ScreenshotsQueueLimit* in the Application Configuration file. See "Session Recording" on page 139 for more information.
- Connection Manager for Windows is currently not rescaling RDP sessions dragged across multiple monitors with different DPI scaling values. The workaround steps for this issue are listed below:
  1. In your *Program Files* folder, right-click on the *Delinea.ConnectionManager.exe* application file and select **Properties**
  2. Select the *Compatibility* tab
  3. Click **Change high DPI settings**
  4. Check the **Override high DPI scaling behavior** box and select **System** from the dropdown.
  5. Click **Ok** to close the *Properties* window

2.5.1 Release Notes (Windows Only)

Release Date: April 24, 2024

> Due to ongoing memory leak issues from the .NET upgrade, this release is no longer available for download. We are actively working on a fix and will share once available. Until a fix is ready, we encourage users to download Connection Manager 2.4 for Windows and MacOS and follow these instructions to ensure as smooth an experience as possible: "Downgrading to an Older Version of Connection Manager" on page 208

Bug Fixes

- Fixed an issue where Connection Manager displayed an "Exception has been thrown by the target of an invocation" error when launching RDP or SSH launcher.

2.5.0 Release Notes

Release Date: April 23, 2024

> Due to ongoing memory leak issues from the .NET upgrade, this release is no longer available for download. We are actively working on a fix and will share once available. Until a fix is ready, we encourage users to download Connection Manager 2.4 for Windows and MacOS and follow these downgrade instructions to ensure as smooth an experience as possible.

Features

- Users can now configure the vault reauthentication behavior in Connection Manager. They can either keep the existing behavior that automatically restarts the authentication flow or force a fresh login when their vault session/refresh tokens have expired--mimicking the existing web API behavior. This new setting is beneficial for users who use SAML configuration through an external identity provider with a longer session/refresh length and enables audit logs to correctly generate upon logout.

Improvements

- The *Session Status* popup window is now disabled by default. This message appears every time a user signed out of a vault confirming that they have also signed out of the server. Users can reinstate this pop-up via configuration if they are experiencing any memory leak issues.
- Connection Manager now displays a "Machine" field from Secret Server, making it easier for users to identify the correct target when the secret name is not explicit. Any machine field that displays in the Secret Server grid view will also show in the Connection Manager grid view.

Deprecations

- The embedded apps functionality, on Windows, has been deprecated in the 2.5.0 release.

Bug Fixes

- Fixed an issue where Connection Manager was not displaying the server name.
- Fixed an issue where customers were unable to import connections from the Devolutions Remote Desktop Manager.
- Fixed an issue where the Secret Server version text was displayed as "Must be on Secret Server Version 11.2" instead of "Must be on Secret Server Version 11.2 or higher" when authenticating to a vault.

Windows Specific

- Fixed an issue where the "Home" and "End" keyboard buttons were not working in the Vim/Vi editor when launched via PuTTY in Connection Manager.
- Fixed an issue where a text message was displayed without an information link when using Connection Manager in dark mode.
- Fixed an issue where the "click here" button did not return RDP to full screen.

macOS Specific

- Fixed an issue where Connection Manager displayed the error message "The client and the server have no common host key algorithm" after running an SSH launcher.

Note: Windows configuration is now split between app configuration and user configuration.
• App configuration is located at `C:\Program Files\Delinea\Delinea Connection Manager\Delinea.ConnectionManager.dll.config`.
• User configuration is located at `C:\Users\%username%\AppData\Local\Delinea_Inc\Delinea.ConnectionManager_Url_%hash%\2.5.0.0\user.config`.

Note: If you are upgrading to 2.5 from 1.7, please upgrade to any version between 1.8 and 2.4 first before upgrading to 2.5. This will ensure you do not experience any issues with the backup functionality as part of the upgrade.

Note: If you experience any unusual error messages, please try uninstalling Connection Manager and doing a clean install or repair of the application.

2.4.0 Release Notes

Release Date: January 29, 2024

Features

- External Browser Authentication enables users to connect to the Delinea Platform via an external browser. This allows users to reuse their existing sessions and password managers in addition to advanced functionality like biometric MFA, FIDO2 support, and conditional access configurations with their preferred identity provider.

Improvements

- Users can also view updated properties and launcher panels with improved usability.

Bug Fixes

- Fixed an issue where Connection Manager was displaying the incorrect checkout time after extending checkout.
- Fixed an issue with bulk connections.

Windows Specific

- Fixed an issue where an error message was displayed after extending the checkout time.
- Fixed an issue where the Smart Card option was intermittently not being displayed in RDP sessions.
- Fixed an issue with multiple display monitors on Connection Manager version 1.9.6.
- Fixed an issue where an object reference error was being displayed when exiting out of full screen mode in SSH sessions.
- Fixed an issue where a "Cannot perform the requested operation in current session state" error was being displayed when connecting via SSH.
- Fixed an issue where Connection Manager was not able to connect to a local Secret Server connection after rebranding with a local URL.
- Fixed an issue where users were not able to start an SSH Group with multiple SSH Secrets.
- Fixed an issue where the "Extend Check Out" pop-up persists after session closure due to checkout time expiry.
- Fixed an issue where the "Connecting" message appeared and the "Reload" button was disabled when reloading Delinea Platform connections.
- Fixed an issue where the Connection Manager UI was not performing as expected when clicking or double-clicking on secrets.
- Fixed an issue where an error message was displayed in Delinea.app tenant's log files.
- Fixed an issue where secrets could not be edited from the Explorer View.
- Fixed an issue where the "Extend Checkout" button was mislabeled in Favorites.
- Fixed an issue where Connection Manager's return URL was malformed when the connection URL contained a trailing "/".
- Fixed issues with the Connection Manager UI where users were unable to click or double click to perform certain actions.
- Fixed an issue where sessions could not be launched from the menu bar when proxy with AD site selection was enabled.

2.3.1 Release Notes

Release Date: November 21, 2023

Improvements

- *PreferredAuthentications* setting added that allows specifying the SSH authentication methods priority order. Leaving the PreferredAuthentications value as empty will use previous version functionality (2.2) and will not use the new methods.

Bug Fixes

- Fixed an issue with the SSH authentication method selecting.

2.3.0 Release Notes

Release Date: November 13, 2023

Features

- Connection Manager now offers support for macOS 14 Sonoma.
- Users are now able to extend the secret checkout timer directly from the Connection Manager UI. (Windows only)
- Connection Manager can now complete logins when MFA is enabled on target machines with the Delinea Privilege Control. (Windows only)

Improvements

- *Auto-fill* has been relabeled to *Auto Resize.*

Bug Fixes

- Fixed an issue where external browser login was not working correctly on Windows Server (Using the Local Group Policy Editor)
- Fixed an issue where users had to complete multiple MFA prompts after upgrading to Connection Manager version 2.0.
- Fixed an issue with a double SAML token request in Connection Manager version 2.0.1 and newer.
- Fixed an issue where the "WinWord Process Launcher" was keeping an RDP connection active, even if the user activated the "Terminate immediately" option.
- Fixed an issue where the Smart Card option was intermittently not being displayed while in an RDP session.
- Fixed an issue where auto-fill was not working correctly when changing a window's size during the launch process.
- Fixed an issue where Connection Manager was not able to launch a URL link with ":" if this symbol was entered manually.
- Fixed an issue where Connection Manager was using a high amount of GPU.
- Fixed an issue where the full screen mode was not actually full screen when using RDP Proxy.

2.2.0 Release Notes

Release Date: September 27, 2023

Features

- When using local secrets mapped to vaulted secrets, Connection Manager users can now select any defined proxy site they need to use for connecting with the target specified in the local secret.

Improvements

- The auto-expand feature has been improved to allow customers to automatically resize their remote connection view when working with RDP connections.

Bug Fixes

- Fixed an issue where the check in/check out information was missing from the countdown timer.
- Fixed an issue where users were unable to automatically map headers from imported CSV files.

Windows Specific

- Fixed an issue where Connection Manager did not clean up memory when connections were closed.
- Fixed an issue where users were unable to create a folder using the right click mouse button.
- Fixed an issue where the Connection Manager tab would not close correctly when attempting to exit out of a proxied connection.
- Fixed an issue where an incorrect app name was displayed in the Connection Manager installer.
- Fixed an issue where the Connection Manager remote session name tab did not display the correct machine name.
- Fixed an issue where auto resize was not working consistently when maximizing the Connection Manager window.
- Fixed an issue where a CSV file could not be imported with a tab delimiter.
- Fixed an issue with Connection Manager instability when the RDP reconnect clipboard would fail.
- Fixed an issue where the Connection Manager session tab would freeze because of multiple reconnection attempts when switching between tabs with an active RDP session.

macOS Specific

- Fixed an issue where Connection Manager would display an RDP Error "Unable to connect to Server to verify its HTTPS certificate".

2.1.0 Release Notes

Release Date: August 17, 2023

Release Date: August 14, 2023

Features

- Users are now able to access secrets guarded by MFA by completing the MFA challenge from within Connection Manager.

Improvements

- Improved scroll-back buffer size in SSH on Windows. Clients can now use a 32k-line scroll-back buffer out of the box for SSH sessions. The macOS buffer size is unlimited
- The launcher icon and text are now clickable. The hover and alt-text now mirror the label for improved accessibility [Windows]
- Connection Manager now assumes https if the user has not entered a protocol as part of their vault URL (Delinea Platform or Secret Server)

Bug Fixes

- Fixed an issue where Connection Manager's custom launcher was not displaying the correct field name
- Fixed an issue where Connection Manager was displaying an error message and allowing users to open unencrypted DAT files in the DEBUG log
- Fixed an issue where Connection Manager was not accepting SSH keys with a passphrase
- Fixed an issue where Connection Manager was displaying an invalid response when an RDP Launcher session was launched with a server field on Windows
- Fixed an issue where the Connection Manager launcher allowed the prompt to contain an forward slash character
- Fixed an issue where Connection Manager was displaying a warning about the version when using the external browser with Secret Server Cloud
- Fixed an issue where Connection Manager would crash after closing the popup window that is waiting for authentication
- Fixed an issue where Connection Manager was not checking secrets when connected to Secret Server Cloud using the external browser and local connection
- Fixed an issue where Connection Manager was not displaying the version of Secret Server and information text for the *Connection* dialog
- Fixed an issue where Connection Manager was displaying an incorrect URL message error message for Secret Server sites on macOS

2.0.1 Release Notes

Release Date: July 5, 2023

Improvements

- Connection Manager now supports universal-token based authentication with the Delinea Platform.

Bug Fixes

- Fixed a bug that caused instability with Connection Manager when a secret was checked out by a different user

2.0.0 Release Notes

Release Date: May 24, 2023

Features

- Users can add connections to their vault by using their Delinea Platform tenant URLs. Connection Manager will connect seamlessly to their Platform tenant vault and users will be able to use secrets in the vault in the same way as they do today with a direct Secret Server integration.

Bug Fixes

- Fixed an issue where Connection Manager was only displaying the top 30 secrets of a Secret Server folder containing more than 30 secrets.
- Fixed an issue where Connection Manager was evaluating Batch Launcher Parameters incorrectly.

Known Issues

- Audit session recordings can be found in the vault direct web portal (Secret Server web UI). The ability to send audit session recordings to the Delinea Platform will be added in a future release.
- Users with MFA-enabled secrets (a Platform-only feature) will not be able to use these secrets from Connection Manager version 2.0.0. A future release of Connection Manager will support this capability.
- Connection Manager version 2.0.0 does not currently support a small subset of federated logins related to Azure AD Conditional Access when used with the Delinea Platform. Support for this ability is scheduled for a future release.

1.9.7 Release Notes

Release Date: April 18, 2023

Bug Fixes

- Fixed an issue on the Mac platform, where Connection Manager would crash when viewing a secret with an active "Hide Password" flag.

1.9.6 Release Notes

Release Date: April 3, 2023

Features

- Connection Manager now offers support for the *Preserve SSH Client Process*. This prevents custom launchers that result in single tabbed processes from exiting when multiple launches are pulled into it.

Bug Fixes

- Fixed an issue where a tab would not close after Connection Manager crashed.
- Fixed an issue where an incorrect *Properties* panel was displayed in the secret check-out timer.
- Fixed an issue where Connection manager would close third-party apps after the connection was terminated.
- Fixed an issue where an error message was displayed to the users when a connection was terminated after the secret check-out timer expired.
- Fixed an issue where an incorrect screen was displayed to the users after the secret check-out timer expired.
- Fixed an issue where Connection Manager would crash after updating from version 1.8 to 1.9.5.
- Fixed an issue where Connection Manager would crash when attempting to check-out two secrets.
- Fixed an issue where an incorrect *Properties* panel was displayed if the user was not able to connect to host on the secret.
- Fixed an issue where an error message was not being displayed after the checkout timer expired on a secret.
- Fixed an issue where Connection Manager would crash after clicking the *Check-Out* button.
- Fixed an issue where Connection Manager would crash after clicking *Check-In* on Secret Server in browser.

1.9.5 Release Notes (Windows)

Release Date: January 17, 2023

Features

- Connection Manager now supports custom launchers using the *Proxied SSH Process* launcher type when the *Preserve SSH Client Process* is selected. Closing the Connection Manager tab for these sessions will no longer enforce terminating the external application, allowing for other connections within the external application to continue uninterrupted.
- Connection Manager now shows a secret checkout timer which allows users to see how much time they have before the checkout expires.
- Connection Manager now offers a new version number which makes it easier for users to see which version of Connection Manager they are using from the *About* menu.

General Improvements

- When creating a new Secret Server connection, the "External browser" option will now be selected as the default connection type. This was implemented to support a security hardening initiative in Secret Server.

Maintenance Improvements

- The EULA link in Help > About was updated to point to Delinea’s Master Subscription and License Agreement. Previously the link pointed to the delinea.com website EULA

Bug Fixes

- Fixed an issue where users would encounter an error message after double-clicking on a connection to a Secret Server instance
- Fixed an issue where proxied RDP connections would disconnect when the screen was resized
- Fixed an issue where Connection Manager was preventing users from launching Unix secrets that use "User Input" for the launcher
- Fixed an issue where users would encounter an error when attempting to launch SSH connections from a mapped secret where an Active Directory secret template was used
- Fixed an issue where Connection Manager would crash when clicking on the Favorites folder
- Fixed an issue where the Help button in the 1.8 version of Connection Manager would take users to an old documentation page for the 1.7 version of Connection Manager
- Fixed an issue where Connection Manager would prompt users for credentials if the connection was interrupted
- Fixed an issue where Connection Manager would disable the Alt+F4 keystroke combination across all windows
- Fixed an issue where Connection Manager's RDP clipboard was rendered inoperable with the CrowdStrike Falcon agent installed on Windows

1.9.2 Release Notes

Release Date: September 1, 2022

Features

- Users can now create a Secret Server connection via an external browser. This resolves issues with limitations in the embedded browser that prevent some SAML logins from completing successfully.
- Users can now automatically see secrets created on new templates without editing connection settings. The 3rd step of the **Edit Connection** dialog now contains two options: one to select all templates including ones created later, and one to select specific templates to view in Connection Manager. The default option for new installations is *All Templates* and can be changed by the user by editing the Secret Server connection.
- Silent installations will now set the selected templates to *All Templates*. This can be changed by the user after installation by editing the Secret Server connection.

General Improvements

- Updated FreeRDP 2.4.0 to the latest version.

Security Improvements

- Updated Coverlet.Collector to the latest version.
- Updated Newtonsoft.Json to the latest version.
- Updated log4net 2.0.13 to the latest version.

Bug Fixes

- Fixed an issue where Connection Manager was not showing the full password.
- Fixed an issue where the 1.8 version of Connection Manager was missing the Refresh button in dark theme.
- Fixed an issue with the RDP Client title bar behavior with RDP Proxy. The title was not showing the target in full screen mode.
- Fixed an issue where the connections list attempted to connect to the wrong server.
- Fixed an issue where users were seeing the wrong font for SSH Local Connection after installing Connection Manager.
- Fixed an issue where users where getting an error message when clicking the **Show** button to show the password.
- Fixed an issue where Connection Manager was not honoring the *Hide Password* setting when adjustments were made at the Secret Template level

iOS Specific

- Fixed an issue where the cursor position would change when the window was resized on a Mac.

1.8.0 Release Notes

Release Date: April 19, 2022

Features

- Delinea Connection Manager now supports:
  - All M1 chipsets
  - Windows 11
- Delinea Connection Manager now allows AD Site Selection.
- This release includes the new Delinea Inc rebranding along with our new company colors and icons.

General Improvements

- Users will now be able to see the ServerName (proxied over "proxy name") in a tab header when connecting through proxy.
- We optimized load performance in larger environments with 65K or more secrets and 40K or more folders. This performance improvement should be especially noticeable on slower connections.

Bug Fixes

- Fixed an issue users were experiencing where the screen size would automatically change from the set desktop size to the one in the secret settings.
- Fixed an issue where Connection Manager command lines did not allow both -disablelocalvault and Secret Server connection switches.

- Fixed an issue where the remote host name is not displayed on the tab for proxied RDP session.
- Fixed an issue where users were unable to scroll inside Connection Manager if there is any text selected.
- Fixed an issue where an update couldn't be automated under local system account (in quiet mode)
- Fixed an issue where Connection Manager cannot be uninstalled with SYSTEM account

iOS Specific

- Fixed an issue with the Clipboard feature macOS users were experiencing, which prevented them from copying from a Mac to an RDP endpoint.

1.7.1 Release Notes

Release Date: November 30, 2021

Bug Fixes

- Fixed an issue where the login URL is not detected properly if SS URL ends with '/'.
- Fixed an issue where an error occurs when connecting to a RDP session when proxy is enabled.
- Fixed issues related to SecretServer URL validation in certain federation scenarios.
- Fixed an issue with SAML login when the Secret Server web services timeout is set to "Unlimited". We do not recommend setting the web services timeout to "Unlimited".

1.7.0 Release Notes

Release Date: November 9, 2021

Product Enhancements

SSH Grouping

- Users can now create one or more groups of active SSH sessions using a new toolbar icon or by using the **Create SSH Group** option in right-click context menus. By creating an SSH group, a user can send a command or series of commands in bulk to all active sessions in the group. See Using SSH Session Groups.

General

- The way Connection Manager takes screen shots of active connections has been optimized for efficient resource usage.
- Users can now drag the left edge of a secret's Properties panel to enlarge the panel.
- Users can now view helpful information about Secrets in pop-up windows by mousing over different parts of a Secret in the main Secrets view.
- On Secret Details screens, users can now manually refresh the display of the secret's information by clicking a Refresh button. The information is refreshed simultaneously in the Properties, Shared With Me, and Favorites panels.

- Using the column picker, you can now add a Heartbeat column to the main Secrets view to display heartbeat results returned by Secret Server.

  The heartbeat value represents a point in time; it is not automatically updated in real time. The user must manually refresh the page yo see the most current value.
- Every password field and Private Key Passphrase field now offers the user an option to show the hidden password characters if you have View permissions. Depending upon permissions in Secret Server, you might be able to copy the password using the Copy icon, without having View permissions.
- WLOG output can now be viewed in Connection Manager debug logs for macOS.
- We added more command line arguments to the Connection Manager documentation and we clarified related content such as which arguments should be used for installation and which should be used for startup.
- We added information to the Connection Manager documentation identifying default folders for macOS.
- We updated and clarified the content in the Connection Manager documentation on Global Configuration options and their related behaviors.
- For secrets protected by both Checkout Required and Enter Comment workflows, users can input their comment text and then simply click the “Enter Comment” button to automatically check out the secret.

Bug Fixes

- We fixed an issue where RDP screen shots came out black when taken in full screen mode.
- We fixed an issue where auto-sizing was not working as expected.
- We fixed an issue where only the first machine was displayed in a secret's Machine field list, rather than the machine connected to when launching from Secret Server.
- We fixed an issue where Connection Manager's Map Secret feature was throwing no authentication method for .ppk (private key) files.
- We fixed an issue that arose when a user using two monitors opened an RDP connection in full screen mode on one monitor, and that monitor's active session screenshot display was black.
- We fixed an issue in the user interface that was preventing some users from connecting to the last Secret Server connection listed in the left navigation panel.

macOS Bug Fixes

- We fixed an issue where a user reconnecting to Secret Server received the error message, "Object reference not set to an instance of an object," followed by Connection Manager crashing.
- We fixed an issue where Connection Manager was crashing after a PuTTY paste with the error message, "Object referenced not set to an instance of an object."
- We fixed an issue where Connection Manager was crashing when a user performed a copy and paste in an SSH session.
- We fixed an issue where macOS (Big Sur v.11.5) was getting stuck when attempting to connect to Secret Server via Connection Manager.

Known Issues and Workarounds

- Connection Manager "Local Login" allows users to log in with their username, but if they try to log in with their UPN, the login fails.
- Connection Manager does not generated a token when the URL for a web login ends on a /.