Delinea

Connection Manager

Documentation 1.3.0

Table of Contents

With Thycotic Connection Manager, IT teams can launch ad-hoc connections to manage sessions with remote resources, navigating Remote Desktop Protocol (RDP) and Unix Secure SHell (SSH) connection protocols as needed. 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 Thycotic'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.

Installation of 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 below procedures:

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

System Requirements

Connection Manager is a client-side application that can be installed on either Windows or Apple OS X operating systems.

Minimum requirements for client-side installation:

- Windows Installation: Windows 8 or later, 8GB RAM (please be aware that Windows 7 support ended January 14th 2020: https://docs.microsoft.com/en-us/deployoffice/windows-7-support). Thycotic recommends upgrading clients to Windows 10.
- Macintosh Installation: OS X 10.13x (High Sierra) or later, 8GB RAM

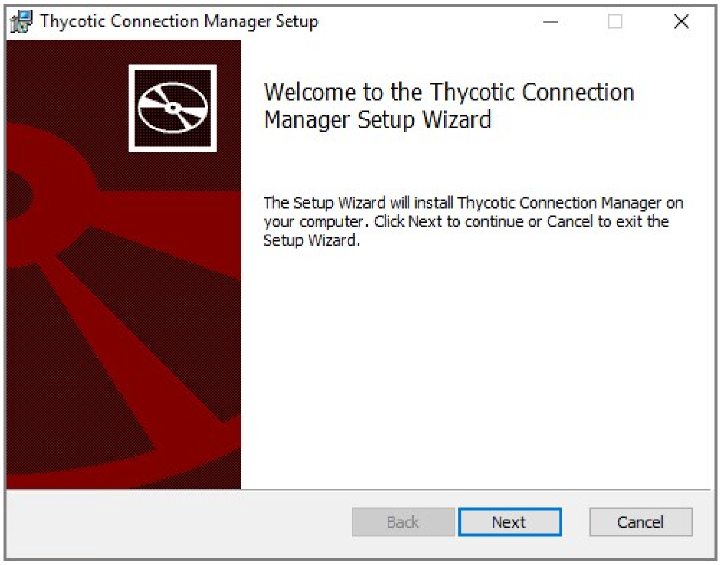
Minimum requirements for connectivity to Secret Server(s):

- Secret Server Installation: 10.7 or later

Windows Installation

Note: On Windows systems when you are upgrading to Connection Manager 1.3.0 only, do not follow the in product update option. Instead uninstall your current version of Connection Manager (make sure to backup/export your local connections first), then install the new 1.3.0 version of Connection Manager. This is only a one-time issue when upgrading from previous Connection Manager versions to the release 1.3.0 version.

1. Download the Windows Installer File (MSI) for Connection Manager.
2. Double-click the MSI file to start the install process.

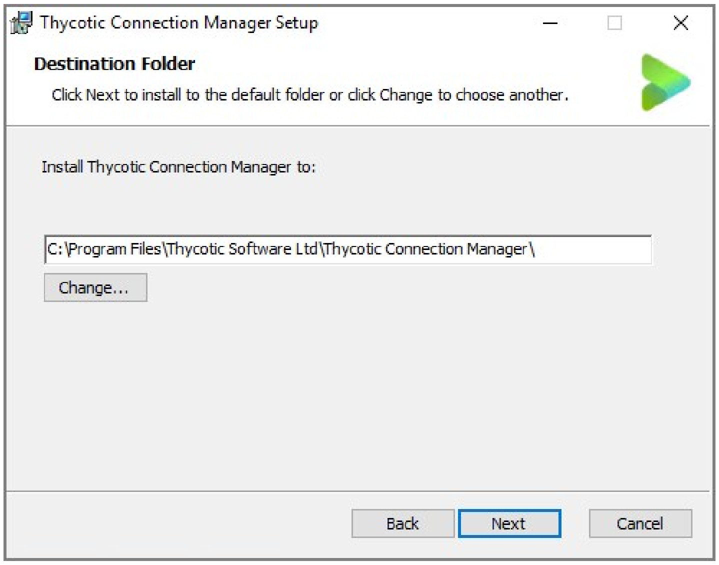


Thycotic Connection Manager Setup

Welcome to the Thycotic Connection Manager Setup Wizard

The Setup Wizard will install Thycotic Connection Manager on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

3. Click **Next** to continue.



Thycotic Connection Manager Setup

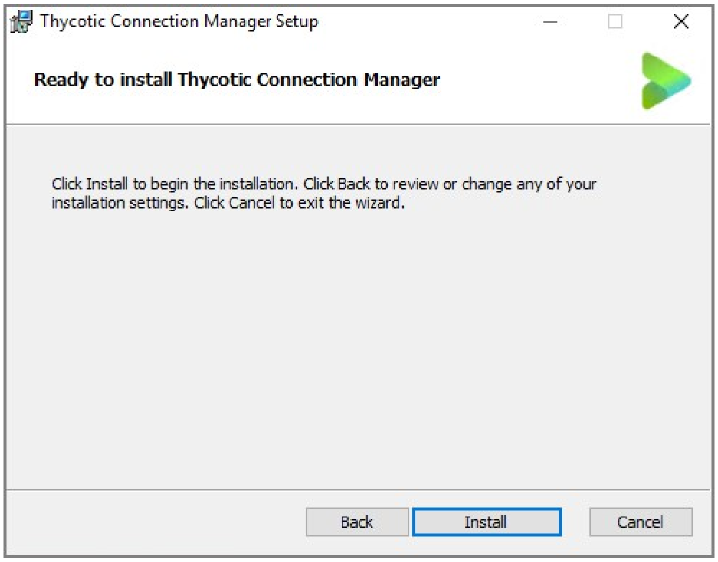
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Thycotic Connection Manager to:

C:\Program Files\Thycotic Software Ltd\Thycotic Connection Manager\

4. Select the **location to install Connection Manager** or leave the default location.
5. Click **Next** to confirm the location and accessibility for the install.

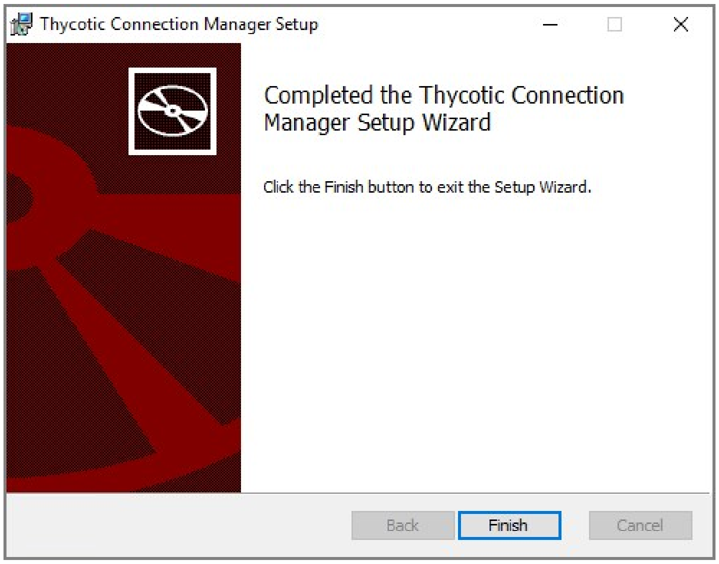


Thycotic Connection Manager Setup

Ready to install Thycotic Connection Manager

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

6. Click **Next** again to start the installation. A progress bar will be displayed while the installation is in progress.



Thycotic Connection Manager Setup

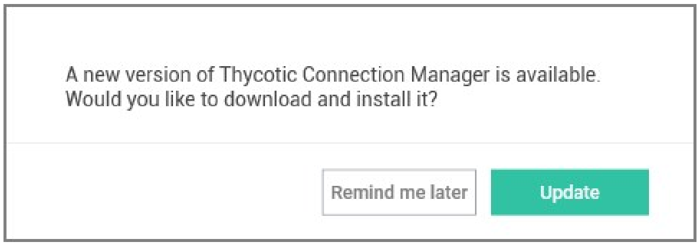
Completed the Thycotic Connection Manager Setup Wizard

Click the Finish button to exit the Setup Wizard.

7. Once the install has finished, click **Finish**.

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

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 to be reminded later.

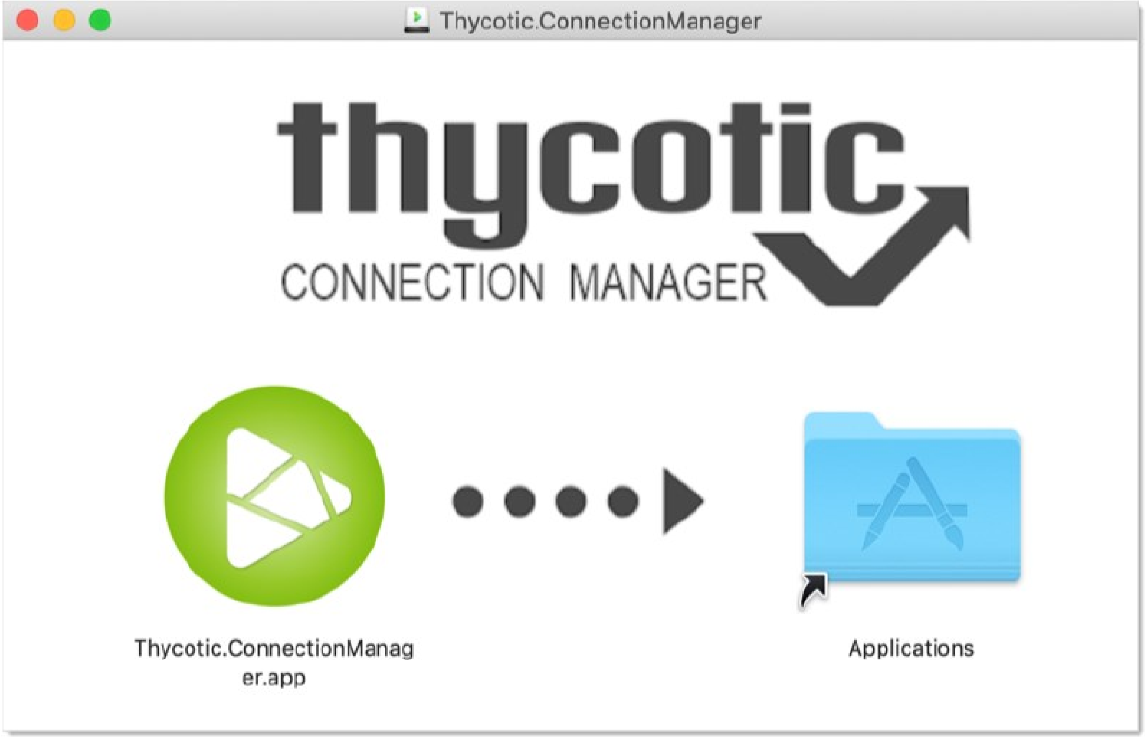


A new version of Thycotic Connection Manager is available.
Would you like to download and install it?

MacOS Installation

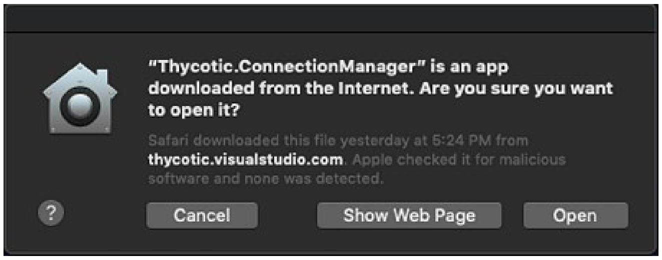
1. Download the DMG file from Thycotic's Free Tools page.
2. Select **Mac** download. A PKG file will download to your system.

   Note: The file extension is a .pkg starting with release 1.2.0.
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 Thycotic 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**.



"Thycotic.ConnectionManager" is an app downloaded from the Internet. Are you sure you want to open it?

Safari downloaded this file yesterday at 5:24 PM from **thycotic.visualstudio.com**. Apple checked it for malicious software and none was detected.

Command Line Arguments to Create a Secret Server Connection on Install

The following command line arguments can be used to install Connection Manager and create a connection to Secret Server when using the MSI file.

> **Important**: /quite mode installation works only with Administrative privileges. If the MSI is run with /quite under normal user context, nothing will happen.

```
Thycotic.ConnectionManager.WixInstaller.msi  /quiet RUNCM=runCM KEYS="-ssurl ""https://connmanagerss.thycotic.net/ss"" -ssname ""n e w s e r v e r"" -ssauth web"
```

```
Thycotic.ConnectionManager.WixInstaller.msi  /quiet RUNCM=runCM KEYS="-ssurl ""https://connmanagerss.thycotic.net/ss"" -ssname ""n e w s e r v e r"" -ssauth local"
```

> **Note**: you have to use double quotes inside the KEYS parameter because the value of the KEYS parameter is quoted itself.

Getting Started

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

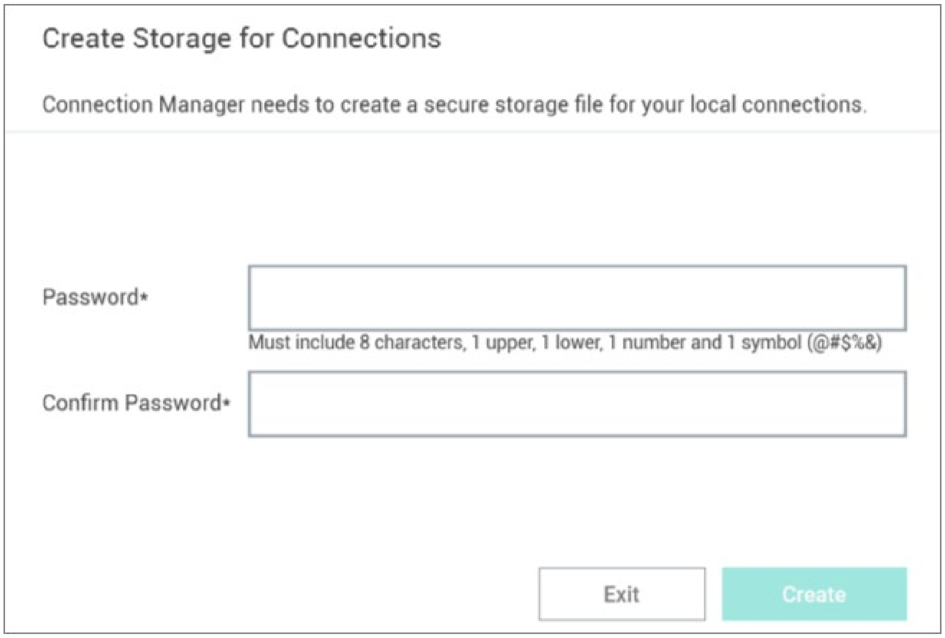
- Secret Server Requirements
- Create a Password
- Sign in
- User Interface Components

Create 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.



Create Storage for Connections

Connection Manager needs to create a secure storage file for your local connections.

Password*

Must include 8 characters, 1 upper, 1 lower, 1 number and 1 symbol (@#$%&)

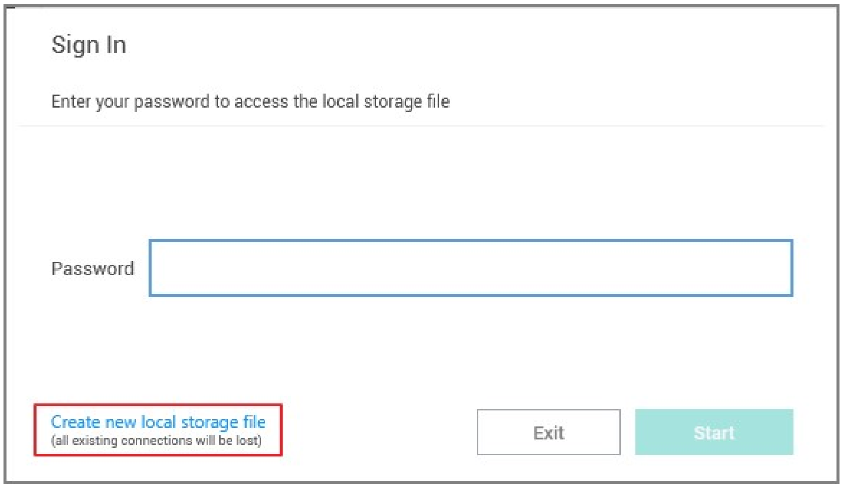
Confirm Password*

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.

Sign in into Connection Manager

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



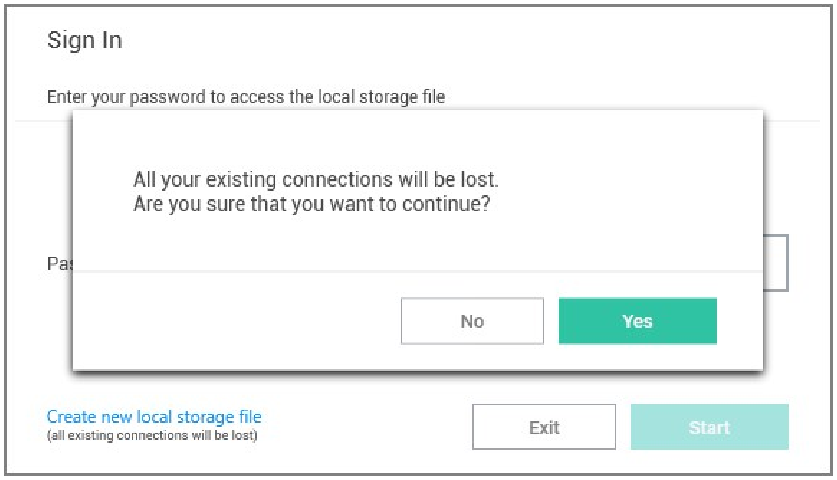
Sign In

Enter your password to access the local storage file

Create new local storage file
(all existing connections will be lost)

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.



Sign In

Enter your password to access the local storage file

All your existing connections will be lost.
Are you sure that you want to continue?

Create new local storage file
(all existing connections will be lost)

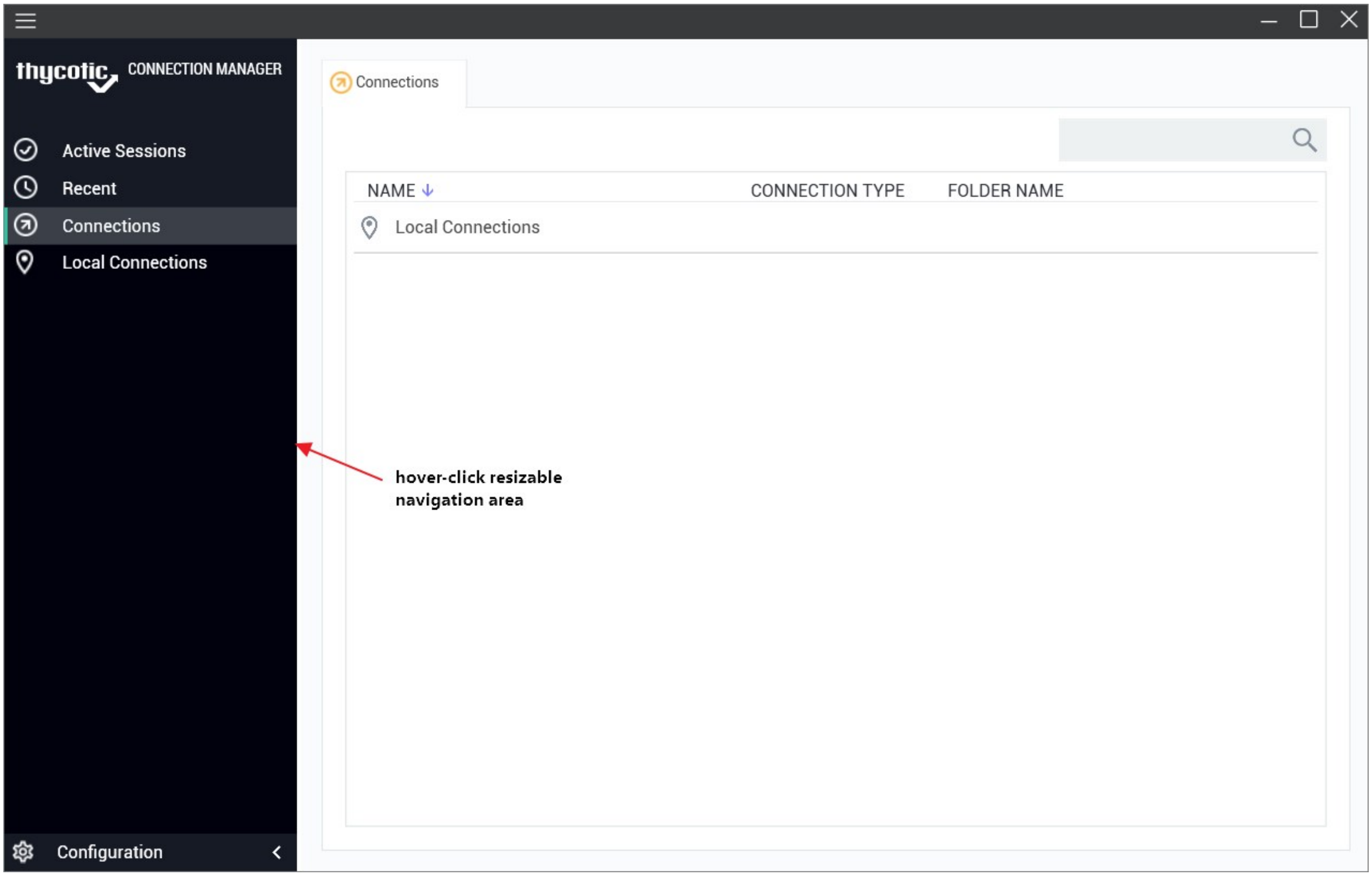
Users of Secret Server's modern interface will find Connection Manager's interface and functionality to be similar in look and feel. The interface takes advantage of some client-side functionality such as right-click menus, double-click menus, and others.

- Main Screen
- Navigation Tree
- Work Area
- Properties Area
- Menus

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.

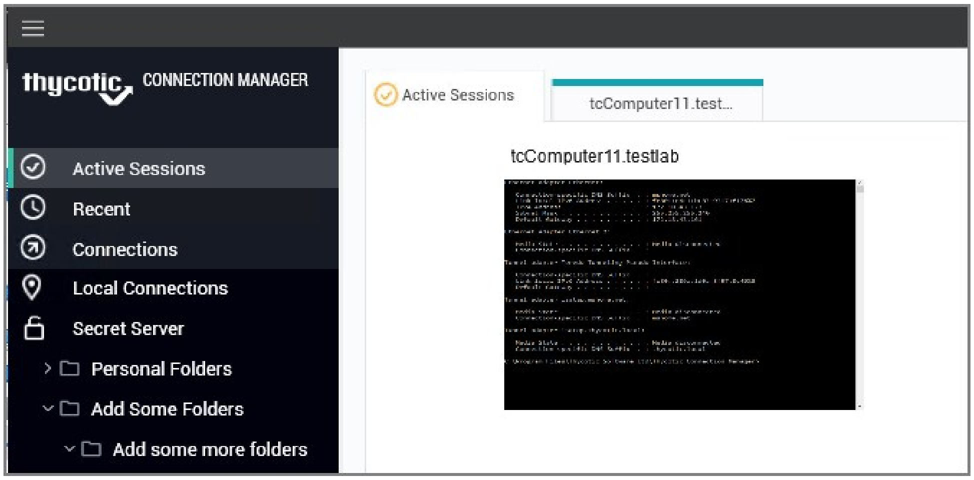


NAME ↓	CONNECTION TYPE	FOLDER NAME
Local Connections		

The navigation area is hover-click resizable.

Active Sessions

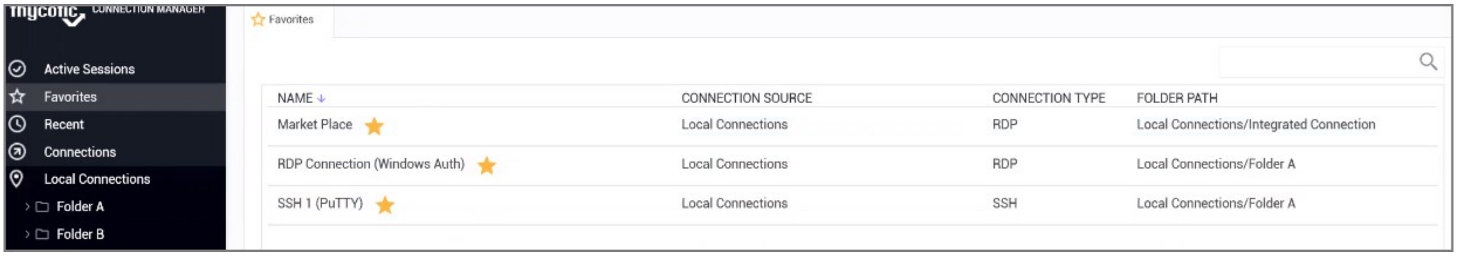
Select to view all active sessions.



Favorites

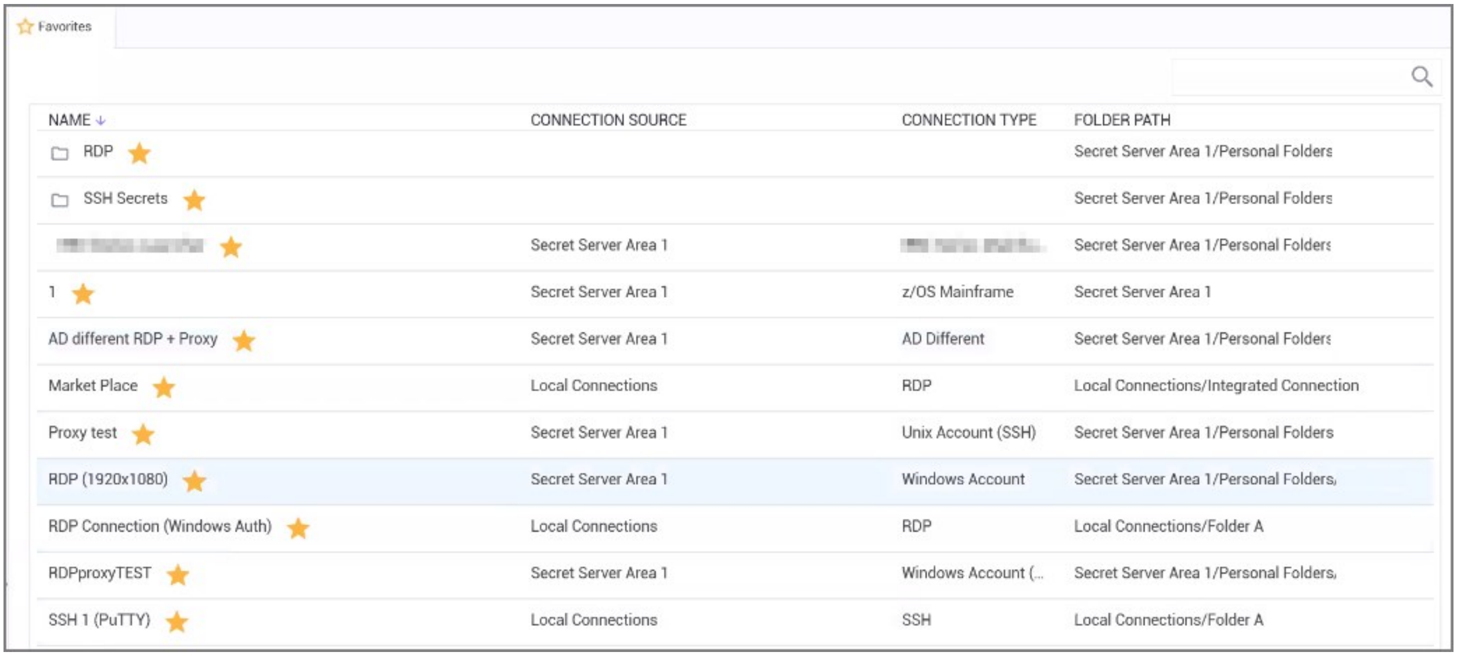
You can add favorite connections by hovering over an existing connection and selecting the star. Favorites that are specified in Connection Manager will also be listed as favorites in Secret Server and vice versa.

Favorites page showing only local connection favorites:



NAME ↓	CONNECTION SOURCE	CONNECTION TYPE	FOLDER PATH
Market Place ★	Local Connections	RDP	Local Connections/Integrated Connection
RDP Connection (Windows Auth) ★	Local Connections	RDP	Local Connections/Folder A
SSH 1 (PuTTY) ★	Local Connections	SSH	Local Connections/Folder A

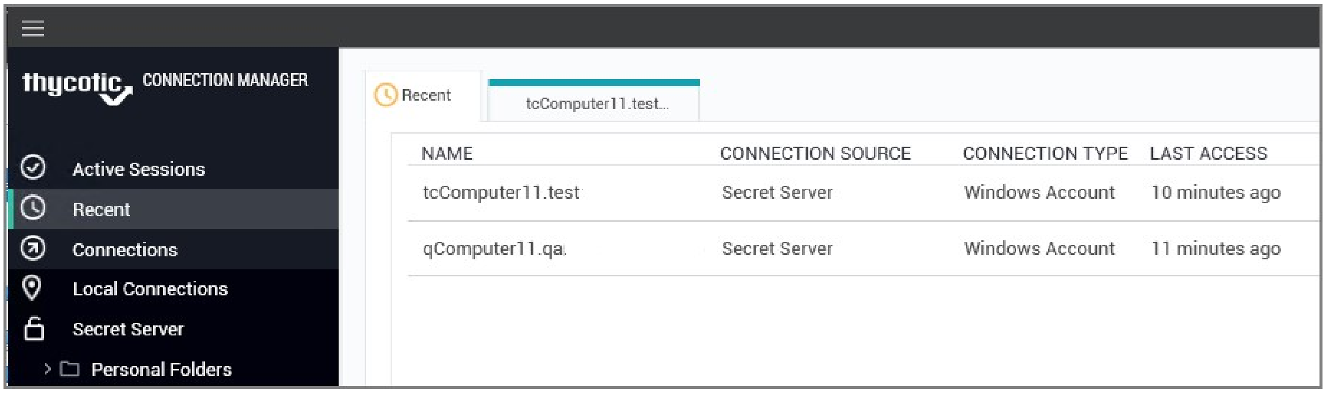
Favorites page showing local and Secret Server connection favorites:



NAME ↓	CONNECTION SOURCE	CONNECTION TYPE	FOLDER PATH
RDP ★			Secret Server Area 1/Personal Folders
SSH Secrets ★			Secret Server Area 1/Personal Folders
[redacted] ★	Secret Server Area 1	[redacted]	Secret Server Area 1/Personal Folders
1 ★	Secret Server Area 1	z/OS Mainframe	Secret Server Area 1
AD different RDP + Proxy ★	Secret Server Area 1	AD Different	Secret Server Area 1/Personal Folders
Market Place ★	Local Connections	RDP	Local Connections/Integrated Connection
Proxy test ★	Secret Server Area 1	Unix Account (SSH)	Secret Server Area 1/Personal Folders
RDP (1920x1080) ★	Secret Server Area 1	Windows Account	Secret Server Area 1/Personal Folders,
RDP Connection (Windows Auth) ★	Local Connections	RDP	Local Connections/Folder A
RDPproxyTEST ★	Secret Server Area 1	Windows Account (...	Secret Server Area 1/Personal Folders,
SSH 1 (PuTTY) ★	Local Connections	SSH	Local Connections/Folder A

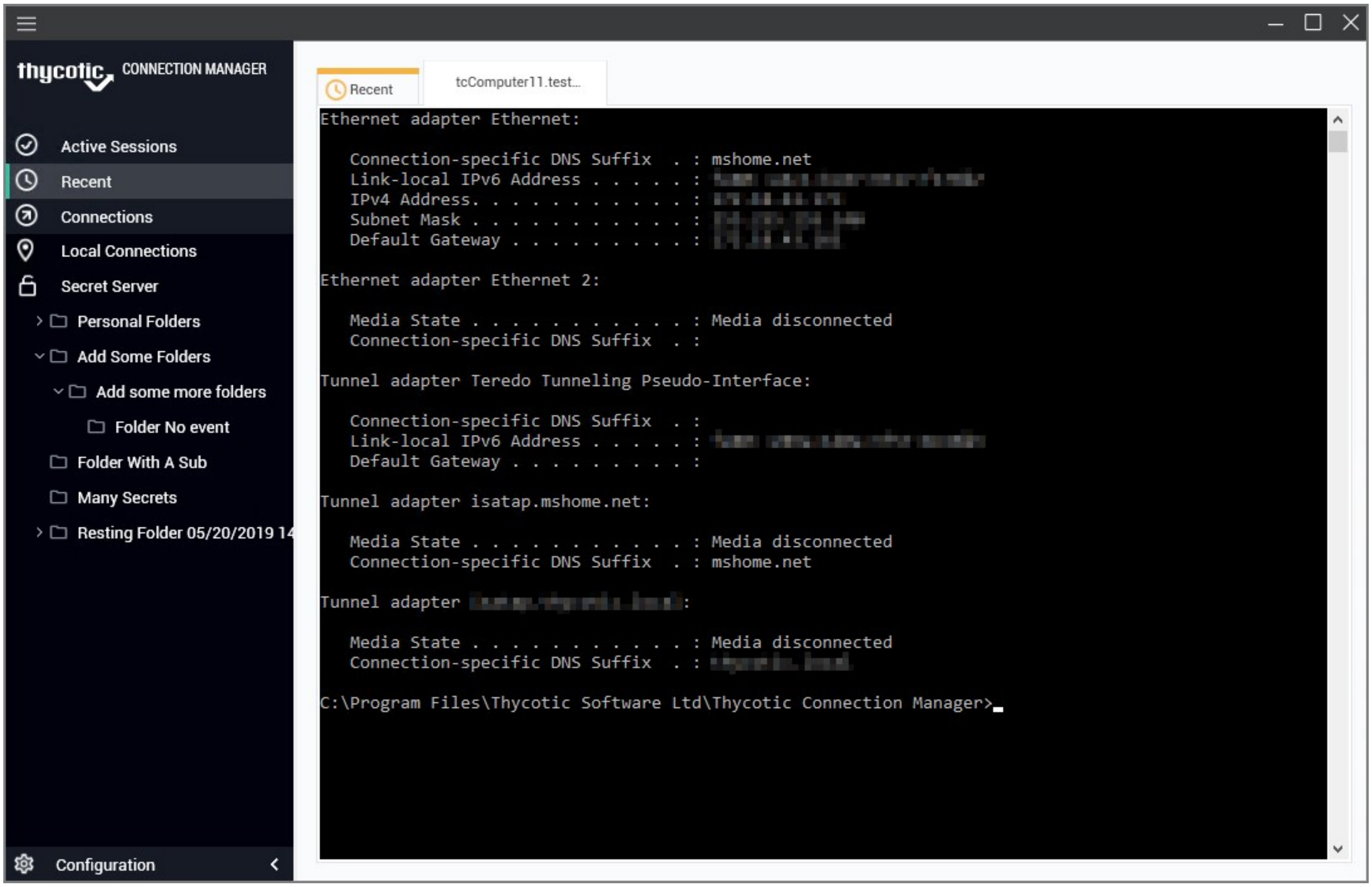
Recent

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



NAME	CONNECTION SOURCE	CONNECTION TYPE	LAST ACCESS
tcComputer11.test	Secret Server	Windows Account	10 minutes ago
qComputer11.qa.	Secret Server	Windows Account	11 minutes ago

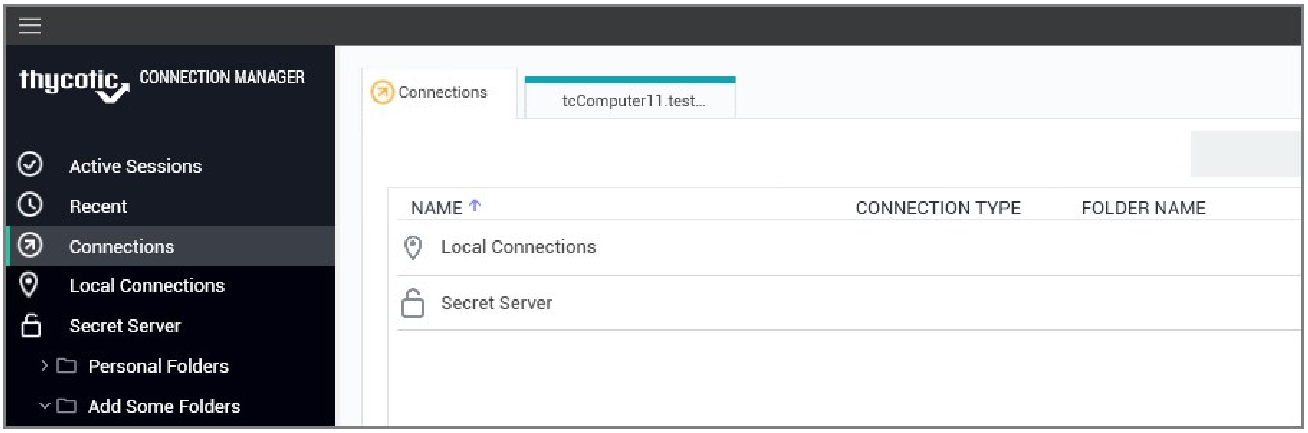
Existing entries also display connection type. These can be viewed via tab.



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   Default Gateway . . . . . . . . . : [redacted]

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.mshome.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : mshome.net

Tunnel adapter [redacted]:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : [redacted]

C:\Program Files\Thycotic Software Ltd\Thycotic Connection Manager>_
```

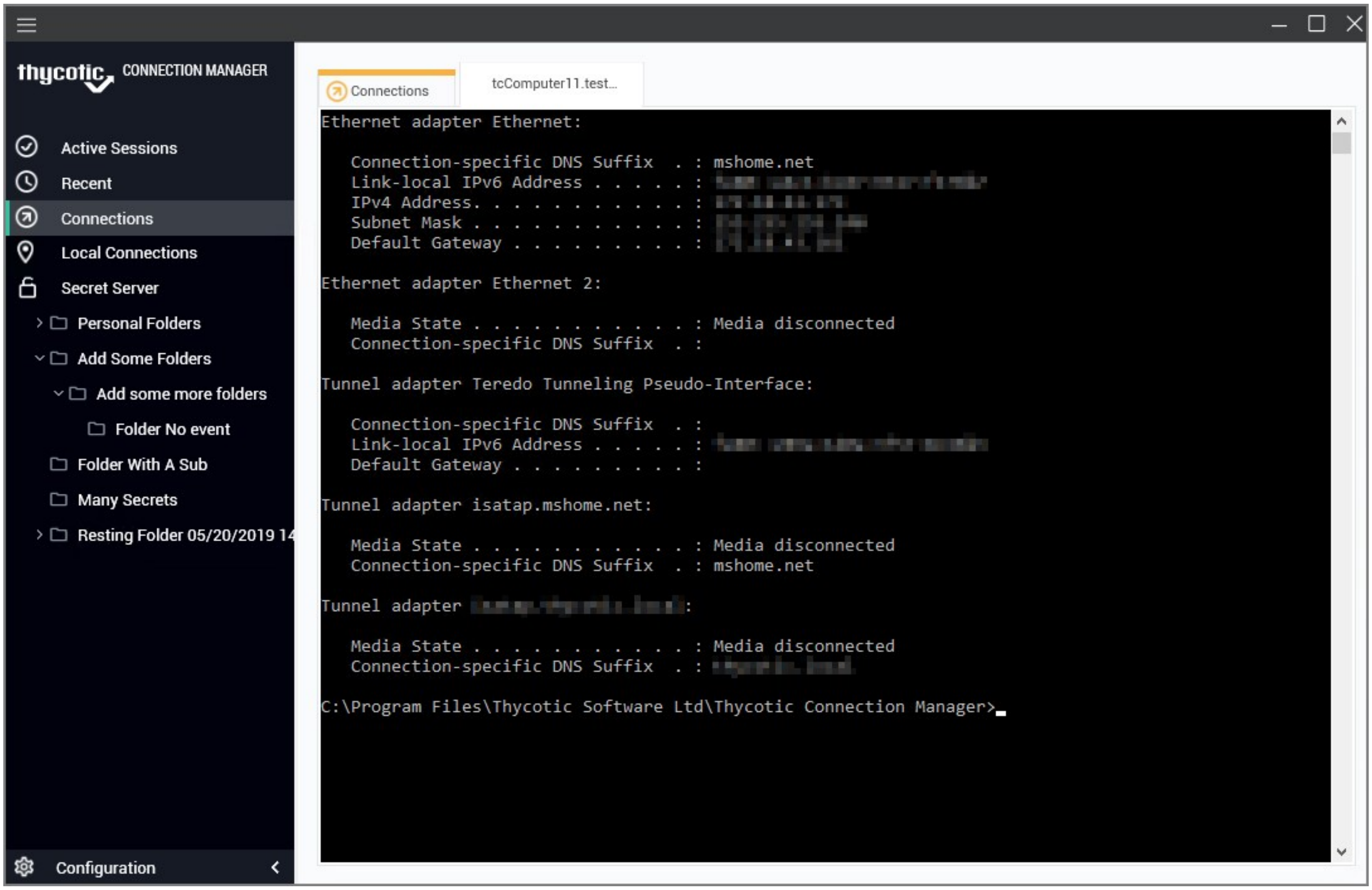
Connections

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



NAME ↑	CONNECTION TYPE	FOLDER NAME
Local Connections		
Secret Server		

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



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   Default Gateway . . . . . . . . . : [redacted]

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.mshome.net:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : mshome.net

Tunnel adapter [redacted]:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : [redacted]

C:\Program Files\Thycotic Software Ltd\Thycotic Connection Manager>_
```

Local Connections

Select to view all local connections.

Configuration

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

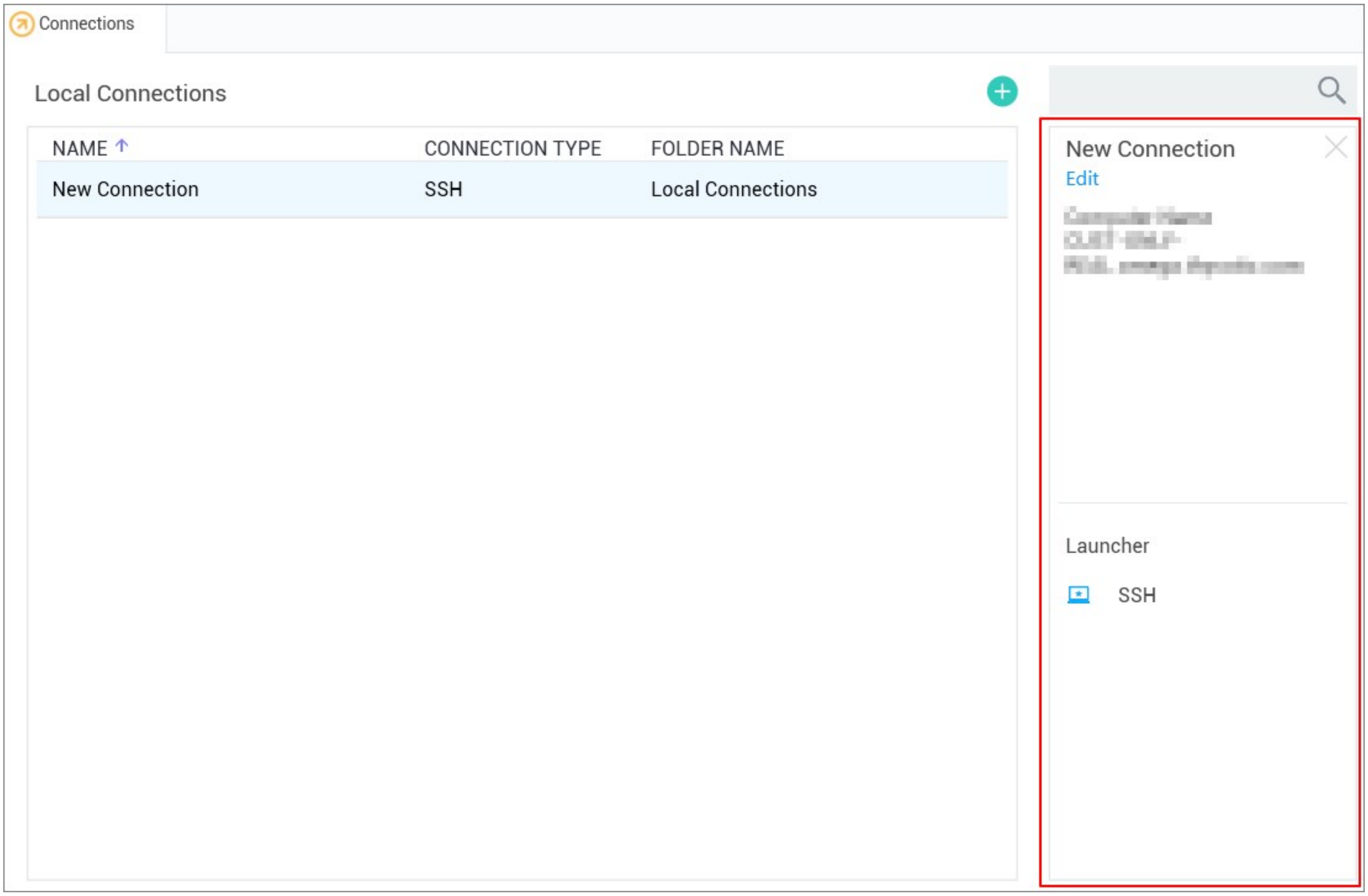
- Secret Server Connections and
- Global Configurations.

The ‹ can be used to collapse and › expand the Navigation menu.

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.

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.



Local Connections

NAME ↑	CONNECTION TYPE	FOLDER NAME
New Connection	SSH	Local Connections

New Connection

[redacted]

Launcher

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

There are several menu types available within the user interface:

Stack Menu

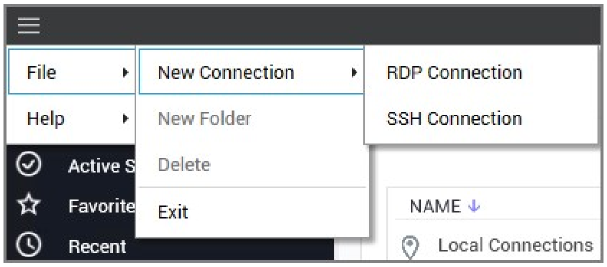
The menu at the top left of the application allows you to select File and Help.

☰

File

Under File you can do the following:

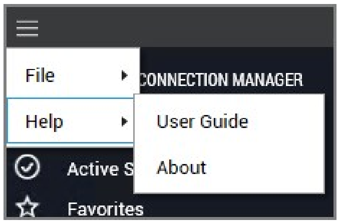
- Create new connections (RDP or SSH)
- Create new folders
- Delete folders/connections
- Exit the application

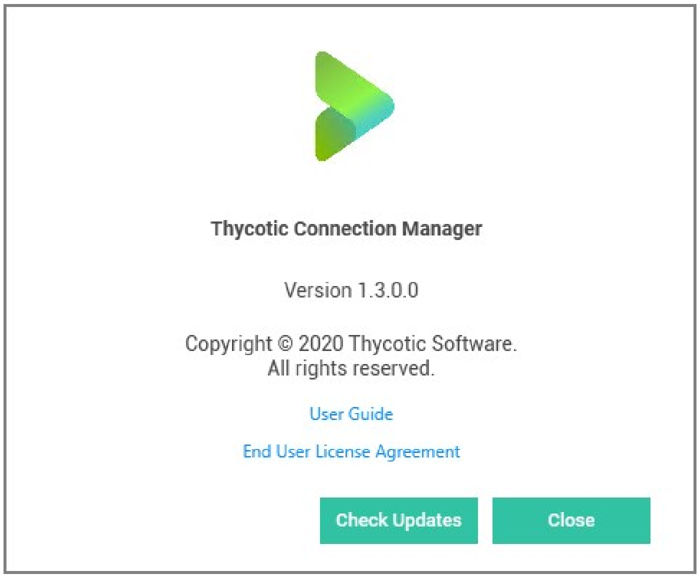


> **NOTE**: The Stack menu is context sensitive so the available, displayed options depend on what is currently selected in the navigation tree or the main work area.

Help

Under Help you can select User Guide and About:





Thycotic Connection Manager

Version 1.3.0.0

Copyright © 2020 Thycotic Software.
All rights reserved.

User Guide

End User License Agreement

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.

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.

Secret Server Requirements

- 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 SS 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 SS and it usually means the Secret Server version # is hidden, and we receive an "Access Denied" message
- A Secret Server Username

Connect to Secret Server

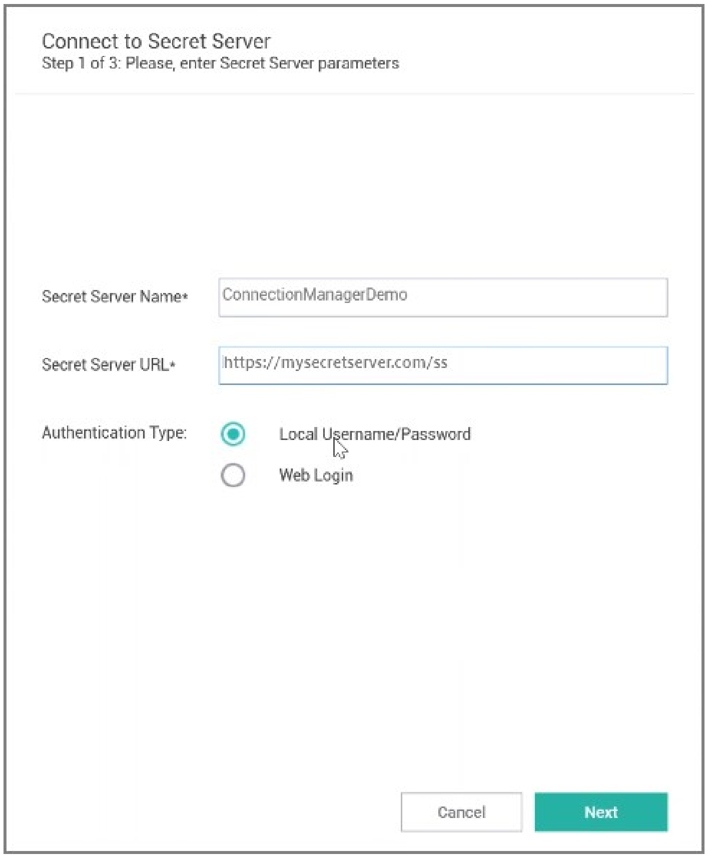
Connection Manager will only connect to Secret Server version 10.7 or later and requires a valid Secret Server license.

> **Note**: For Secret Server implementations using WinAuth, also refer to details in this article Setting Up Integrated Windows Authentication in Secret Server. Use the RestAPI to use the auth method instead of WinAuth.
>
> If you encounter an invocation error refer to Invocation Error when Connecting to Secret Server.

1. On the Configuration menu, select **Secret Server Connections**.

   If no Secret Server connections exist in Connection Manager, selecting the Secret Server Connections option opens *Step 1: Connect to Secret Server*. If other Secret Server connections exist, the Secret Server Connections window opens instead.

2. On the **Secret Server Connections** window select **Add a Connection**. The Secret Server connection wizard opens.



Connect to Secret Server
Step 1 of 3: Please, enter Secret Server parameters

Secret Server Name*: ConnectionManagerDemo

Secret Server URL*: https://mysecretserver.com/ss

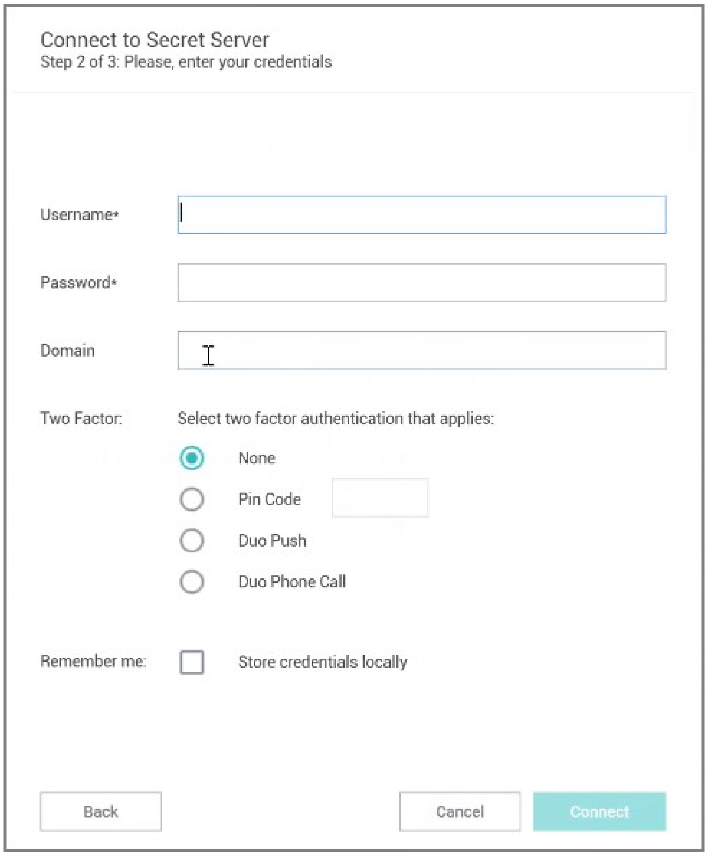
Authentication Type: ● Local Username/Password ○ Web Login

   1. Complete Step 1 required fields, including:

      - **Secret Server Name**: A friendly name for the connection.
      - **Secret Server URL**: The URL for the Secret Server instance, usually https://<Server Name>/SecretServer.
      - **Authentication Type**: Select **Local Username/Password**.

   Click **Next**.

3. On the Step 2 of 3 dialog complete:



Connect to Secret Server
Step 2 of 3: Please, enter your credentials

Username*
Password*
Domain
Two Factor: Select two factor authentication that applies:
● None
○ Pin Code
○ Duo Push
○ Duo Phone Call

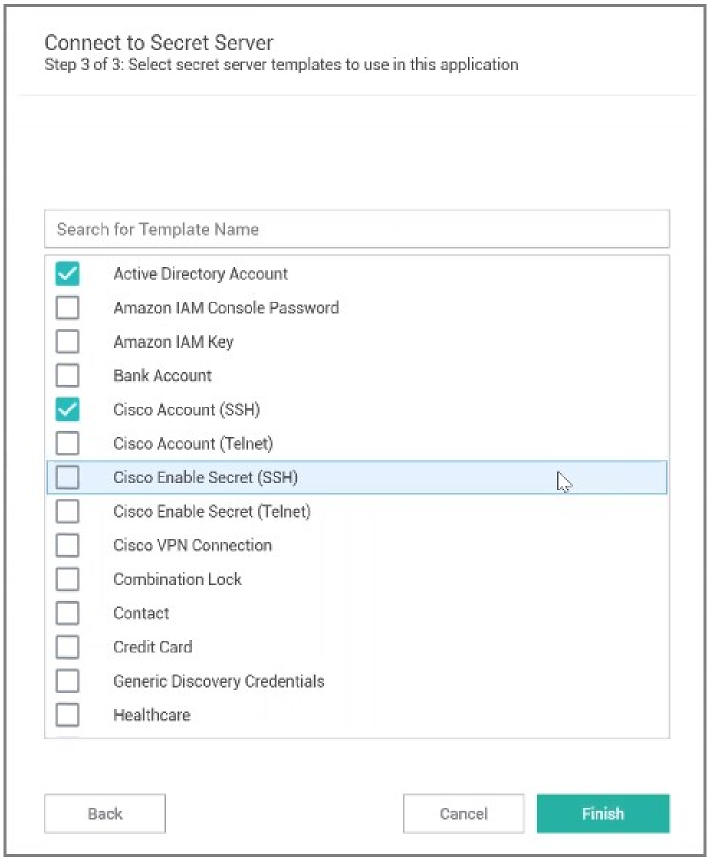
Remember me: □ Store credentials locally

   - **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.
   - **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.

   Click **Connect**.

4. For Step 3 of 3, the system automatically fetches a list of Secret templates from the Secret Server URL provided in step 1 of 3. The most common templates for RDP and SSH sessions are selected by default. You may select and deselect additional templates as needed, and you may also search for a specific template by name.



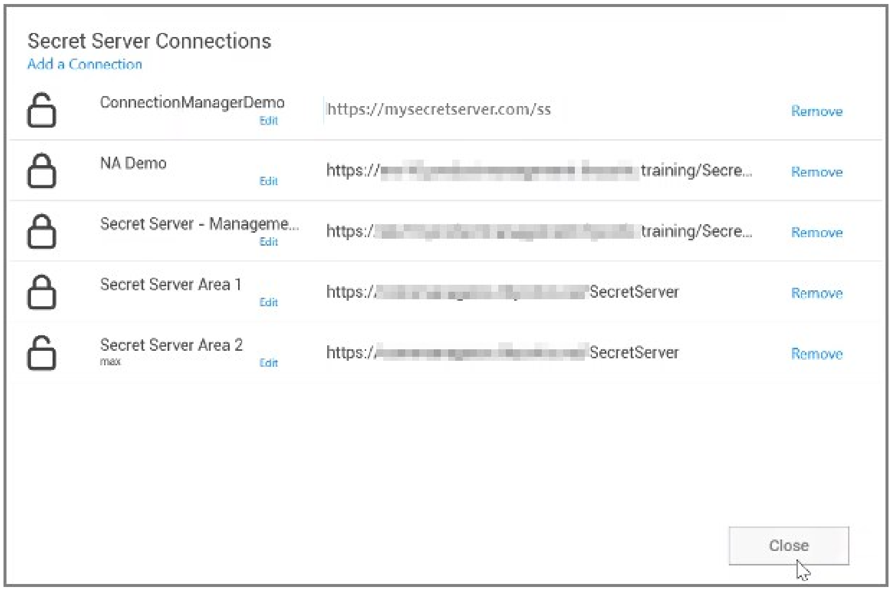
Connect to Secret Server
Step 3 of 3: Select secret server templates to use in this application

Search for Template Name

- ☑ Active Directory Account
- □ Amazon IAM Console Password
- □ Amazon IAM Key
- □ Bank Account
- ☑ Cisco Account (SSH)
- □ Cisco Account (Telnet)
- □ Cisco Enable Secret (SSH)
- □ Cisco Enable Secret (Telnet)
- □ Cisco VPN Connection
- □ Combination Lock
- □ Contact
- □ Credit Card
- □ Generic Discovery Credentials
- □ Healthcare

5. Click **Finish** once all desired templates have been selected.

The Secret Server Connections dialog shows the list of connections, with the authenticated one as unlocked.



Secret Server Connections
Add a Connection

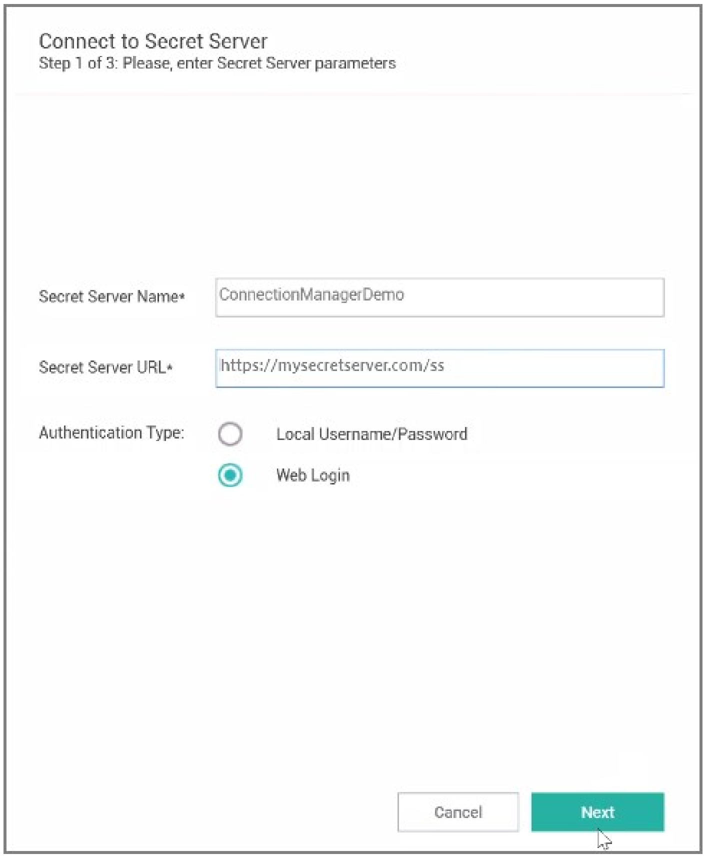
🔓	ConnectionManagerDemo Edit	https://mysecretserver.com/ss	Remove
🔒	NA Demo Edit	https://[redacted]training/Secre...	Remove
🔒	Secret Server - Manageme... Edit	https://[redacted]training/Secre...	Remove
🔒	Secret Server Area 1 Edit	https://[redacted]SecretServer	Remove
🔓	Secret Server Area 2 max Edit	https://[redacted]SecretServer	Remove

The connection is also added to the navigation menu with an open lock icon to the left.

Note: Secret Server connections will persist between sessions of Connection Manager; however, users must re-authenticate the connection after the application is launched, or following a session timeout.

If you are using SAML, follow these steps:

1. On the **Secret Server Connections** window select **Add a Connection**. The Secret Server connection wizard opens.



Connect to Secret Server
Step 1 of 3: Please, enter Secret Server parameters

Secret Server Name*: ConnectionManagerDemo

Secret Server URL*: https://mysecretserver.com/ss

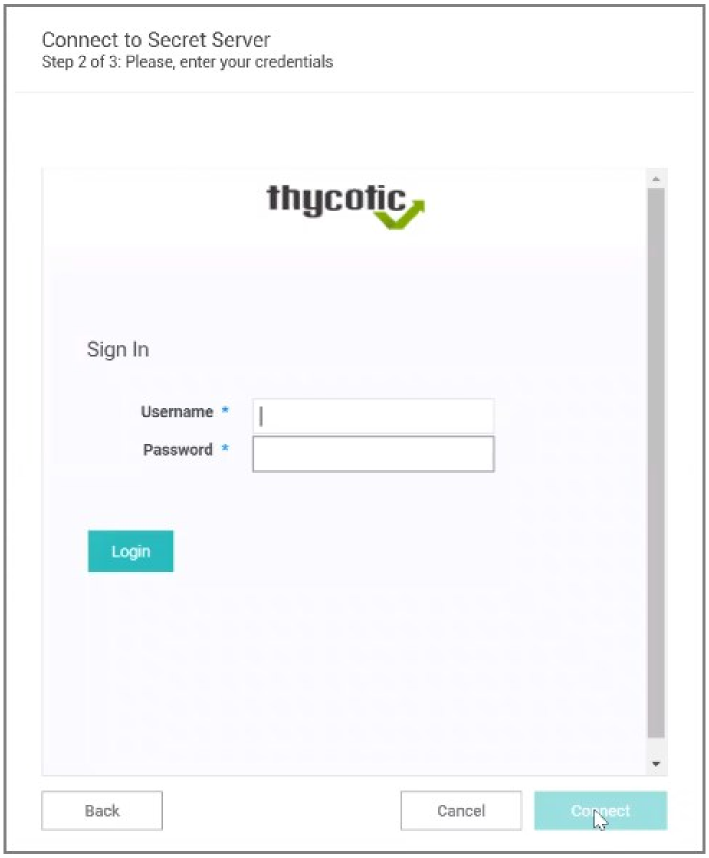
Authentication Type: ○ Local Username/Password ● Web Login

   1. Complete Step 1 required fields, including:

      - **Secret Server Name**: A friendly name for the connection.
      - **Secret Server URL**: The URL for the Secret Server instance, usually https://<Server Name>/SecretServer.
      - **Authentication Type**: Select **Web Login**.

   Click **Next**.

2. On the Step 2 of 3 dialog complete:



Connect to Secret Server

Step 2 of 3: Please, enter your credentials

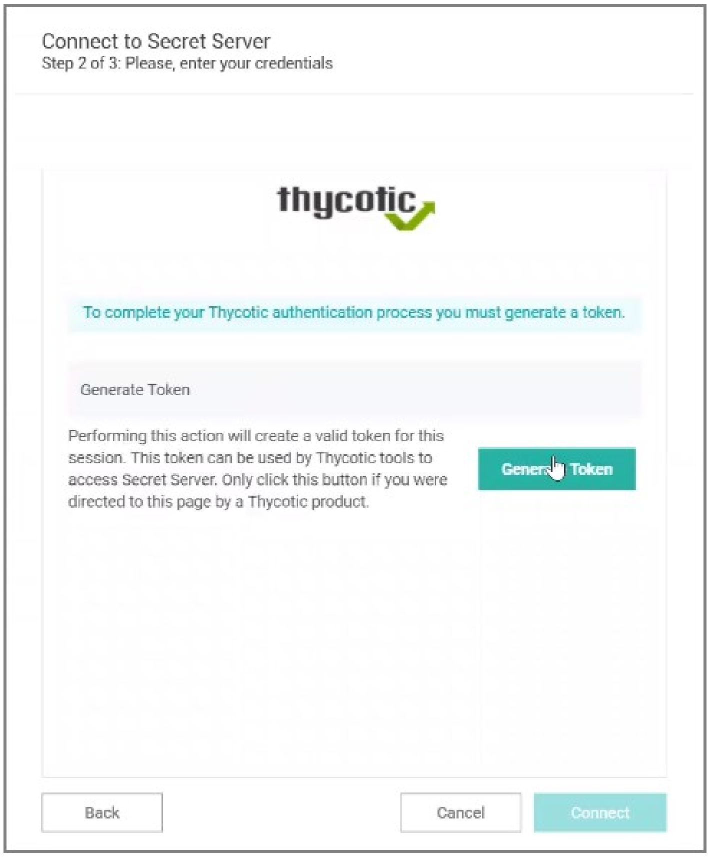
Sign In

Username *

Password *

- **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.

1. Click **Login**.
2. Click **Generate Token**.



Connect to Secret Server
Step 2 of 3: Please, enter your credentials

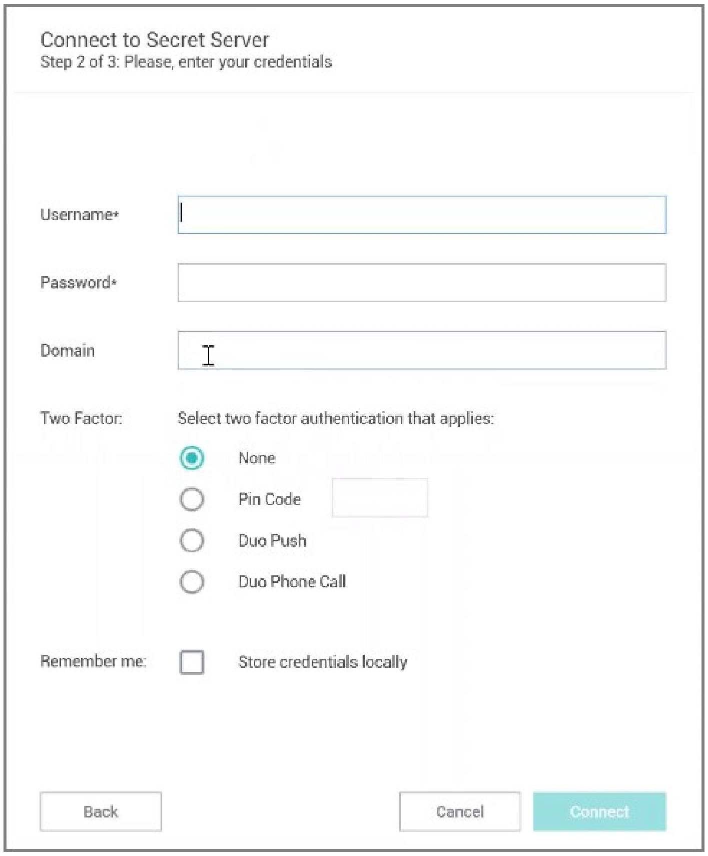
To complete your Thycotic authentication process you must generate a token.

Generate Token

Performing this action will create a valid token for this session. This token can be used by Thycotic tools to access Secret Server. Only click this button if you were directed to this page by a Thycotic product.

Click **Connect**.

3. For Step 3 of 3, the system automatically fetches a list of Secret templates from the Secret Server URL provided in step 1 of 3. The most common templates for RDP and SSH sessions are selected by default. You may select and deselect additional templates as needed, and you may also search for a specific template by name.



Connect to Secret Server
Step 2 of 3: Please, enter your credentials

Username*

Password*

Domain

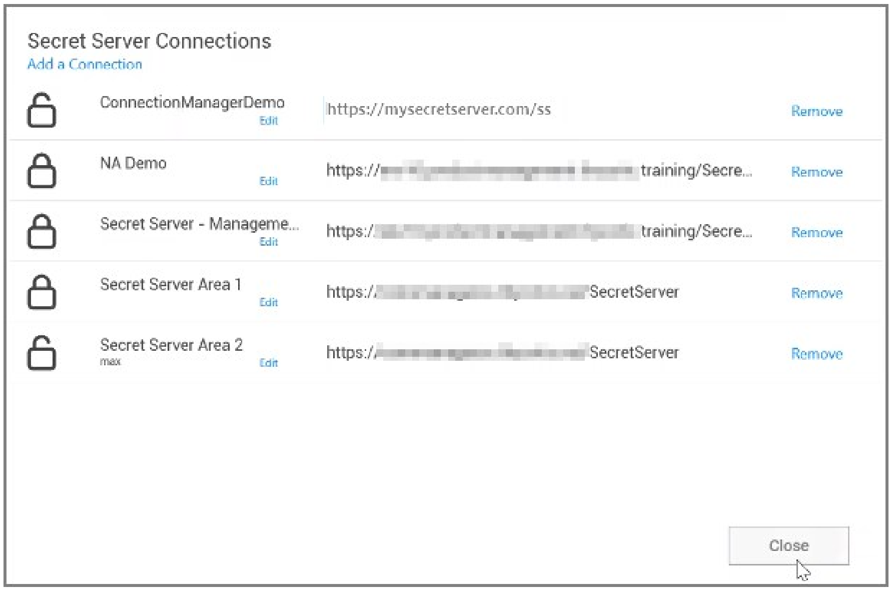
Two Factor: Select two factor authentication that applies:

● None
○ Pin Code
○ Duo Push
○ Duo Phone Call

Remember me: □ Store credentials locally

4. Click **Finish** once all desired templates have been selected.

The Secret Server Connections dialog shows the list of connections, with the authenticated one as unlocked.



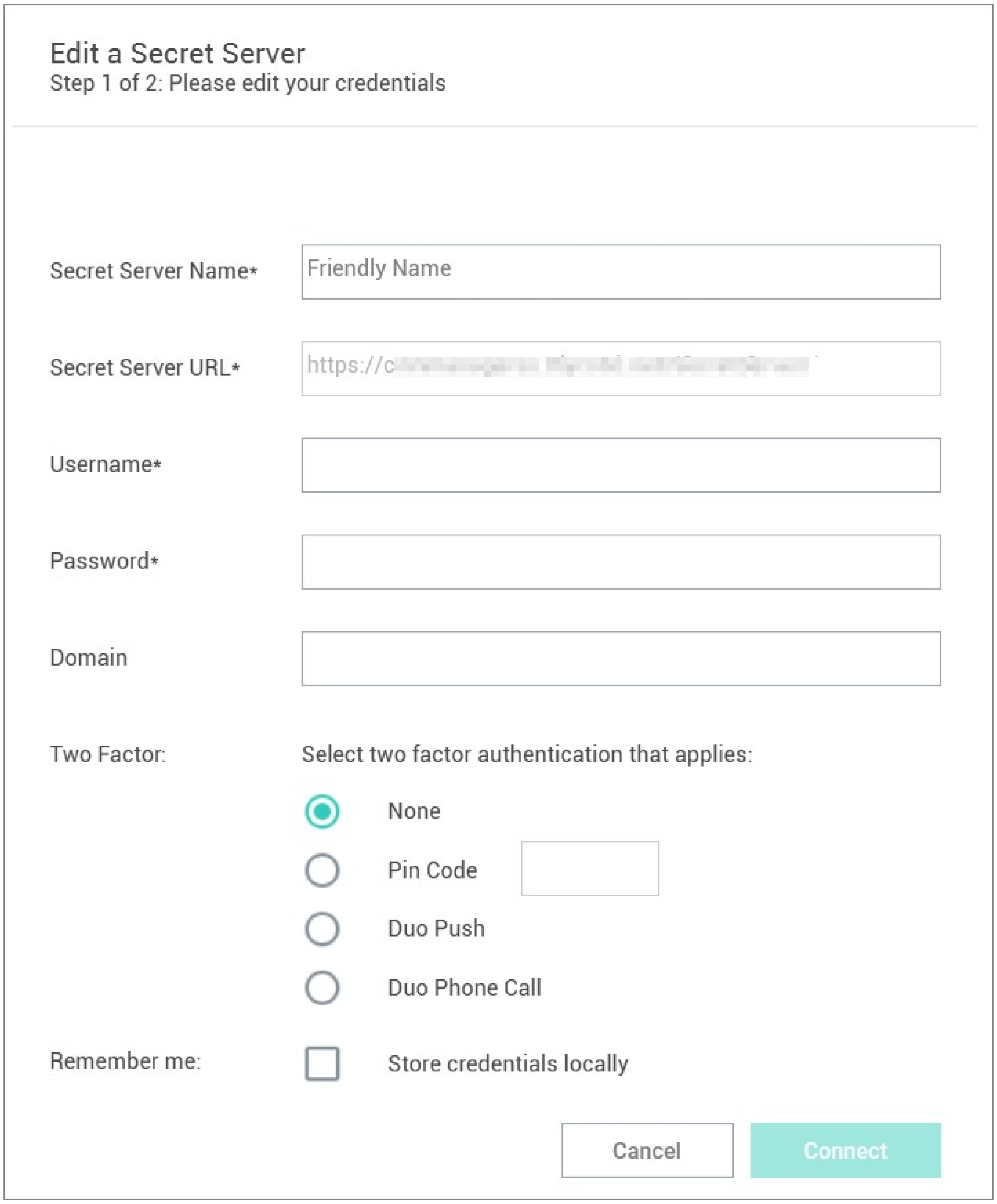
Secret Server Connections
Add a Connection

ConnectionManagerDemo Edit	https://mysecretserver.com/ss	Remove
NA Demo Edit	https://[redacted]training/Secre...	Remove
Secret Server - Manageme... Edit	https:/[redacted]training/Secre...	Remove
Secret Server Area 1 Edit	https:/[redacted]SecretServer	Remove
Secret Server Area 2 max Edit	https:/[redacted]SecretServer	Remove

Modify a Connection

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.



Edit a Secret Server

Step 1 of 2: Please edit your credentials

Secret Server Name* Friendly Name

Secret Server URL* https://c[redacted]

Username*

Password*

Domain

Two Factor: Select two factor authentication that applies:

● None

○ Pin Code

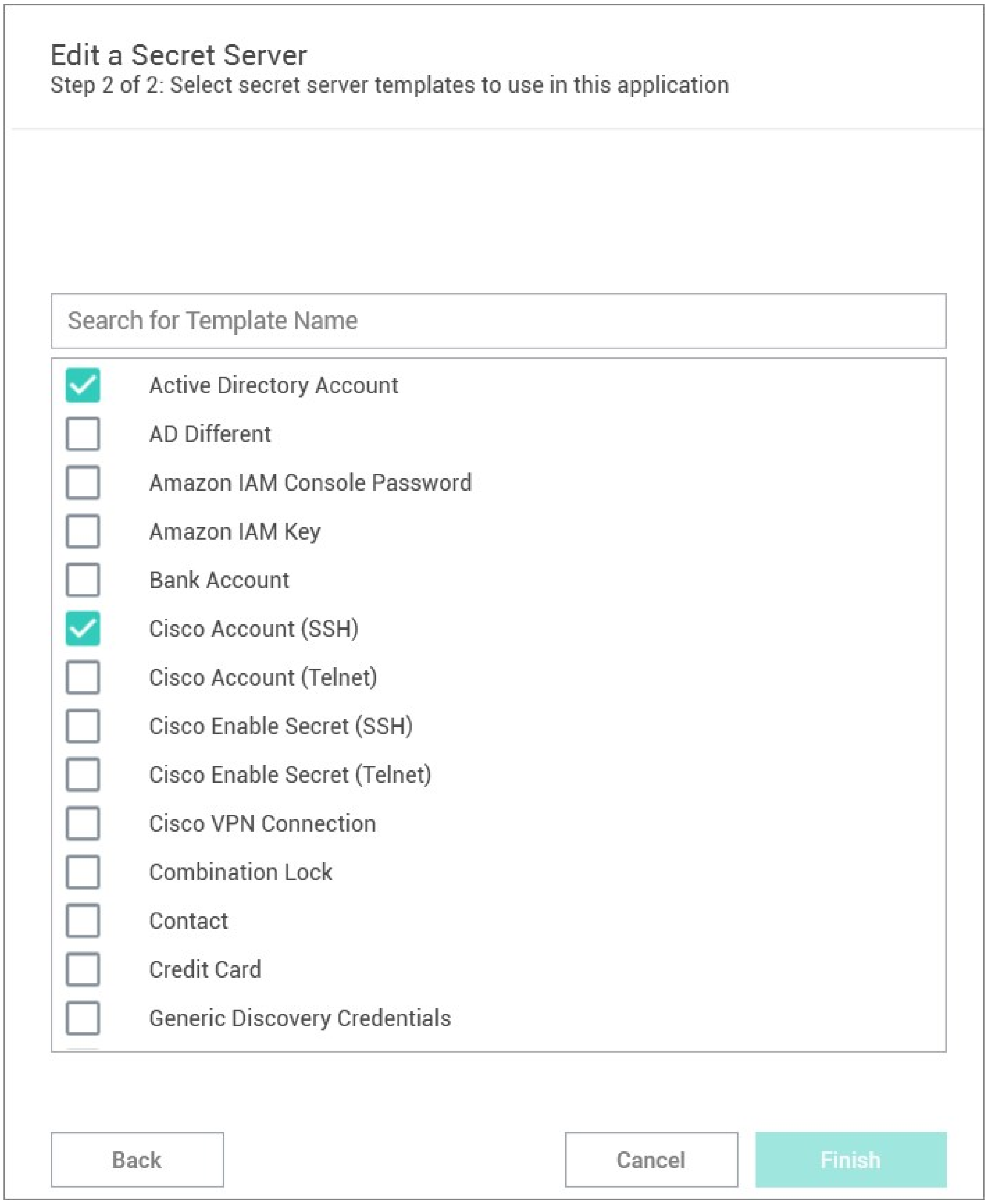
○ Duo Push

○ Duo Phone Call

Remember me: □ Store credentials locally

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.

3. Make any desired changes in Step 1 and click **Connect**.



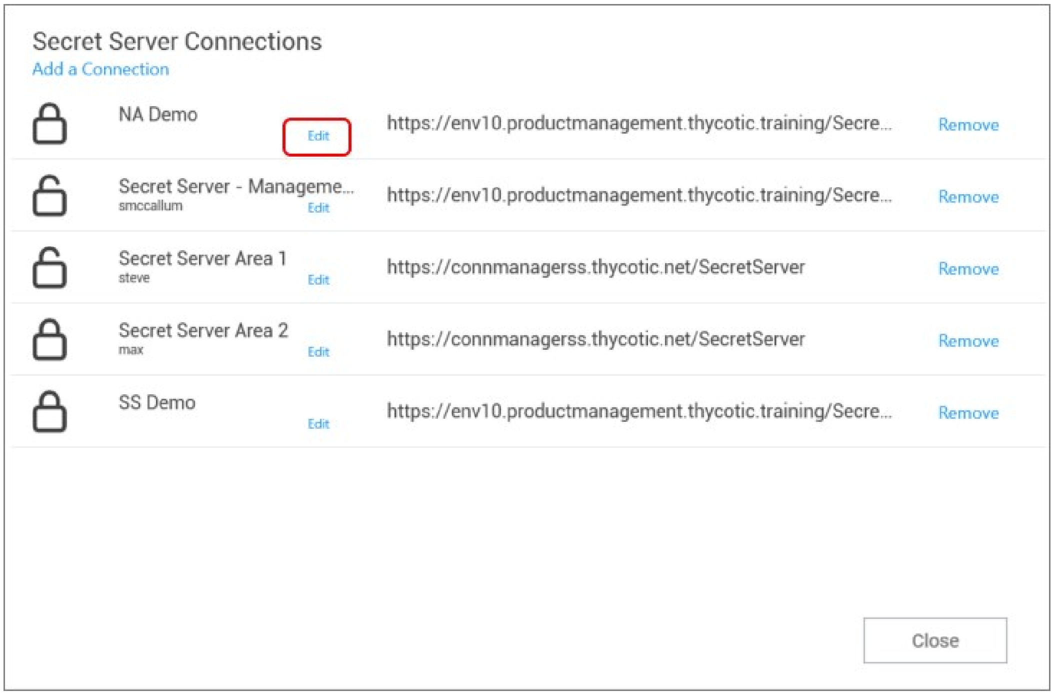
Edit a Secret Server

Step 2 of 2: Select secret server templates to use in this application

☑ Active Directory Account
□ AD Different
□ Amazon IAM Console Password
□ Amazon IAM Key
□ Bank Account
☑ Cisco Account (SSH)
□ Cisco Account (Telnet)
□ Cisco Enable Secret (SSH)
□ Cisco Enable Secret (Telnet)
□ Cisco VPN Connection
□ Combination Lock
□ Contact
□ Credit Card
□ Generic Discovery Credentials

4. Make any desired changes in Step 2 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.



Secret Server Connections

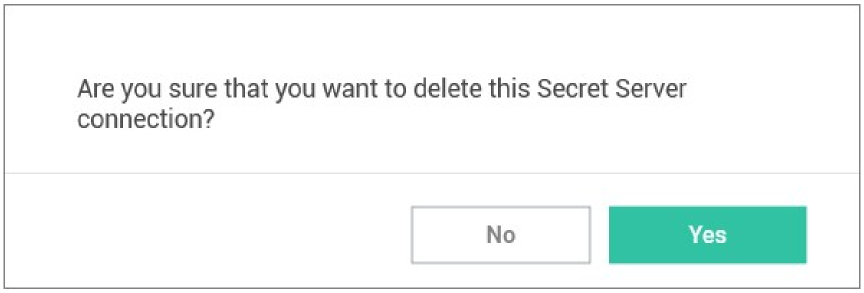
Add a Connection

NA Demo	Edit	https://env10.productmanagement.thycotic.training/Secre...	Remove
Secret Server - Manageme... smccallum	Edit	https://env10.productmanagement.thycotic.training/Secre...	Remove
Secret Server Area 1 steve	Edit	https://connmanagerss.thycotic.net/SecretServer	Remove
Secret Server Area 2 max	Edit	https://connmanagerss.thycotic.net/SecretServer	Remove
SS Demo	Edit	https://env10.productmanagement.thycotic.training/Secre...	Remove

Remove a Connection

To remove a connection:

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.



Are you sure that you want to delete this Secret Server connection?

3. Click **Yes** to confirm.

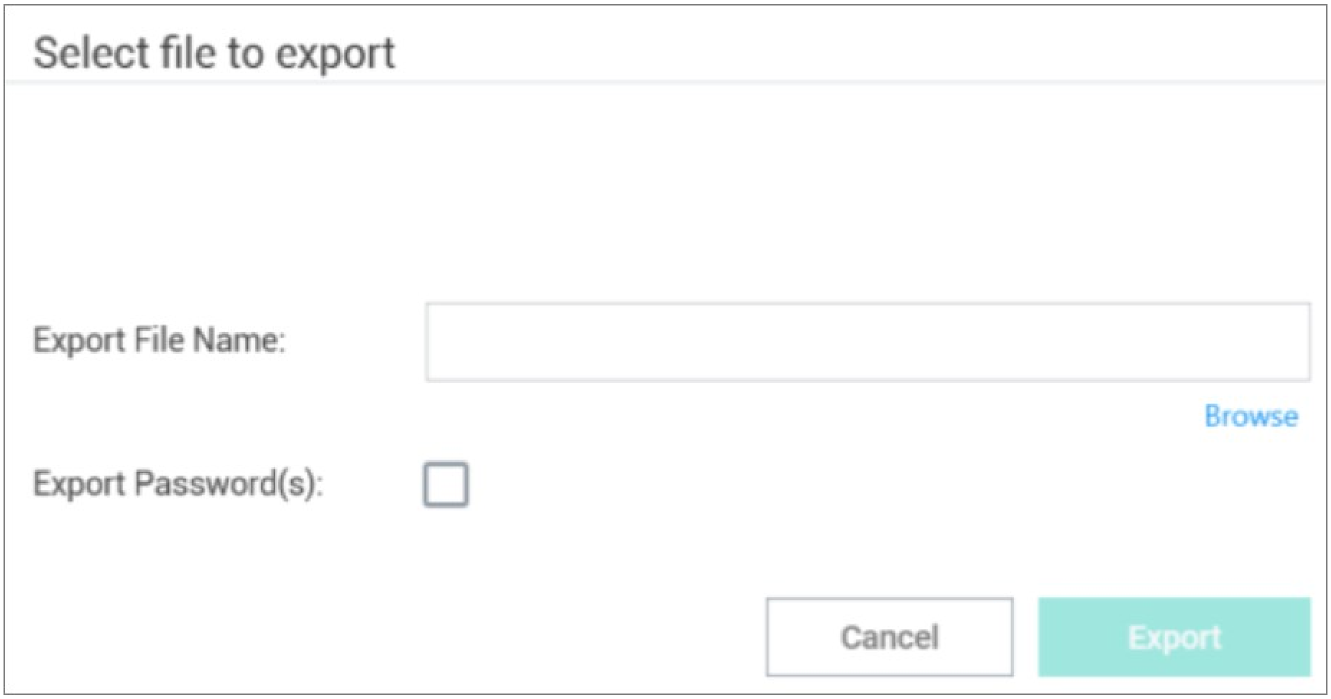
The following topics are available:

- Export Connections
- JSON based Import of Connections
- CSV based Import of Local 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.



Select file to export

Export File Name:

Export Password(s): □

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.

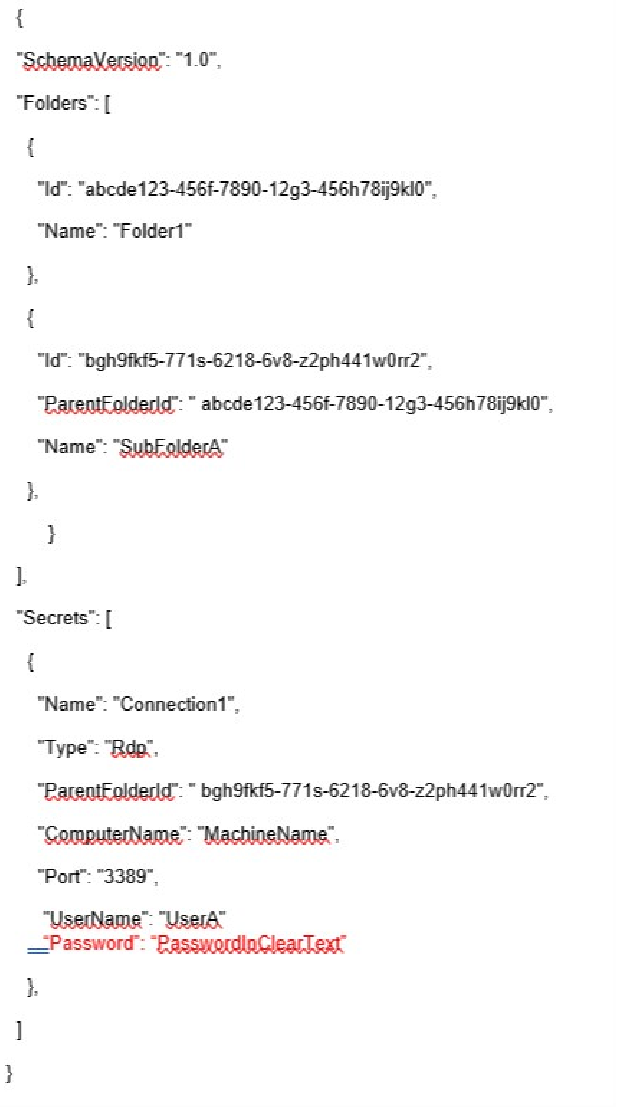
The Import option is only available for Local connections and can only be accessed from the Navigation tree.

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:



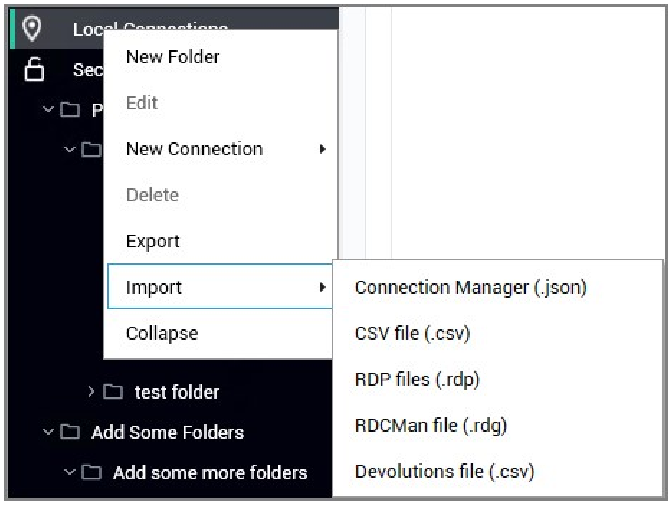
```
{
"SchemaVersion": "1.0",
"Folders": [
 {
  "Id": "abcde123-456f-7890-12g3-456h78ij9kl0",
  "Name": "Folder1"
 },
 {
  "Id": "bgh9fkf5-771s-6218-6v8-z2ph441w0rr2",
  "ParentFolderId": " abcde123-456f-7890-12g3-456h78ij9kl0",
  "Name": "SubFolderA"
 },
    }
],
"Secrets": [
 {
  "Name": "Connection1",
  "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.

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**.

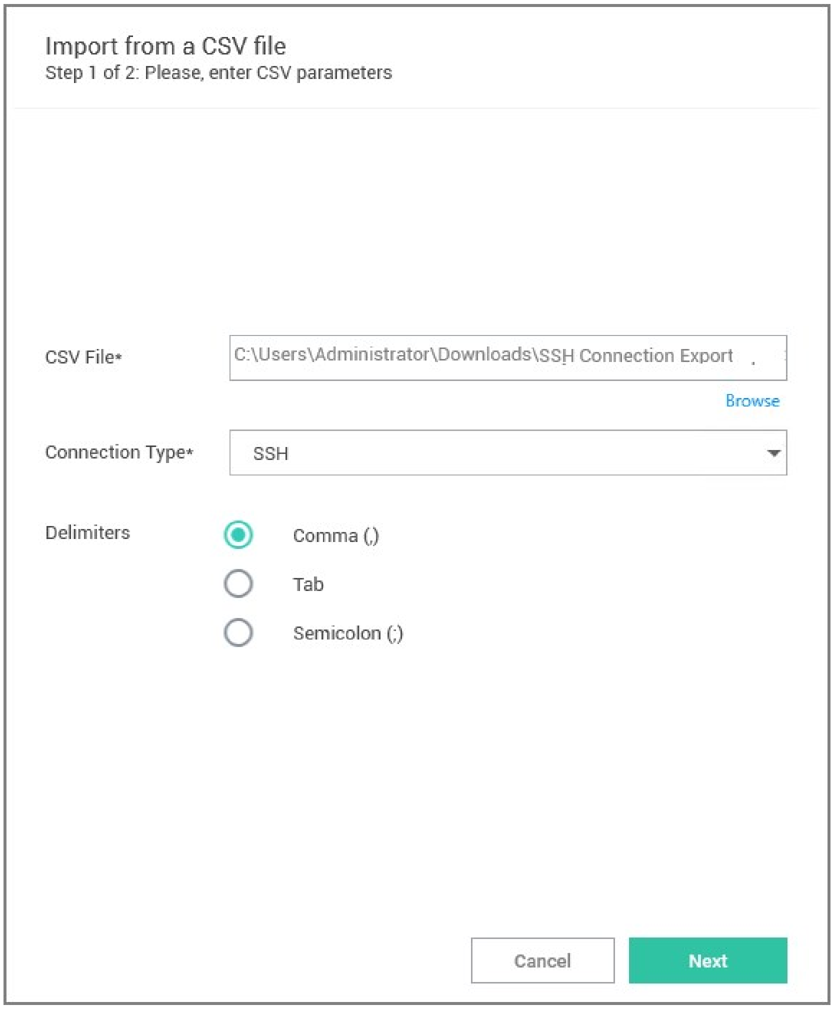


3. Select from the import options available based on your source file.

Importing Local Connection Data

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,
   1. select the file to import,
   2. specify the connection type, and
   3. 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* C:\Users\Administrator\Downloads\SSH Connection Export

Connection Type* SSH

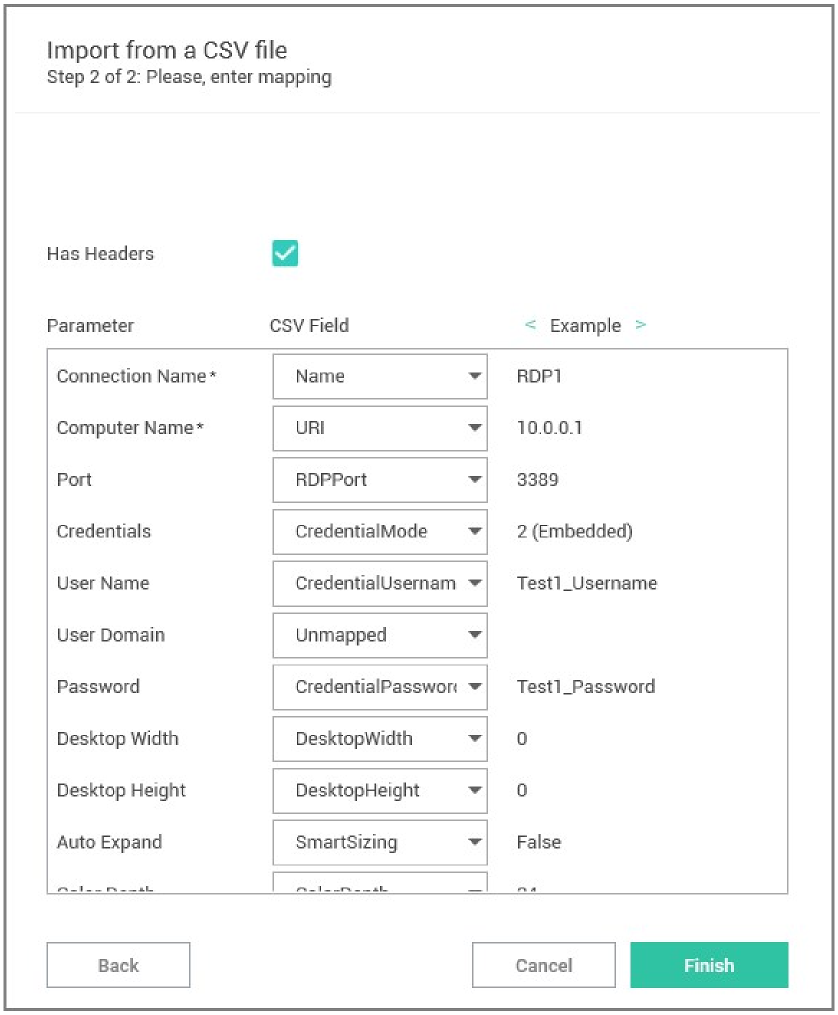
Delimiters

● Comma (,)

○ Tab

○ Semicolon (;)

2. Click **Next**.



Import from a CSV file

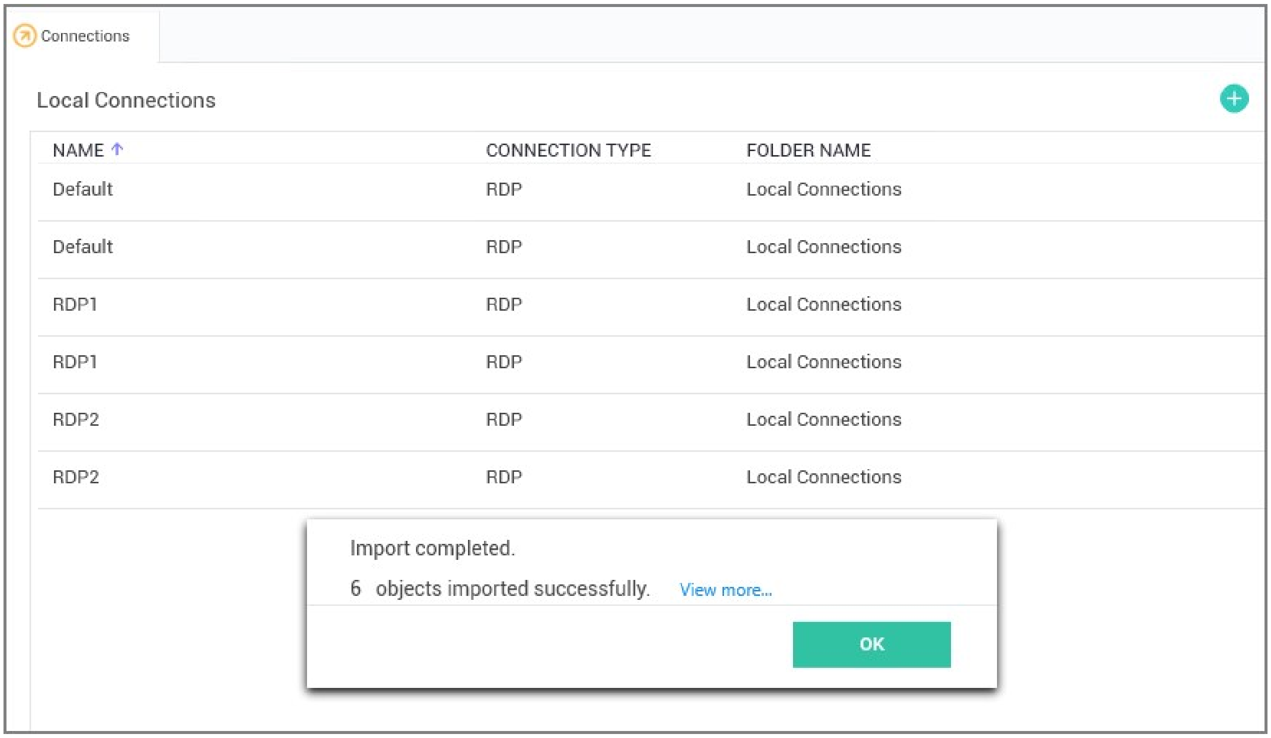
Step 2 of 2: Please, enter mapping

Has Headers ☑

Parameter	CSV Field	< Example >
Connection Name *	Name	RDP1
Computer Name *	URI	10.0.0.1
Port	RDPPort	3389
Credentials	CredentialMode	2 (Embedded)
User Name	CredentialUsernam	Test1_Username
User Domain	Unmapped	
Password	CredentialPassword	Test1_Password
Desktop Width	DesktopWidth	0
Desktop Height	DesktopHeight	0
Auto Expand	SmartSizing	False
Color Depth	ColorDepth	24

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**.



Local Connections

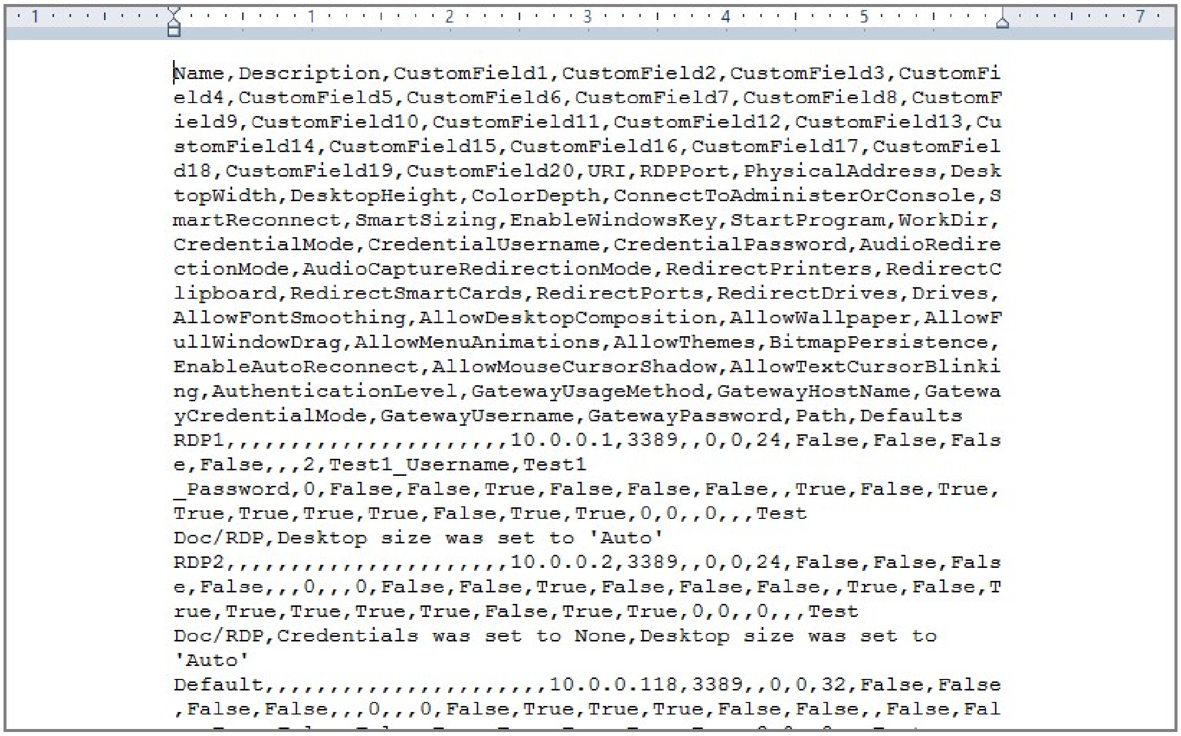
NAME ↑	CONNECTION TYPE	FOLDER NAME
Default	RDP	Local Connections
Default	RDP	Local Connections
RDP1	RDP	Local Connections
RDP1	RDP	Local Connections
RDP2	RDP	Local Connections
RDP2	RDP	Local Connections

Import completed.

6 objects imported successfully. View more...

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...**.

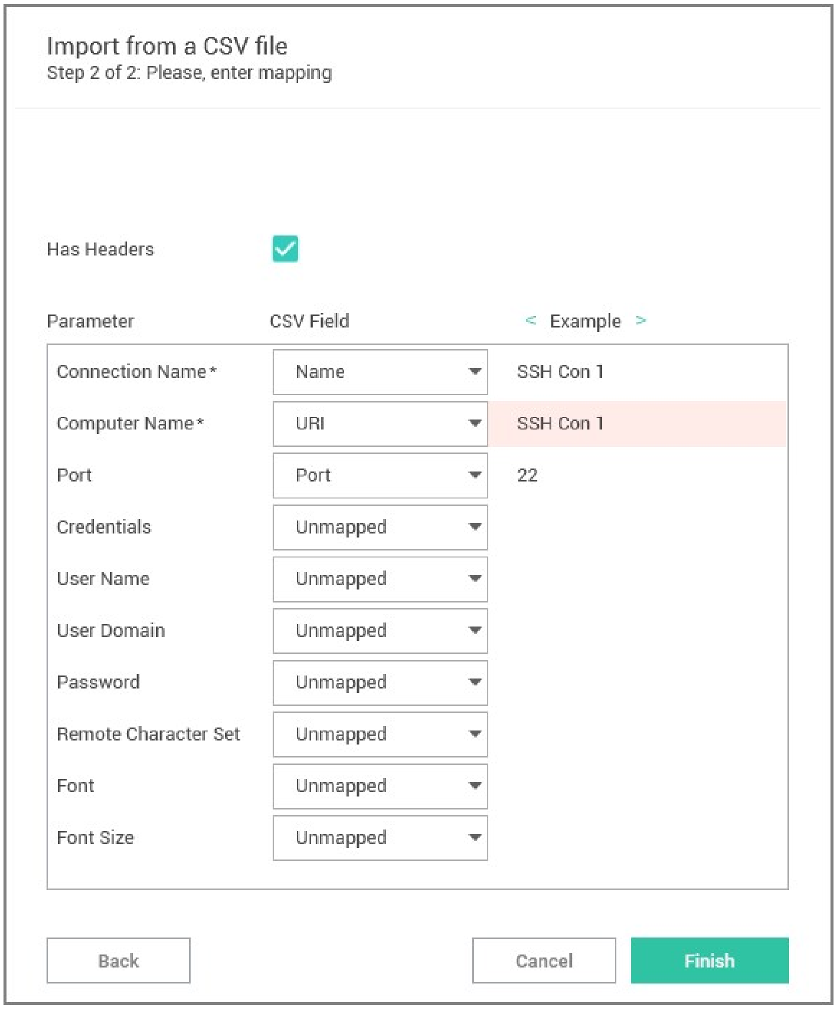


```
Name,Description,CustomField1,CustomField2,CustomField3,CustomFi
eld4,CustomField5,CustomField6,CustomField7,CustomField8,CustomF
ield9,CustomField10,CustomField11,CustomField12,CustomField13,Cu
stomField14,CustomField15,CustomField16,CustomField17,CustomFiel
d18,CustomField19,CustomField20,URI,RDPPort,PhysicalAddress,Desk
topWidth,DesktopHeight,ColorDepth,ConnectToAdministerOrConsole,S
martReconnect,SmartSizing,EnableWindowsKey,StartProgram,WorkDir,
CredentialMode,CredentialUsername,CredentialPassword,AudioRedire
ctionMode,AudioCaptureRedirectionMode,RedirectPrinters,RedirectC
lipboard,RedirectSmartCards,RedirectPorts,RedirectDrives,Drives,
AllowFontSmoothing,AllowDesktopComposition,AllowWallpaper,AllowF
ullWindowDrag,AllowMenuAnimations,AllowThemes,BitmapPersistence,
EnableAutoReconnect,AllowMouseCursorShadow,AllowTextCursorBlinki
ng,AuthenticationLevel,GatewayUsageMethod,GatewayHostName,Gatewa
yCredentialMode,GatewayUsername,GatewayPassword,Path,Defaults
RDP1,,,,,,,,,,,,,,,,,,,,,,10.0.0.1,3389,,0,0,24,False,False,Fals
e,False,,,2,Test1_Username,Test1
_Password,0,False,False,True,False,False,False,,True,False,True,
True,True,True,True,False,True,True,0,0,,0,,,Test
Doc/RDP,Desktop size was set to 'Auto'
RDP2,,,,,,,,,,,,,,,,,,,,,,10.0.0.2,3389,,0,0,24,False,False,Fals
e,False,,,0,,,0,False,False,True,False,False,False,,True,False,T
rue,True,True,True,True,False,True,True,0,0,,0,,,Test
Doc/RDP,Credentials was set to None,Desktop size was set to
'Auto'
Default,,,,,,,,,,,,,,,,,,,,,,10.0.0.118,3389,,0,0,32,False,False
,False,False,,,0,,,0,False,True,True,True,False,False,,False,Fal
```

Connection Manager saved the connection data that failed to import in a separate 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** modal.

Example of Step 2 of 2 modal showing errors:



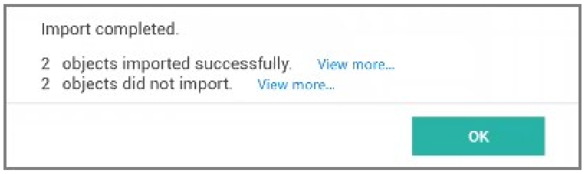
Import from a CSV file
Step 2 of 2: Please, enter mapping

Has Headers ☑

Parameter	CSV Field	< Example >
Connection Name*	Name	SSH Con 1
Computer Name*	URI	SSH Con 1
Port	Port	22
Credentials	Unmapped	
User Name	Unmapped	
User Domain	Unmapped	
Password	Unmapped	
Remote Character Set	Unmapped	
Font	Unmapped	
Font Size	Unmapped	

Import Completed Reports

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



Import completed.

2 objects imported successfully. View more...
2 objects did not import. View more...

- 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.

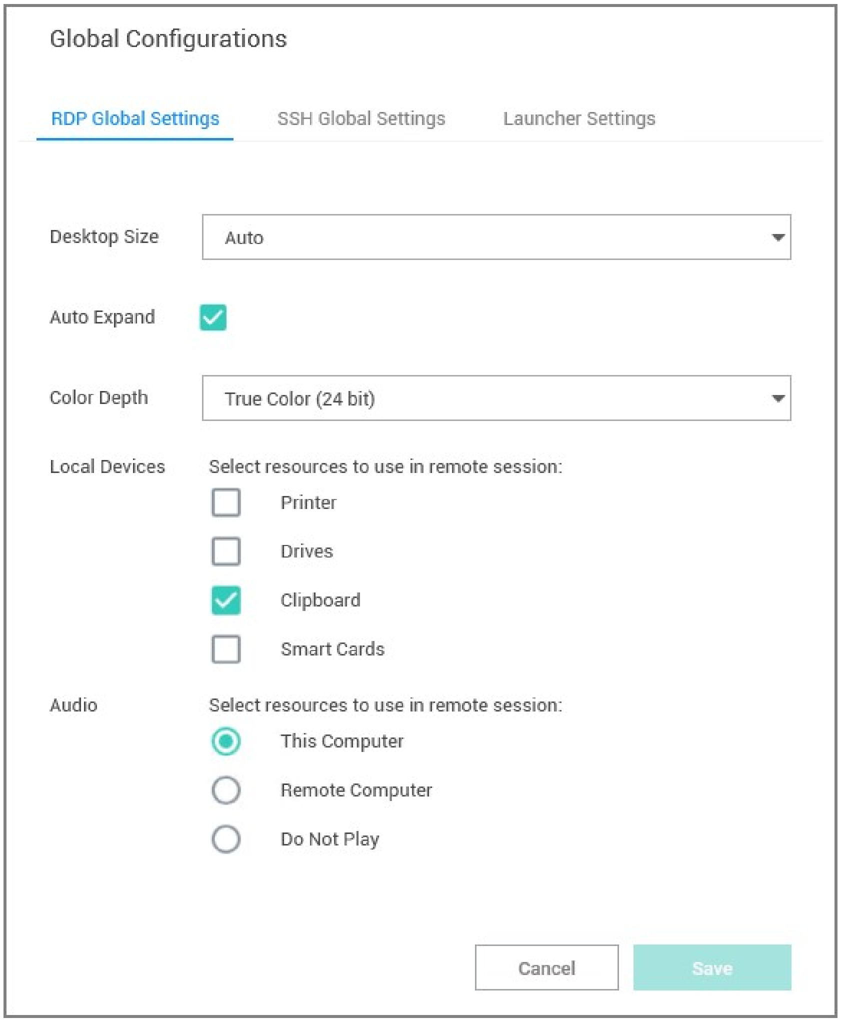
CSV Import Differences

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.

Configure Global Settings

Global Settings allows a user to control default parameter values when creating Local connections. To access:

1. On the Configuration menu, click **Global Settings**. The Global Configurations dialog box opens.



Desktop Size: Auto

Auto Expand ☑

Color Depth: True Color (24 bit)

Local Devices: Select resources to use in remote session:

- □ Printer
- □ Drives
- ☑ Clipboard
- □ Smart Cards

Audio: Select resources to use in remote session:

- ● This Computer
- ○ Remote Computer
- ○ Do Not Play

The available options are accessible via tab controls and include

- **RDP Global Settings** - allows to specify default desktop size settings, etc.
- **SSH Global Settings** - allows to specify the default font, etc.
- **Launcher Settings** - allows administrators to switch protocol handlers.

All default options may be overridden within the individual connections. Connections from Secret Server do not support all available parameters. In such cases the default parameters will be substituted.

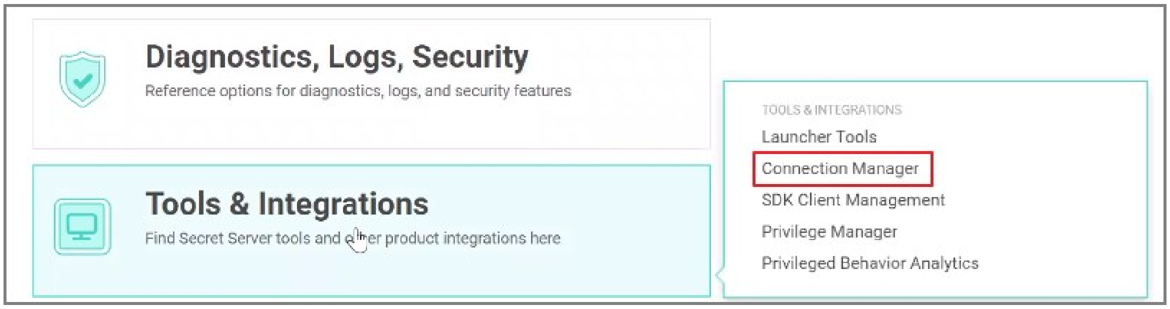
Any of the default configuration values that are specified in a Secret, from a Secret Server connection, will use the values from the Secret instead of the Global Configurations.

When accessing the Launcher Settings tab, Connection Manager checks for the legacy protocol handler. To make any changes the user needs to be an administrator. Connection Manager detects the file type version appropriately.

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

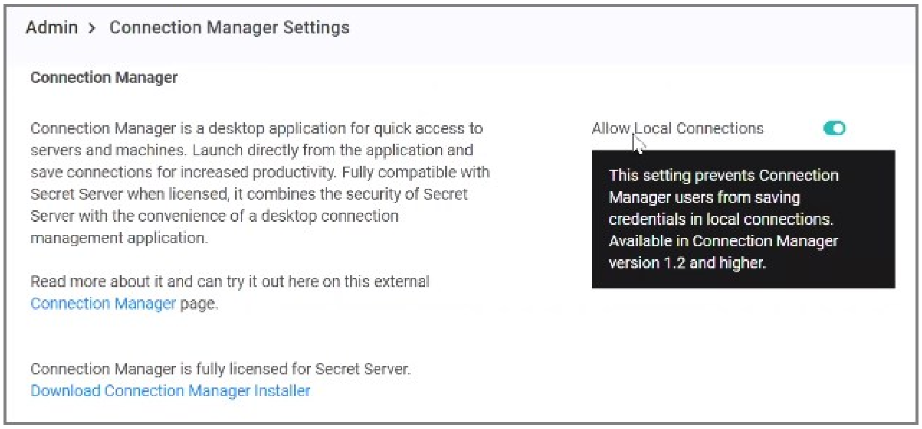
To access this in Secret Server,

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


Diagnostics, Logs, Security
Reference options for diagnostics, logs, and security features
Tools & Integrations
Find Secret Server tools and other product integrations here
TOOLS & INTEGRATIONS
Launcher Tools
Connection Manager
SDK Client Management
Privilege Manager
Privileged Behavior Analytics

These options are by default enabled:

- Allow Local Connections – Allows or disables saving credentials for any Local Connections. The default is Yes.


Admin > Connection Manager Settings

Connection Manager

Connection Manager is a desktop application for quick access to servers and machines. Launch directly from the application and save connections for increased productivity. Fully compatible with Secret Server when licensed, it combines the security of Secret Server with the convenience of a desktop connection management application.

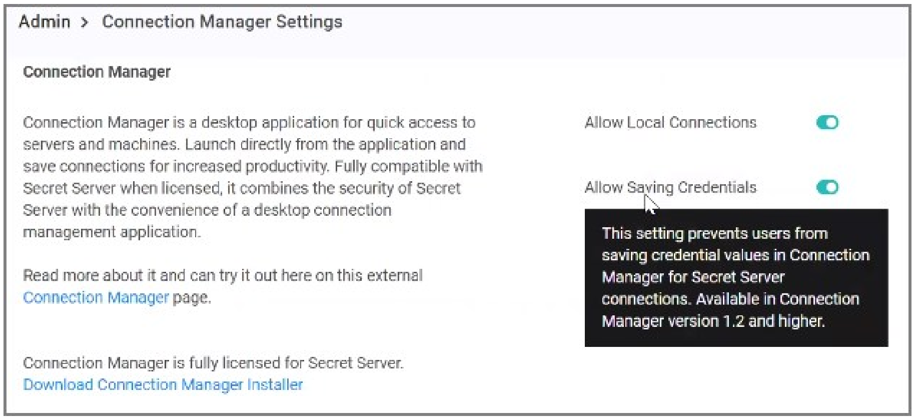
Read more about it and can try it out here on this external Connection Manager page.

Connection Manager is fully licensed for Secret Server.
Download Connection Manager Installer

Allow Local Connections

This setting prevents Connection Manager users from saving credentials in local connections. Available in Connection Manager version 1.2 and higher.

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



Admin > Connection Manager Settings

Connection Manager

Connection Manager is a desktop application for quick access to servers and machines. Launch directly from the application and save connections for increased productivity. Fully compatible with Secret Server when licensed, it combines the security of Secret Server with the convenience of a desktop connection management application.

Read more about it and can try it out here on this external Connection Manager page.

Connection Manager is fully licensed for Secret Server.
Download Connection Manager Installer

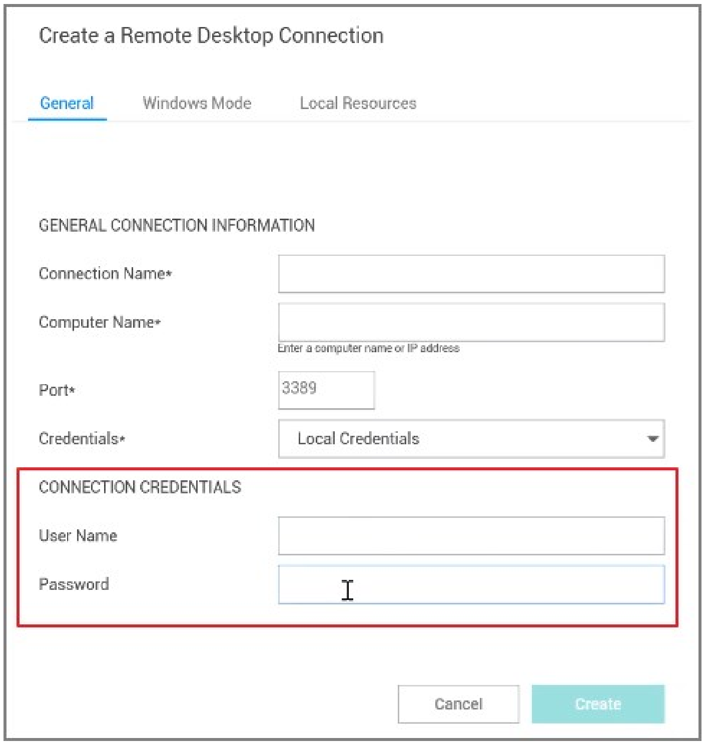
Allow Local Connections: On

Allow Saving Credentials: On

This setting prevents users from saving credential values in Connection Manager for Secret Server connections. Available in Connection Manager version 1.2 and higher.

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.



Create a Remote Desktop Connection

GENERAL CONNECTION INFORMATION

Connection Name*

Computer Name*
Enter a computer name or IP address

Port* 3389

Credentials* Local Credentials

CONNECTION CREDENTIALS

User Name

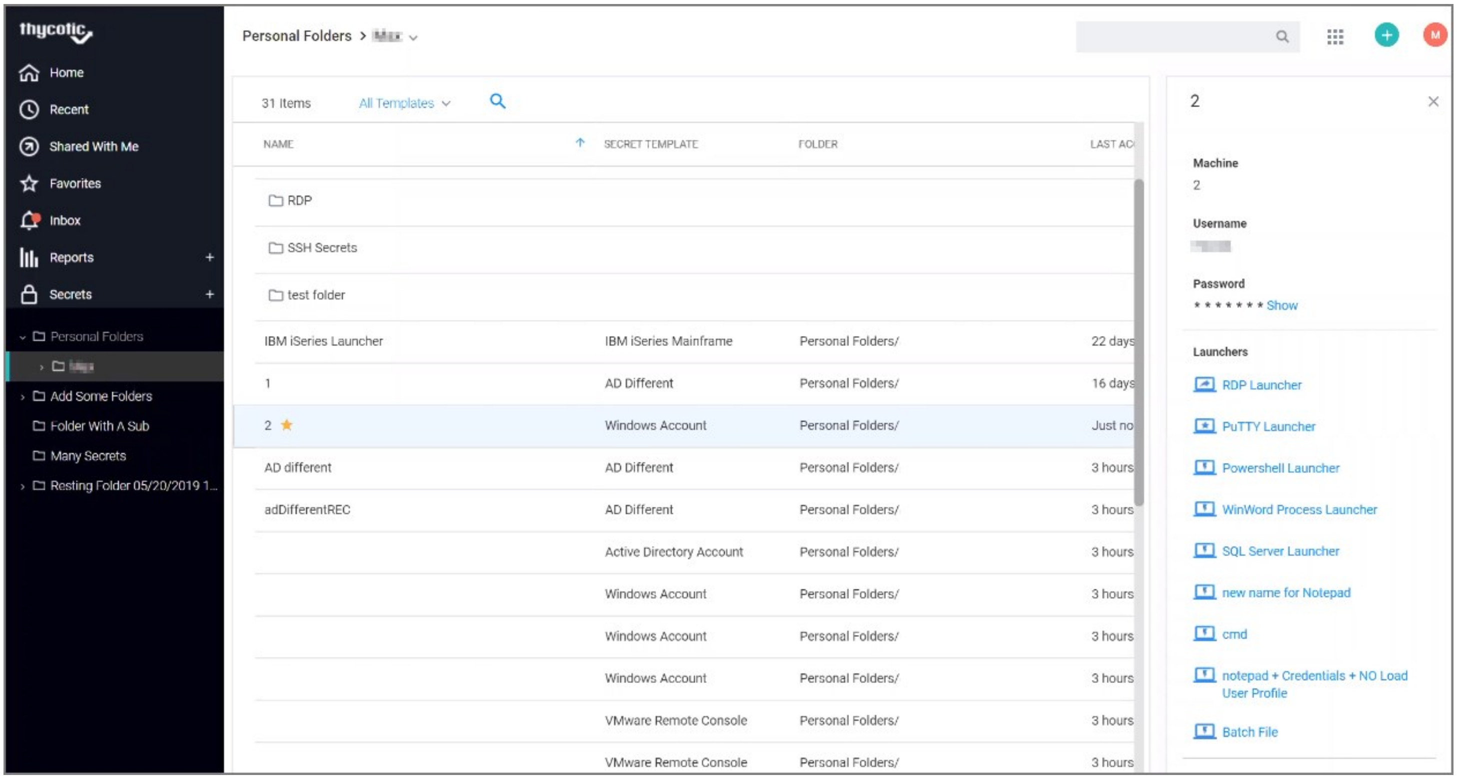
Password

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.

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.



NAME	SECRET TEMPLATE	FOLDER	LAST AC
RDP			
SSH Secrets			
test folder			
IBM iSeries Launcher	IBM iSeries Mainframe	Personal Folders/	22 days
1	AD Different	Personal Folders/	16 days
2 ★	Windows Account	Personal Folders/	Just no
AD different	AD Different	Personal Folders/	3 hours
adDifferentREC	AD Different	Personal Folders/	3 hours
	Active Directory Account	Personal Folders/	3 hours
	Windows Account	Personal Folders/	3 hours
	Windows Account	Personal Folders/	3 hours
	Windows Account	Personal Folders/	3 hours
	VMware Remote Console	Personal Folders/	3 hours
	VMware Remote Console	Personal Folders/	3 hours

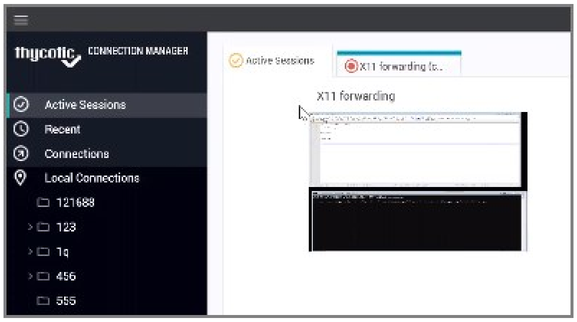
2

Machine
2

Username
[redacted]

Password
******* Show

Launchers
- RDP Launcher
- PuTTY Launcher
- Powershell Launcher
- WinWord Process Launcher
- SQL Server Launcher
- new name for Notepad
- cmd
- notepad + Credentials + NO Load User Profile
- Batch File



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.

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.

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

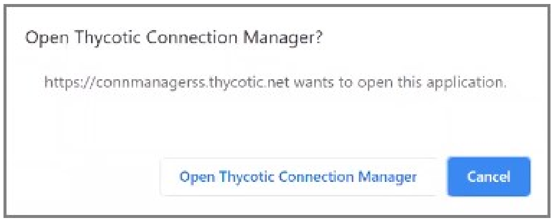
When you resize or switch to/from full screen mode in Connection Manager with an active RDP session, we disconnect and reconnect to the session so we can get the higher screen resolution settings. However, when the connection is using an **RDP Proxy**, Connection Manager is unable to auto reconnect to the session. RDP Proxy sessions generate one time passwords (OTP) when launched, and those passwords are used when making the connection. As a result, Connection Manager cannot reconnect to RDP proxy without generating a new OTP which it cannot retrieve, since the credential generation is part of the launcher process.

Resizing an RDP window inside Connection Manager does not have an impact on the connection, as the Connection Manager resolution remains the same.

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.

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.

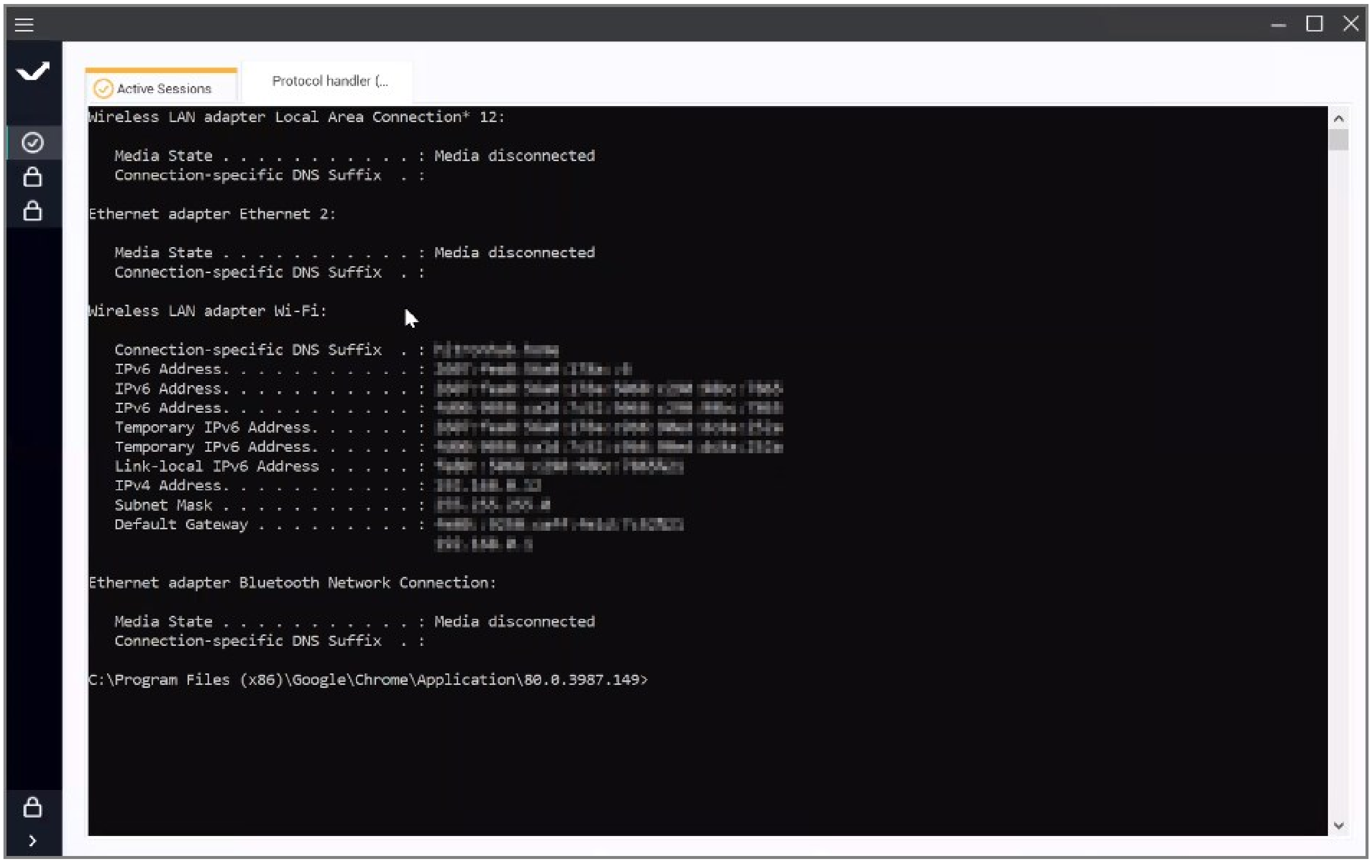
If a protocol handler is launched from Secret Server, without having an open Connection Manager, the **Open Thycotic Connection Manager?** modal opens:



Open Thycotic Connection Manager?

https://connmanagerss.thycotic.net wants to open this application.

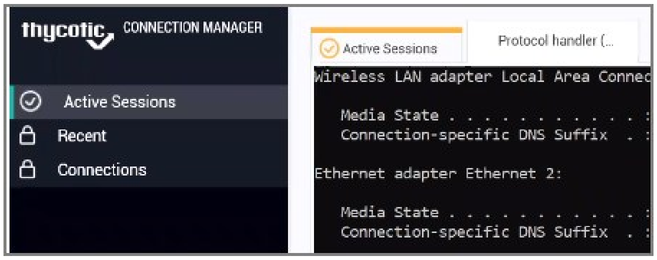
Click **Open Thycotic Connection Manager** and an active session is launched in Connection Manager:



```
Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : [redacted]
   IPv6 Address. . . . . . . . . . . : [redacted]
   IPv6 Address. . . . . . . . . . . : [redacted]
   IPv6 Address. . . . . . . . . . . : [redacted]
   Temporary IPv6 Address. . . . . . : [redacted]
   Temporary IPv6 Address. . . . . . : [redacted]
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   Default Gateway . . . . . . . . . : [redacted]

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Program Files (x86)\Google\Chrome\Application\80.0.3987.149>
```

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.

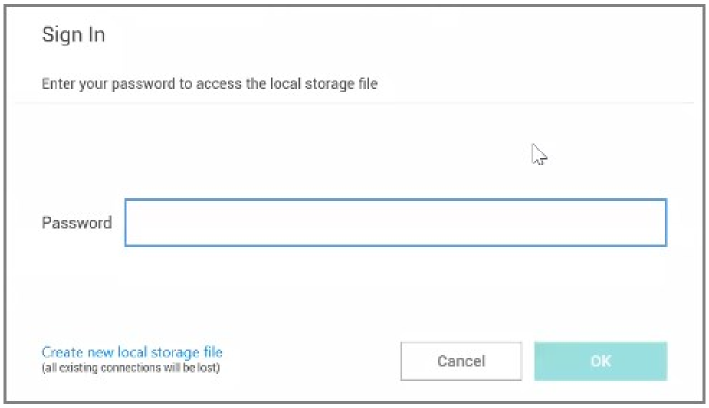


```
Wireless LAN adapter Local Area Connec

   Media State . . . . . . . . . . . :
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . :
   Connection-specific DNS Suffix  . :
```

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

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**.



Sign In

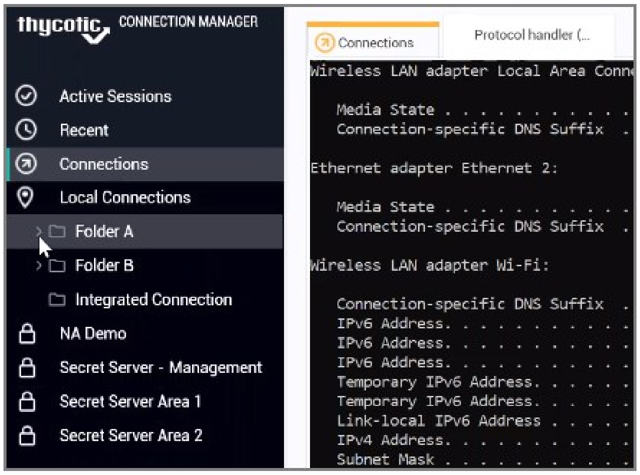
Enter your password to access the local storage file

Password

Create new local storage file
(all existing connections will be lost)
Cancel
OK

2. Enter your password.
3. Click **OK**.

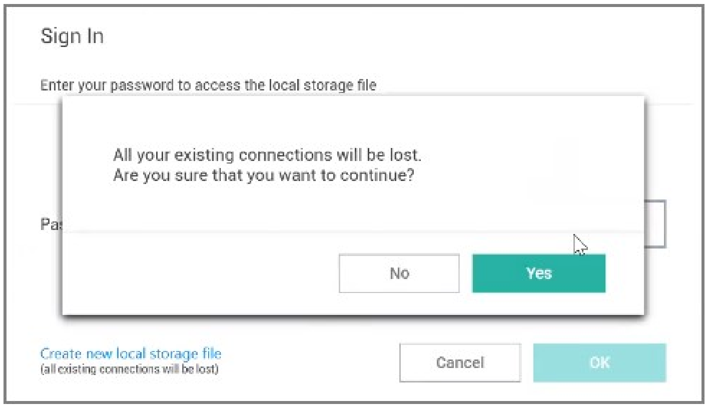
Once signed in, the user has access to all connections and all Connection Manager functionality is unlocked.



```
Wireless LAN adapter Local Area Conn

   Media State . . . . . . . . . . .
   Connection-specific DNS Suffix  .

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . .
   Connection-specific DNS Suffix  .

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  .
   IPv6 Address. . . . . . . . . . .
   IPv6 Address. . . . . . . . . . .
   IPv6 Address. . . . . . . . . . .
   Temporary IPv6 Address. . . . . .
   Temporary IPv6 Address. . . . . .
   Link-local IPv6 Address . . . . .
   IPv4 Address. . . . . . . . . . .
   Subnet Mask . . . . . . . . . . .
```

Create 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 modal:



Sign In

Enter your password to access the local storage file

All your existing connections will be lost.
Are you sure that you want to continue?

Pa
No
Yes
Create new local storage file
(all existing connections will be lost)
Cancel
OK

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

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.

- Create, edit or delete a folder
- Connection to Remote Systems
- Integrated Connections
- Re-authenticate to Secret Server
- Log File Location

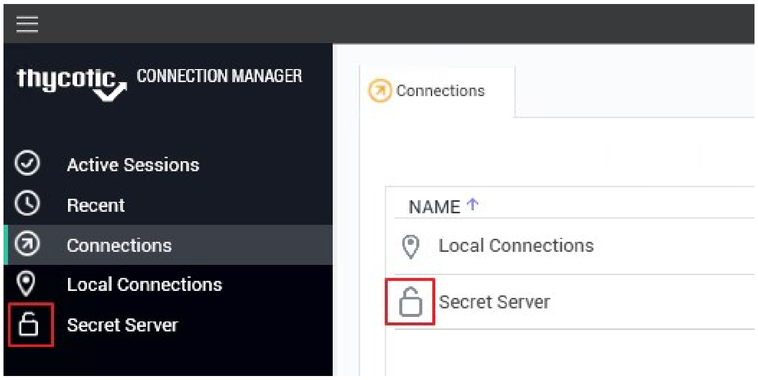
The following Connections related topics are available:

- Re-authenticate
- Remote connections
- Integrated connections

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

To re-authenticate 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**.



Create a New Connection to Remote Systems

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).

   Dependent 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 for additional information on credentials.

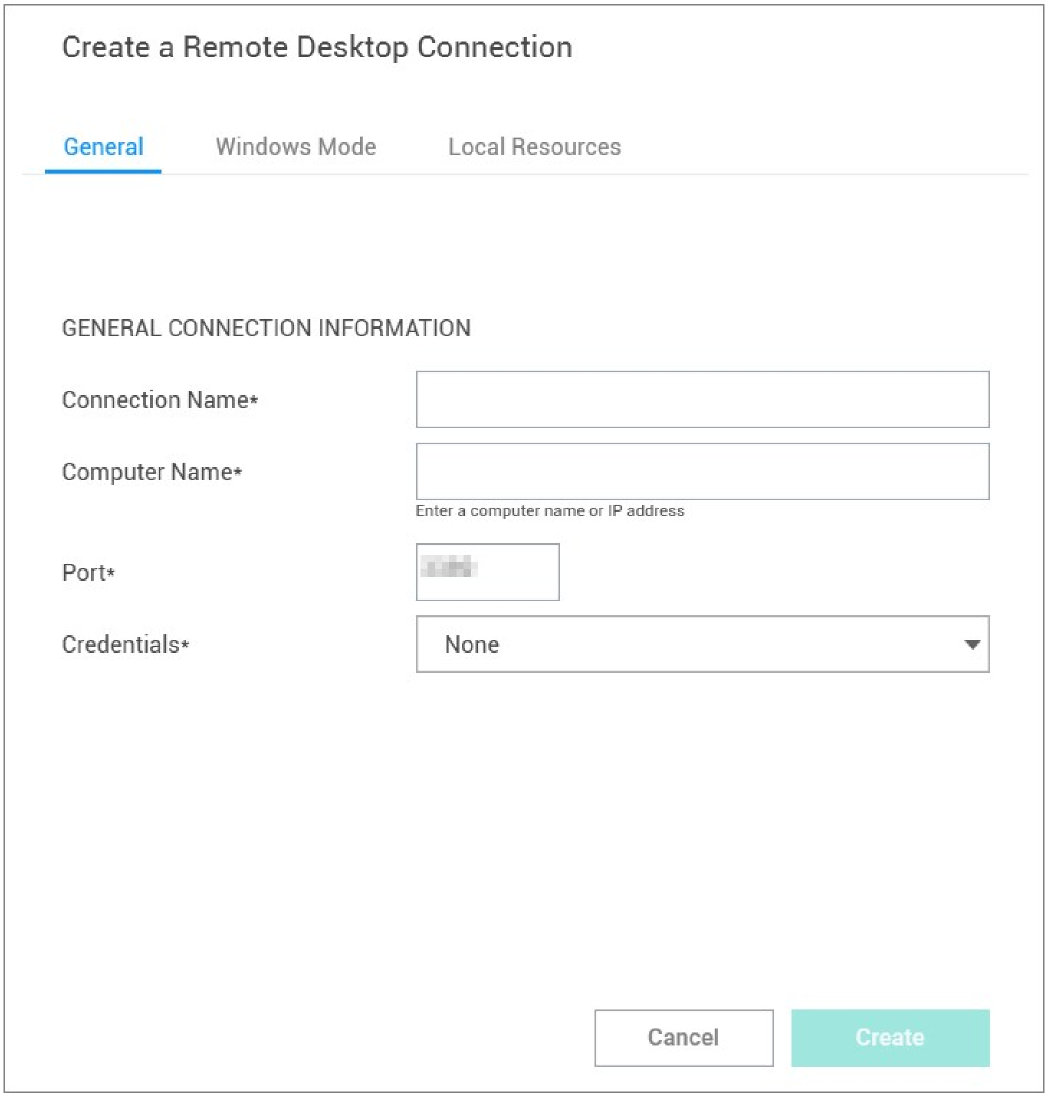
   RDP Connection

   - **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.



Create a Remote Desktop Connection

GENERAL CONNECTION INFORMATION

Connection Name*

Computer Name*

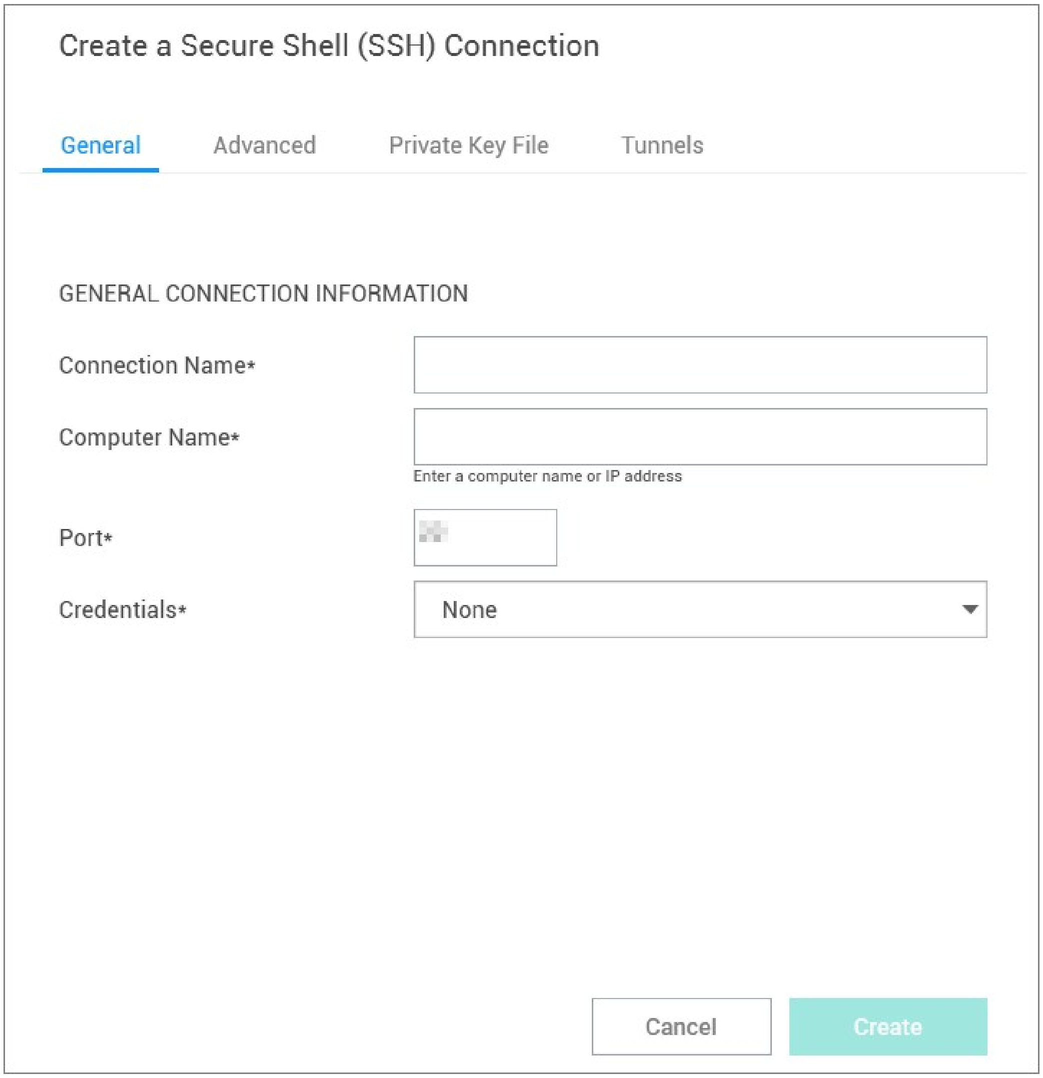
Enter a computer name or IP address

Port* [redacted]

Credentials* None

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.



Create a Secure Shell (SSH) Connection

GENERAL CONNECTION INFORMATION

Connection Name*

Computer Name*

Enter a computer name or IP address

Port* [redacted]

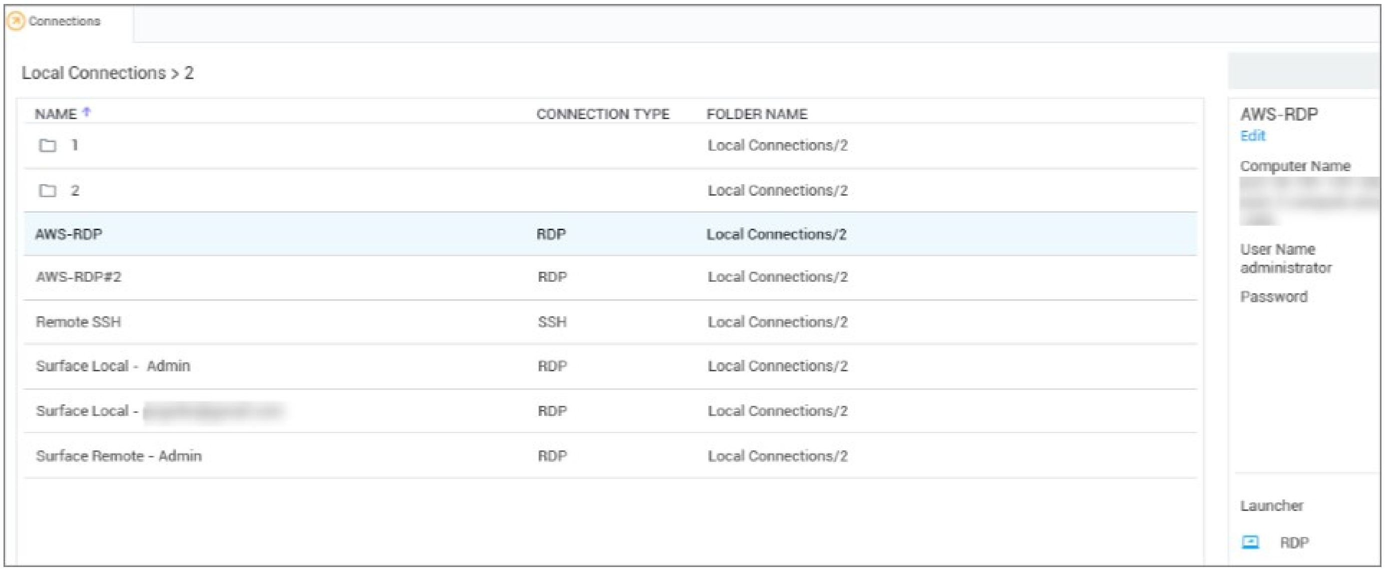
Credentials* None

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.

Edit Connections to Remote Systems

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



Connections

Local Connections > 2

NAME ↑	CONNECTION TYPE	FOLDER NAME
🗀 1		Local Connections/2
🗀 2		Local Connections/2
AWS-RDP	RDP	Local Connections/2
AWS-RDP#2	RDP	Local Connections/2
Remote SSH	SSH	Local Connections/2
Surface Local - Admin	RDP	Local Connections/2
Surface Local - [redacted]	RDP	Local Connections/2
Surface Remote - Admin	RDP	Local Connections/2

AWS-RDP
Edit

Computer Name
[redacted]

User Name
administrator

Password

Launcher

RDP

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

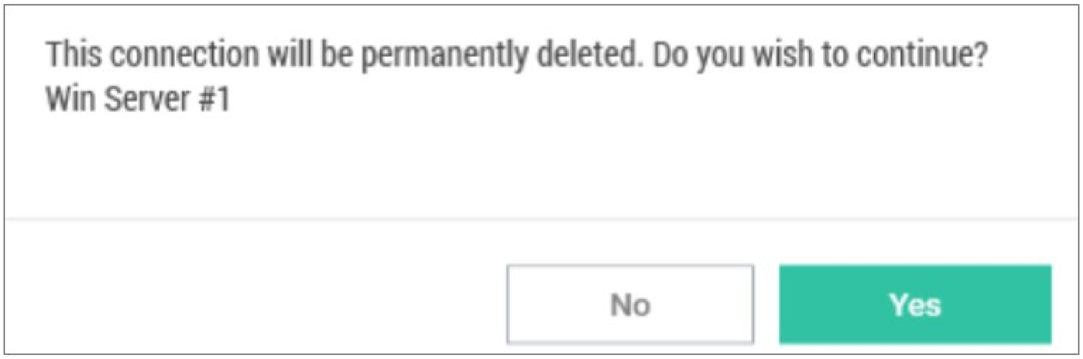
1. Modify the fields as desired. (Most values in a local connection may be edited, except the required fields and the username field.)
2. Click **Save** when finished.

Delete Connections from Remote Systems

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.



This connection will be permanently deleted. Do you wish to continue?
Win Server #1

3. Click **Yes** to confirm.

Open a Remote Connection

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:

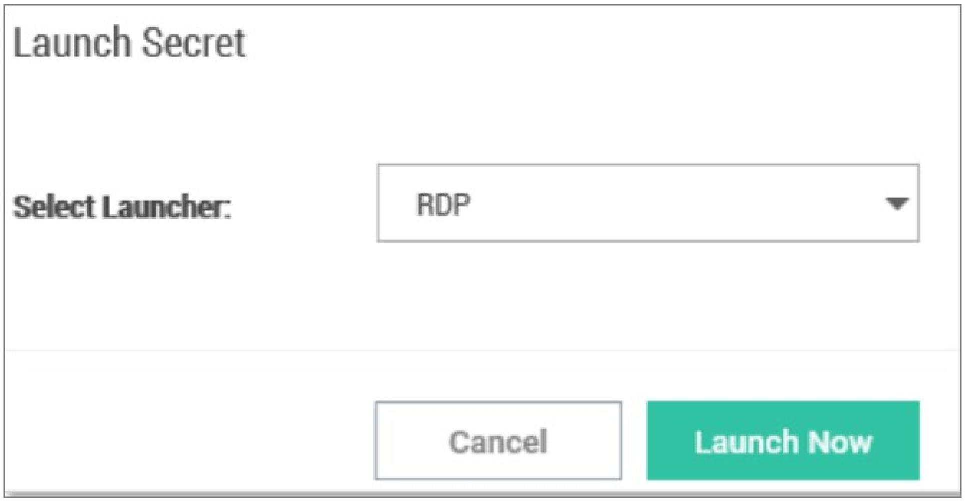
   - In the main window, double-click the connection name. A new connection tab will open, or

   - 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 a whitelist, 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.

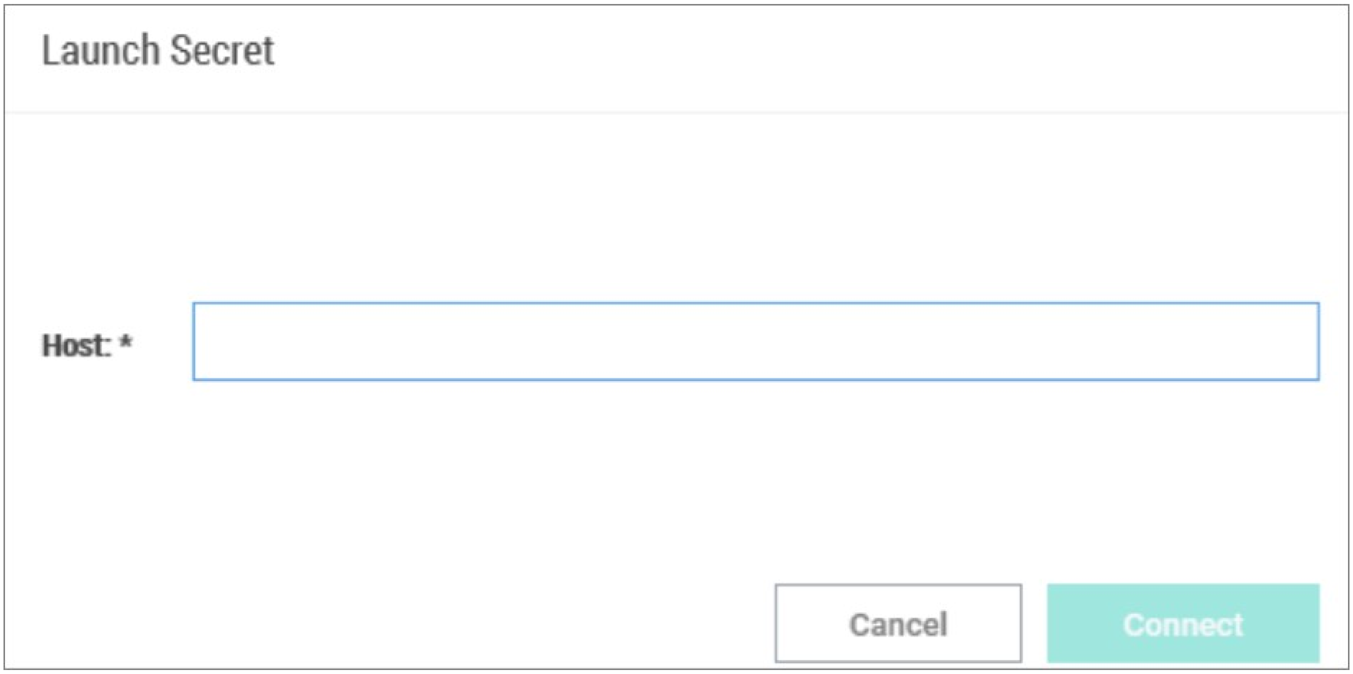
   

   Launch Secret

   Select Launcher: RDP

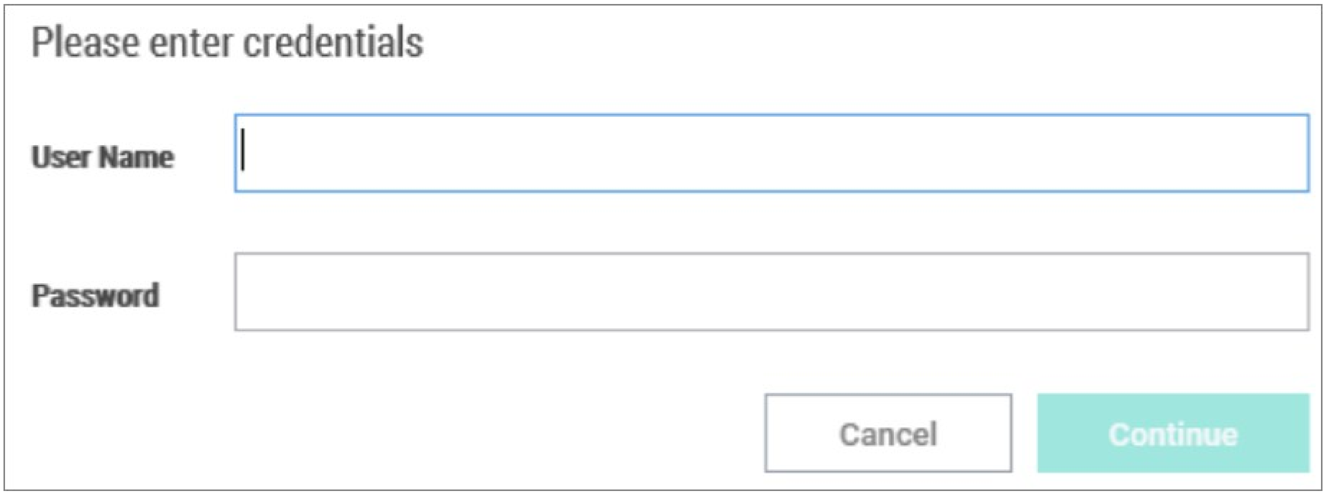
   Click **Launch Now**.

3. Select a **Host** or **Machine ID**. For Secrets where a host is not specified, you are prompted to enter one.



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**.

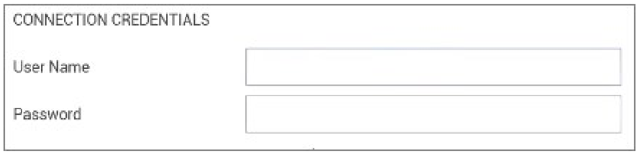
Create an Integrated Connection

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 Connect 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.

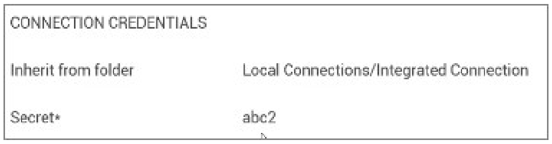


CONNECTION CREDENTIALS

User Name

Password

- **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.

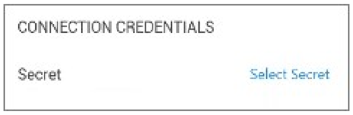


CONNECTION CREDENTIALS

Inherit from folder Local Connections/Integrated Connection

Secret* abc2

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



CONNECTION CREDENTIALS

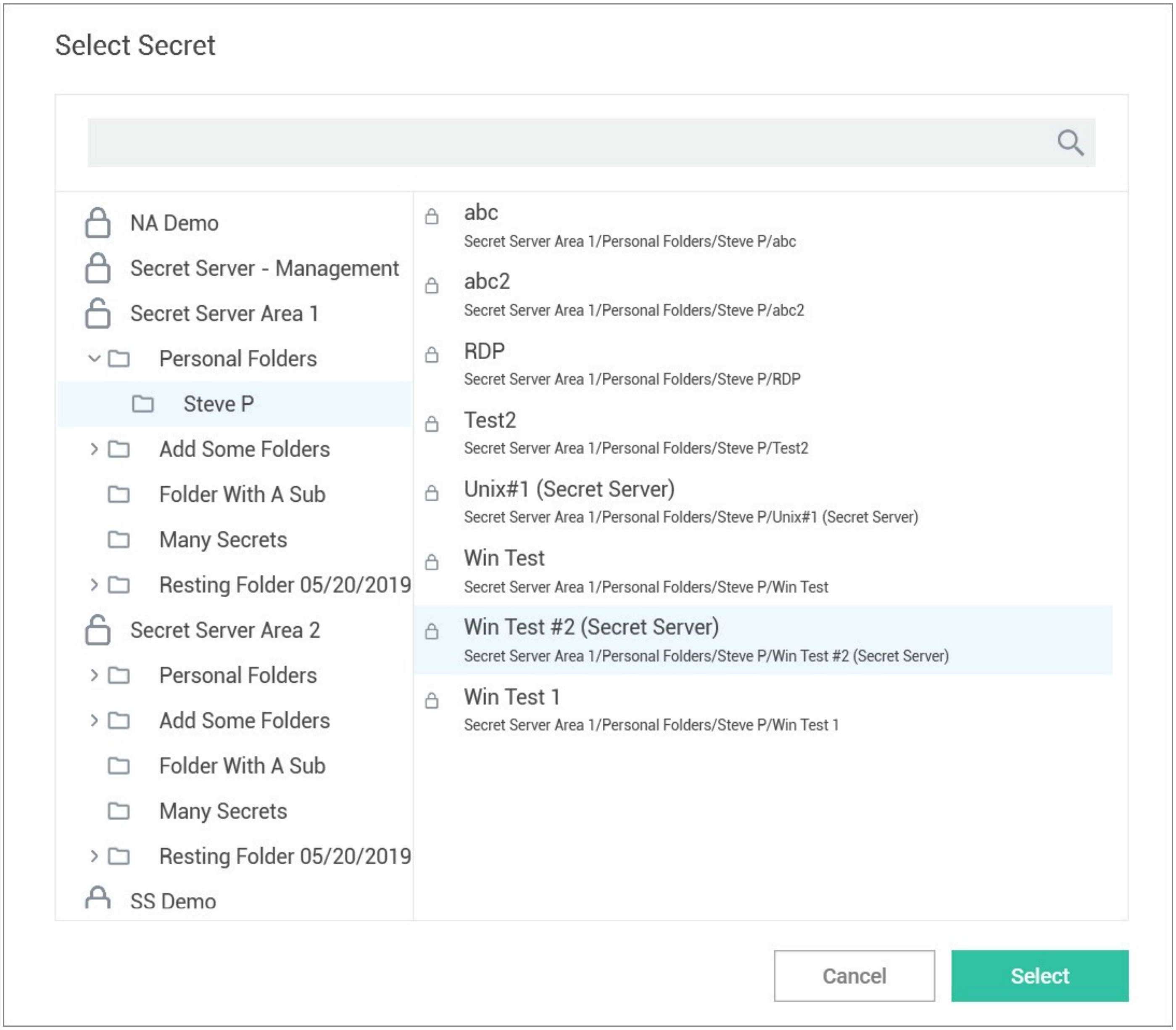
Secret Select Secret

Map a 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.

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.



Select Secret

- NA Demo
- Secret Server - Management
- Secret Server Area 1
  - Personal Folders
    - Steve P
  - Add Some Folders
  - Folder With A Sub
  - Many Secrets
  - Resting Folder 05/20/2019
- Secret Server Area 2
  - Personal Folders
  - Add Some Folders
  - Folder With A Sub
  - Many Secrets
  - Resting Folder 05/20/2019
- SS Demo

abc
Secret Server Area 1/Personal Folders/Steve P/abc

abc2
Secret Server Area 1/Personal Folders/Steve P/abc2

RDP
Secret Server Area 1/Personal Folders/Steve P/RDP

Test2
Secret Server Area 1/Personal Folders/Steve P/Test2

Unix#1 (Secret Server)
Secret Server Area 1/Personal Folders/Steve P/Unix#1 (Secret Server)

Win Test
Secret Server Area 1/Personal Folders/Steve P/Win Test

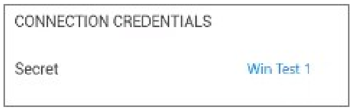
Win Test #2 (Secret Server)
Secret Server Area 1/Personal Folders/Steve P/Win Test #2 (Secret Server)

Win Test 1
Secret Server Area 1/Personal Folders/Steve P/Win Test 1

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.



CONNECTION CREDENTIALS

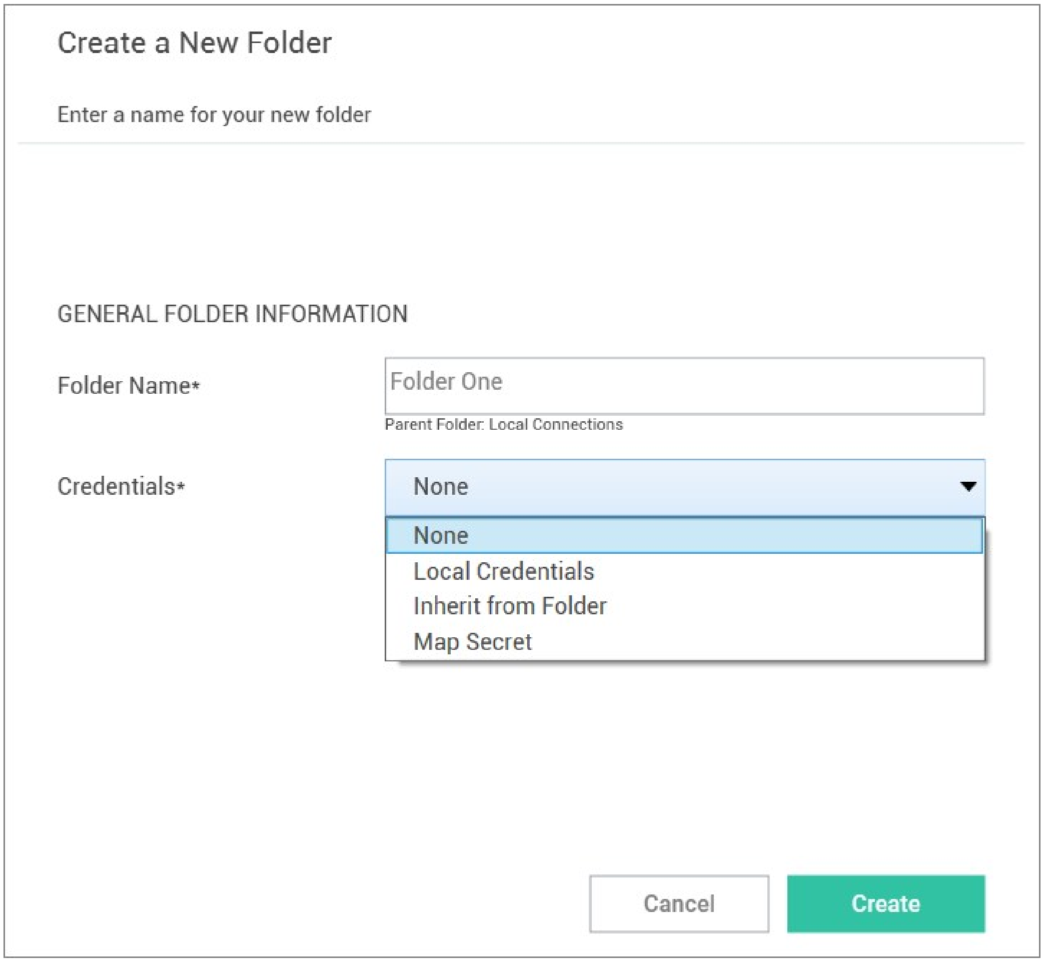
Secret Win Test 1

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

Create, Edit or Delete a 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**.



Create a New Folder

Enter a name for your new folder

GENERAL FOLDER INFORMATION

Folder Name* Folder One

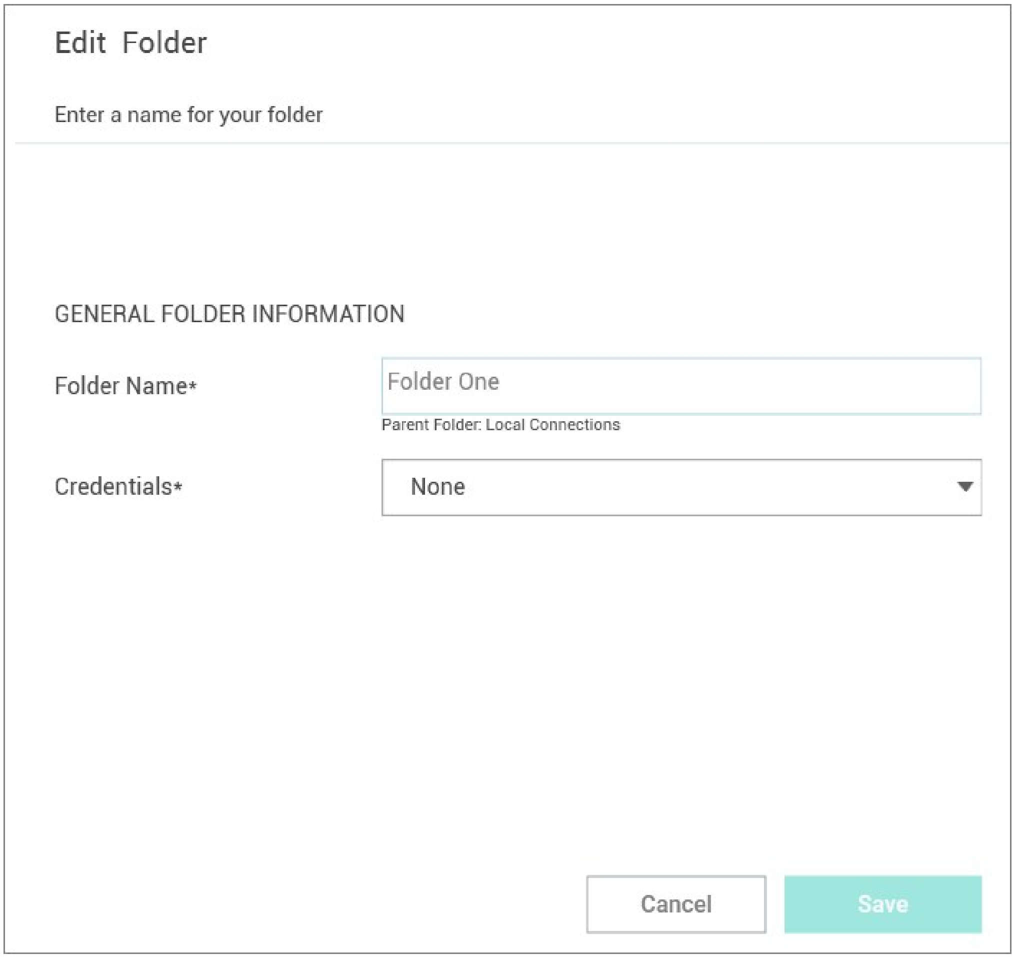
Parent Folder: Local Connections

Credentials* None

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.

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



Edit Folder

Enter a name for your folder

GENERAL FOLDER INFORMATION

Folder Name* Folder One

Parent Folder: Local Connections

Credentials* None

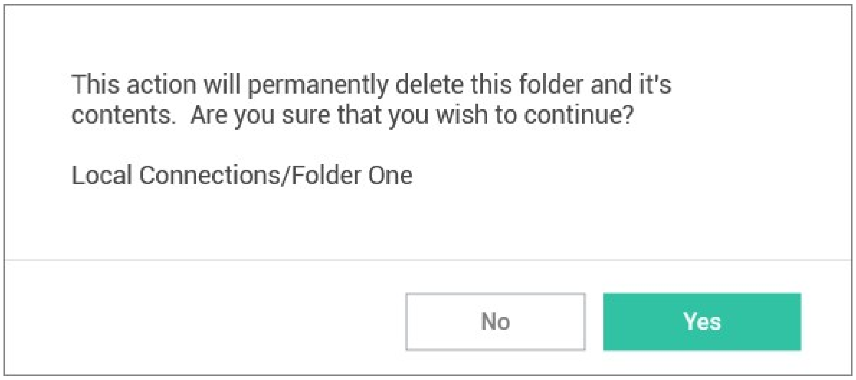
2. Make any desired change to the folder and click **Save**.

View the Integrated Connections section for additional information on credentials.

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.



This action will permanently delete this folder and it's contents. Are you sure that you wish to continue?

Local Connections/Folder One

3. Select **Yes** to confirm.

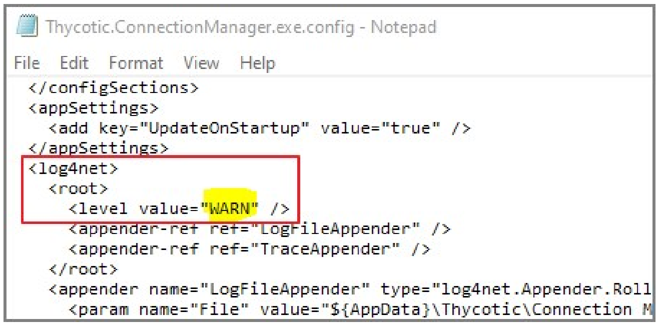
Log Files

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

C:\Users\Administrator\AppData\Roaming\Thycotic\Connection Manager

Changing the Log Level

On Windows system the default log level can be changed via the **Thycotic.ConnectionManager.exe.config** file. Under *log4net* search for the default **WARN** level and change it to **DEBUG** for detailed troubleshooting logging.


Thycotic.ConnectionManager.exe.config - Notepad
File Edit Format View Help

```
</configSections>
<appSettings>
  <add key="UpdateOnStartup" value="true" />
</appSettings>
<log4net>
  <root>
    <level value="WARN" />
    <appender-ref ref="LogFileAppender" />
    <appender-ref ref="TraceAppender" />
  </root>
  <appender name="LogFileAppender" type="log4net.Appender.Roll
    <param name="File" value="${AppData}\Thycotic\Connection M
```

Catalina: ~/Library/Application Support/Thycotic/Connection Manager/ConnectionManager.log

Changing the Log Level

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

```
defaults write com.Thycotic.ConnectionManager FileLogLevel 'Debug'
```

Secrets with Workflows

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

- 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
- Double Lock

Users will see a notification in the properties area of the secret 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 Multi-Tier Secret Access Workflow.

Once the workflow is successful, the connection is established.

Troubleshooting

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

- General
- Application Crash when Editing Existing Secret Server Connection
- AVBlock Error with Session Recording
- Host Names
- Invocation Error on Connect
- Encryption
- Licensing
- Related Resources

General

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).

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.

Yes. - The Secret Server connection got a refresh button with the 1.2.0 version update.

A Connection Manager data file containing the list of connections is stored in C:\Users\\AppData\Roaming\Thycotic\Connection Manager. The file is stored using AES 256 (256-bit) encryption.

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.

Connection Manager does monitor Secret Server heartbeat. If an active RDP/SSH session detects a heartbeat failure the session will be closed automatically.

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.

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.

Application Crash when Editing Existing Secret Server Connection

This topic reviews an issue that can cause an application crash for the Connection Manager 1.2.1 release, including what causes the issue and possible workarounds.

In the Connection Manager 1.2.1 release a condition can be reached that causes the Connection Manager application to crash. There is no specific error message associated with the crash, but it occurs when the following conditions are met:

1. There is an existing connection to Secret Server.
2. The existing connection uses an **Authentication Type** of “Local Username/Password” and has the **Two Factor** option set to anything other than “None”.
3. The user edits the existing connection and changes the **Authentication Type** to “Web Login”.
4. The user tries to complete the web login connection.
5. The application crash occurs once the web login tries to store the login Token from Secret Server.

If the application crash occurs, the next time the user starts Connection Manager the Secret Server connection will be reset back to the original settings.

In the Connection Manager 1.2.1 release, if the **Authentication Type** is set to “Local Username/Password” and the **Two Factor** option is set to anything other than “None”, the value of the **Two Factor** option is saved within the application. The crash occurs when Connection Manager receives the SAML Login token from Secret Server, but it is expecting one of the Local Two Factor options instead (like the “Pin Code”), and as a result cannot process the token and the application crashes.

There are two possible workarounds for this issue.

Workaround 1

1. Open Connection Manager and click “Edit” on the Secret Server connection you want to modify.
2. Keeping the **Authentication Type** as “Local Username/Password” click “Next”.
3. In the **Two Factor** option, change it to “None”.

   By setting the **Two Factor** option as “None” it forces Connection Manager to clear the expected value out from the settings so the conflict cannot occur.
4. Click the “Back” button on the bottom left to return to the previous screen.
5. Now, back on Step 1 of the Edit Secret Server connection dialog, you can change the **Authentication Type** value to “Web Login”.
6. You can now proceed with establishing the Web Login connection. Once the connect is made the new settings for the connection will be saved and the next time you log into this connection it will use the new settings

Workaround 2

The second workaround option is about avoiding the issue initially instead of trying to “fix” the error state.

Instead of editing the existing connection users can create a totally new Secret Server connection using the “Web Login” option and specifying the remaining settings. They can then delete the previously existing connection to help ensure that the connections don’t get confused.

This issue will be resolved in the Connection Manager 1.3.0 Release.

AVBlock Error with Session Recording

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 Thycotic.ConnectionManager.Core.ViewModels.ExplorerViewModel: Unhandled exception in Connect: Autofac.Core.DependencyResolutionException: An exception was thrown while activating Thycotic.ConnectionManager.SecretServer.SecretServerSessionBackgroundWork.
- ERROR Thycotic.ConnectionManager.Core.Managers.ErrorProcessingManager: Show error to user: An exception was thrown while activating Thycotic.ConnectionManager.SecretServer.SecretServerSessionBackgroundWork.

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.

1. Re-enable access to https://lms.primosoftware.com/.
2. Delete the contents of %temp%\primosoftware.lm.cache for all affected users.

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

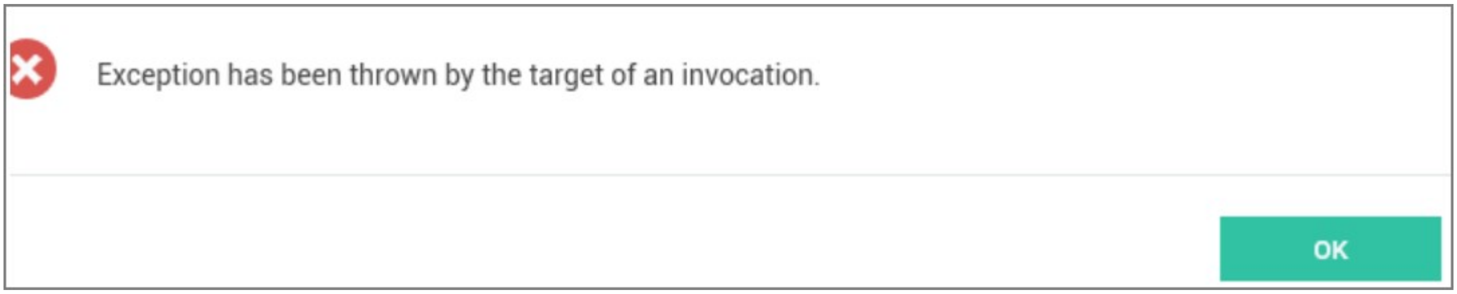
Invocation Error when Connecting to Secret Server

This topic reviews an error that can be encountered in the Connection Manager 1.2.0 Release, including why the issue might be encountered, what causes it, and a solution to resolve it.

In the Connection Manager 1.2.0 release some users might encounter the following error:

`Exception has been thrown by the target of an invocation`

As seen below.



Exception has been thrown by the target of an invocation.

This error can be thrown when trying to connect to a Secret Server instance from Connection Manager, and only occurs for Windows installations.

In the Connection Manager 1.2.0 release a new Feature was added to allow users to login and connect to Secret Server environments using a **Web login** method. The purpose of this was to provide a login option that would help support SAML login configurations for Secret Server instances. As a result, this new feature leverages the .NET framework code and bindings for some Chromium Embedded Framework in order to display and use the **Web login** method.

In most cases the underlying framework for these components is already pre-installed for Windows based workstations, however, some Windows installs may not have these components installed, and this results in the error message above.

> **NOTE**: Most reported cases as of April 18, 2020 seem to occur on new/clean Windows Server installs with minimal configurations.

The `Exception has been thrown by the target of an invocation` error can be resolved for the Connection Manager 1.2.0 release by downloading and installing the following component:

- Visual C++ Redistributable for Visual Studio 2015 - https://aka.ms/vs/16/release/vc_redist.x64.exe

In the Connection Manager 1.3.0 Release and later this issue should be resolved since the component will be included as part of the Connection Manager installation/update process.

Encryption

- Encryption for CM login:
  - 256-bit encryption > AES 256. To check its integrity, we use HMAC + AES 256

Licenses

Yes, if the platinum trial license was created recently.

Connection Manager can connect to any Secret Server instance that is licensed with the Connection Manager Add-on license for Secret Server.

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.

Related Resources

- Secret Server Multi-Tier Secret Access Workflow
- Supported Characters for Machine Host Name

Release Notes

The following Connection Manager release notes are available:

- 1.3.2 - Release Notes
- 1.3.0 - Release Notes
- 1.2.1 - Release Notes
- 1.2.0 - Release Notes
- 1.1.2 - Release Notes
- 1.1.1 - Release Notes
- 1.1.0 - Release Notes
- 1.0.1 - Release Notes
- 1.0.0 - Initial Release

1.3.2 Release Notes

Release Date: 2020-08-11

- Resolved an issue where Local and Secret connections that use non-FQDN Host names no longer launch sessions.

MacOS Specific

- Mac OS version 10.14.16 (Mojave): Resolved an issue when launching a Secret from Secret Server and using Connection Manager as a protocol handler fails with a “could not resolved” message.

1.3.0 Release Notes

Release Date: 2020-07-28

> **Note**: Installer versions:
>
> - Windows: 1.3.0
> - macOS: 1.3.1

- Ability to import connections from third party platforms in CSV format.
  - Adding option to import from CSV.
  - Includes "Import" dialog which allows mapping of fields in CSV to Connection Manager fields.
  - Imported connections import as Local connections.
  - Import can generate 2 reports:
    - Failed items – This report can be imported again to retry just the failed items.
    - Informational report – This report provides information for any fields that were set to use "default" values.
- Improve dynamic resizing for RDP sessions when tab window is expanded beyond original size (resizing session for larger windows/full screen).
- Added "About" screen to display version number, EULA and docs links.
- Added support for "Favorites":
  - Favorites tab/page to view items that are marked as Favorites.
  - Launch connections from Favorites page.
  - Mark Local connections/Secrets/Folders as Favorites and add them to the Favorites page.
- Dark theme support for Mac and Windows (determined by OS).
- Improving validation for basic import/export file in JSON format.
- Added a back-off delay for Connection Manager login, which allows 3 attempts before adding a 5 second delay, increasing the delay by 5 seconds on each following attempt up to 25 second.
- Enforce Secret Server connections to use HTTPS (and not allowing HTTP).
- Added support for smart card passthrough for Secret Server based RDP connections.
- Additional options/settings for using Connection Manager as a protocol handler for Secret Server.
- Setting in CM to switch between using CM as SS protocol handler or SS as the protocol handler.
- Connection Manager build package will ship with Secret Server (to act as the SS Mac protocol handler).

- Fixed an issue that prevented Connection Manager from fully launching a session using the protocol handler on macOS.
- Fixed the size of the file download dialog not being correct (too small) when updating the application.
- Resolved CefSharp (CVE-2020-6418) vulnerability in web browser for Secret Server login.
- Fixed an issue for launching Secrets that connect using RPD proxy.

1.2.1 Release Notes

Release Date: 2020-04-28

- Fixed an issue for connecting to Secret Server using Multi-factor authentication (like DUO or RADIUS). The issue resulted with the message "Connection failed reason: A task was cancelled" and a failed connection after 20 seconds. The timeout setting for this authentication has been extended to 5 minutes.

MacOS Specific

- Fixed an issue where some dialogs and settings options were not displayed correctly if the macOS system was set to Dark Theme.

1.2.0 Release Notes

Release Date: 2020-04-14

- Added ability to create a new Local Storage file (for Local Connections) directly from the Connection Manager Sign In dialog.
- Updated the User Interface so the Navigation section can be resized.
- Updated the general style for the Properties tab (bolding the headers, and text formats).
- When a large number of tabs are open, double-clicking on the left or right scroll arrows will jump to the far end of the tab list (in either direction).
- Added ability to login to Secret Server using the Secret Server web login (for SAML support).
- Added ability to launch Secret Server Secrets that use other Launcher types. Connection Manager will support 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.
- Added the ability to launch a Secret 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 then launching it will use Connection Manager if it's available. When Connection Manager opens it will be in a "Locked" state where only the Secret Server launched session(s) are available.
    - If Connection Manager is launched using the protocol handler and is in the "Locked" state, users will have a "Sign In" option available to them to fully log into Connection Manager to use their other connections.
- Added support for two new Secret Server settings. Changing these settings in Secret Server will globally enforce the changes for Connection Manager applications that are connected. The Secret Server Settings are:
    - Allow Local Connections - Allows or disables the saving of credentials for any Local Connections. By default, this is set to Yes.
    - Allow Saving Credentials - Allows or disables the saving of credentials for any Secret Server connections. By default, this is set to Yes.

- Fixed an issue, where if you selected the first row in the main Work area the context menu options (on right-click) did not display all of the available options.
- Fixed an issue, where if the Secret Server URL contained "v1" in the path it was replaced with "v2".
- Fixed an issue with Integrated connections (a local connection with a Secret Server Secret for credentials) where a Local SSH connection was retuning an "incorrect username or password" message if the Secret uses Secret Server Proxy.

1.1.2 Release Notes

Release Date: 2020-01-28

- Fixed an issue causing remote sessions, with Session Recording on the Secret, to timeout after 1 minute.

1.1.1 Release Notes

Release Date: 2020-01-13

- Fixed an issue returning a "Failed to configure RDP component" message when opening a Local Connection using a Secret Server Secret with RDP proxy configured.

1.1.0 Release Notes

Release Date: 2020-01-08

- Added ability to make an Integrated Connection: a Local Connection that uses a Secret from Secret Server for credentials.
- Added ability to perform Global Search when at the root for Local Connections or at the root of a Secret Server connection.
- Made loading of Folder, Connection, and Secret data dynamic when a folder is selected.
- Displayed Personal Folders folder at the top of a Secret Server connection.
- Added support for screen resolution size down to 1280x720.
- Added ability to refresh a Secret Server connection or folder from the navigation bar.
- Allow expanding and collapsing of Secret Server connections or Local Connections (at the root) in the navigation bar.
- Included Computer Name value in the tab title and tab tool-tip pop-up.
- Added support for a client PC running in FIPS mode.
- On the Recent page, added a Connection Source column to identify if a connection is Local or from Secret Server.
- On the Recent page, added a Connection Type column to identify whether Local Connection are SSH or RDP, or list the Secret template for Secret Server connections.
- Secret connections from Secret Server will be listed on the Recent page.
- When opening a Secret Server connection from the Recent page, a notification will be presented if the Secret has been deleted.
- Secret connections that use the Check-In/Check-Out workflow will display a Check-In button if the Secret is currently checked out by the user.
- The properties panel for Secret connections that use the Access Request workflow have been updated so the Access Request pop-up more closely matches the Access Request dialog from Secret Server.
- If a Secret connection from Secret Server uses an empty white list, launching a connection will open a text box to enter a value.
- If a Secret connection from Secret Server uses an SSH proxied session, Connection Manager will respect the Secret Server option to only record the SSH keystrokes from the session.
- If no Secret Server connection exists in Connection Manager, opening the Secret Server Connections configuration will open directly to the Connect to Secret Server dialog.
- Display user information message when a user has been disconnected from a remote session due to another user logging in.
- Improved error message handling when attempting to create a connection to Secret Server.
- When installing Connection Manager, allow for users to set a different location to store the local storage data file.
- In the File menu for Connection Manager, added a quick link to the documentation.

- Fixed an issue preventing users from seeing any Secrets listed at the root of a Secret Server connection.

1.0.1 Release Notes

This document includes the most recent version of the Connection Manager Release Notes.

1.0.1 Release Notes

Release Date: 2019-09-27

- Fixed an issue that caused Connection Manager to not connect with Secret Server Cloud.

1.0.0 Release Notes

Release Date: 2019-09-17

This is for the initial release of Connection Manager.

Functionality in Connection Manager is broken down into two primary sections: Connection Manager – Free Tool and Connection Manager – Secret Server Integration.

Remote Sessions

- Able to create ad-hoc connections for RDP sessions.
- Able to create ad-hoc connections for SSH sessions using PuTTY sessions.
- Encrypt and store the credentials and general connection information for any Local connections.
- RDP Session - Add additional RDP session options (standard RDP options) when making a connection, including Windows Mode options (desktop size, color depth and auto window resizing) and Local Resource options (sharing of local devices, including audio).
- RDP Session - When editing a Local RDP connection, users should be able to change: the password, Windows Mode options and Local Resource options.
- SSH Session - Add additional SSH session options (standard SSH options) when making a connection, including Advanced SSH options (character set, font and font size).
- SSH Session - Add ability to specify a private key file and password to use when connecting to SSH session.
- SSH Session - Add ability to set and specify multiple Tunnel (using values for: Port, Destination server and Destination Port) for SSH sessions.
- SSH Session – When editing a Local SSH session, users should be able to change: the password, Advanced options (font size, type and character set), Private Key options and Tunnels.
- When Local sessions for RDP or SSH are launched the remote session will open as a new Tab in the work area.
- Remote sessions (RDP or SSH) have the ability to expand to a "Full Screen" mode.

User Interface

- Added left-hand tree style navigation bar.
- Create Local folders to store, manage and sort Local connections.
- Added breadcrumb navigation to the top of the work area.
- RDP and SSH session types are marked by different colors for the tabs.
- Added a Properties panel to the right inside the main work area when users select a connection or folder.
- In the properties panel for Local connections, allow users to view the password for that connection.
- Local connections can be launched using two methods: Double-click on the connection row in the work area or click the launcher icon in the properties panel.
- Existing Local connections and folders can be edited by right-clicking on the row in the work area or by clicking an "Edit" button in the properties panel.
- When editing a folder under the Local connections section the folder name can be changed.
- Add ability to Remove any Local connections or folders.
- Added ability to view a list of any "Recent" sessions by selecting "Recent" in the navigation bar.
- Sessions can be launched by double-clicking on a connection in the "Recent" page.
- Add ability to view a list/display of all active remote sessions on an "Active Session" page
- Show a screen view of a session on the Active Session page from the last time the session was accessed.
- Allow users to quickly navigate to a active session from the Active Session page by double-clicking on the session image.
- Add a scroll bar to the Tabs section of the work area so if multiple tabs are open and extend beyond the page, a user can scroll over to

them.

- Add a Search bar to the top right of the work area so users can run a search on the current folder for a connection.
- Add a "Configuration" menu to the bottom of the navigation bar for application options.
- Make Global options for RDP and SSH sessions available for modification from the Configuration > Global Configuration option in the navigation bar.
- Add a set of Global RDP sessions options (using Windows Mode options and Local Resource options) that are used for new sessions by default.
- Add a set of Global SSH sessions options (using Advanced options [font size, type and character set], Private Key options and Tunnels) that are used for new sessions by default.
- Make Global options for RDP and SSH sessions available for modification from the Global Configuration option in the navigation bar.
- Add ability to Export existing Local connections and folders to an output file (JSON format).
- Make export action for Local connections available by right-clicking in the navigation bar or by right-clicking on a folder/connection in the workspace.
- When exporting a connection, users should have the option to include the Password (This will be in Clear Text so the file can be imported later).
- Add ability to Import a set of folders and connections (using the JSON format from the Export) under the Local Connections section.
- Make the import action only available from the navigation bar.
- The import action should add all folders and connection details specified in the JSON file under the specific folder location that was selected when selecting the option.

Integration

- Add ability to connect to a specific Secret Server instance (On-prem or Cloud).
- Add ability to add multiple Secret Server connections to a single Connection Manager instance.
- Display a list of all Secret Server connections under Configuration > Secret Server Connections.
- When connecting to Secret Server, allow for multi-factor login options (pin-code, duo push, duo phone call, none) to be used.
- When connecting to Secret Server add ability to select Secret templates to fetch for displaying Secrets.
- When a connection is established with Secret Server the folder structure containing the Secrets that can be accessed for the logged in user should be displayed in the navigation bar.
- Add ability to edit an existing Secret Server connection including the "friendly" name for the connection, password, domain field, multi-factor options and modify the list of templates.
- Add ability to remove a Secret Server connection.
- When selecting a Secret Server folder in the navigation bar, the work area should display all the Secrets and folders that are available to the user.
- Display a "Locked" icon when a Secret Server connection has not been authenticated and an "open lock" icon when it has been authenticated (for easy viewing).
- Add ability to launch a Secret with RDP or SSH credentials as a remote session similar to how Local connections are launched.
- When selecting a Secret from a Secret Server connection, do not display the Password field for the Secret in the properties panel.
- If a Secret doesn't have all the necessary fields to launch a remote RDP/SSH session, a dialog should open that prompts the user to enter the missing values (like machine name/IP).
- When selecting a Secret from a Secret Server connection, do not display the Password field for the Secret in the properties panel.
- Add ability to support Secret Server workflows including Check-In/Check-Out, Change password on Check-In, Double Lock, Prompt for Reason or Ticket System, Request Access and Require Comment.
- When accessing Secrets that use workflows, display a prompt for the workflow in the properties panel.
- Add support for Session Recording that is set on Secrets from Secret Server following the standards that Secret Server uses for Session Recording.
- When viewing a Secret in the work area that has Session recording set in the Secret, display a "Record" indicator on the launcher icon in the properties panel.
- When launching a Session that has Session recording set in the Secret, display a "recording" icon in the session tab.
- When Session recording for a remote session is active or completes, send all session information back to Secret Server for processing.

- When a Secret is accessed in Connection manager, send Audit information back to the specific Secret Server instance for logging purposes.

Changelog

This topic provides a chronological list of documentation changes, to help track additions, deletions, and contents edits other than spelling and grammar corrections.

- 1.3.2 Hotfix release updates, refer to Release Notes for details.

- 1.3.0 Release Updates, refer to Release Notes for details.

- Added two topics to the Troubleshooting section:
  - Application Crash when Editing Existing Secret Server Connection
  - AVBlock Error with Session Recording

Support

Thycotic customers have access to support by phone and email. You also can open a case in Thycotic's support ticketing system, which promotes follow-through to issue resolution.

> **Note**: Please see our Support Services Guide for details about our support policy. This page provides a high-level summary of portions of that guide.

Use the means you prefer, except for Severity 1 issues—for those, always use phone support.

Severity 1 means a critical problem that has caused *complete loss of service* and work cannot reasonably continue at your worksite.

To obtain support by email or phone, first log in to the Support Portal to obtain a PIN. The PIN validates that your license includes support, and you must provide the PIN in your email or when you call. The PIN also makes it easier for the person helping you to locate your customer records and give you better support.

- Visit the Support Portal Login Page using the credentials you received when you became a customer.
- After logging in, you will be on the main page. Click on the large blue bar labeled PIN to obtain a PIN number.

Thycotic delivers support by phone worldwide. Select the applicable number from this list:

AMERICAS	all	+1 202 991 0540
EMEA	UK	+44 20 3880 0017
	Germany	+49 69 6677 37597
APAC	Australia	+61 3 8595 5827
	Philippines	+63 2 231 3885
	New Zealand	+64 9-887 4015
	Singapore	+65 3157 0602

Send your email to support@thycotic.com **with the PIN number as part of the subject line** of your email, for example:

- PIN 345 Workflow Stopped Unexpectedly

Include this information:

1. company name
2. contact name

3. contact phone number
4. product name
5. details of the issue

You must send your email using an email address already noted in your account with Thycotic.

- Sending a support request from an email address not on file may delay our response.

As an alternative to support by email or phone, you can open a support ticket and track your issue to resolution.

- Visit the Support Portal Login Page using the credentials you received when you became a customer.
- After logging in, you will be on the main page. Click the **Cases** tab, then **Create a Case**.
- Follow the instructions to complete your case.