



# Delinea

Connection Manager

Documentation © 1.8.0



## Table of Contents

Introduction to Connection Manager	7
Installation of Connection Manager	8
Permissions Required to Install/Uninstall Connection Manager	8
Connection Manager Hashes	8
<i>Version 1.8.0</i>	8
<i>Version 1.7.1 Hashes</i>	8
<i>Version 1.7.0 Hashes</i>	8
System Requirements	10
Windows Installation	11
Updates	12
MacOS Installation	14
Enabling Screen Recording and Input Monitoring	15
Command Line Arguments	16
Disable Local Vault on Installation	16
Specify Custom Logo Images to Copy to the Proper Location	16
Pre-create Secret Server Connection	16
<i>Local Connection</i>	16
<i>Web Connection</i>	17
Getting Started	18
Create a Password	19
Sign in into Connection Manager	20
User Interface Components	21
Main Screen	22
Navigation Tree	23
<i>Active Sessions</i>	23
<i>Favorites</i>	23
<i>Shared With Me</i>	24
<i>Recent</i>	25
<i>Connections</i>	26
<i>Local Connections</i>	27
<i>Shared with me</i>	27
<i>Configuration</i>	27
Work Area	28
Properties Area	29
Menus	30
<i>Stack Menu</i>	30

File	30
Help	30
<i>Right Click Navigation Menu</i>	31
<i>Work Area Menu</i>	32
<i>Search</i>	32
<i>Global Search</i>	32
<i>Configuration</i>	32
<b>Secret Server Requirements</b>	33
What are the quick, hard requirements for connecting to Secret Server?	33
<b>Connect to Secret Server</b>	34
Local Username/Password	34
Web Login	37
External Login	41
<b>Modify a Connection</b>	45
<b>Remove a Connection</b>	48
Import and Export Connections	49
Export Connections	50
Import of JSON Files	51
<i>JSON Example</i>	51
Import of CSV Files	53
<i>Importing Local Connection Data</i>	53
<i>Field Values and Types</i>	57
Desktop Size	58
<i>Import Completed Reports</i>	59
<i>CSV Import Differences</i>	59
Import of RDP Files	60
Import of RDG Files	64
<b>Local Data Vault</b>	66
Local Data Vault Enabled	66
Local Data Vault Disabled	66
Enable or Disable Local Data Vault on Installation or Upgrade	66
<i>Windows</i>	67
<i>Mac</i>	67
Enable or Disable Local Data Vault when Connecting to Secret Server	67
Enable or Disable Local Data Vault at Any Time	67
<b>Global Configuration Settings</b>	69
Globally Enforced Secret Server Settings	71
Use a Custom Logo in the Connection Manager Interface	75
<i>Manual Procedure</i>	75
<i>Command Line Procedure</i>	75

Protocol Handler Approved URLs	76
Desktop Size and Auto Expand	77
Launchers	79
Proxy Tabs Show Remote Host Name	80
Screen Resolution for New Session Window Views	80
Moving and Reorganizing Session Tabs and Windows	80
Session Recording	82
Launching from Secret Server without Connection Manager Open	82
Signing In After the Launch	83
<i>Create a New Local Storage File</i>	84
Common User Activities	85
Connections	86
Re-authenticate	87
<i>Create a New Connection to Remote Systems</i>	89
<i>Edit Connections to Remote Systems</i>	91
<i>Delete Connections from Remote Systems</i>	92
<i>Open a Remote Connection</i>	93
<i>Batch Edit Local Connections</i>	95
Batch Edit Local Connections Using Multi-select	95
Batch Edit Credentials for All Connections in One or More Folders	95
<i>Batch Open Connections</i>	97
Batch Open Connections Using Multi-select	97
Batch Open All Connections in a Folder	97
<i>Duplicate Remote Connection</i>	99
<i>Create an Integrated Connection</i>	100
Credentials	100
Map a Secret to a Folder	100
Configuration File	102
Windows Configuration File Location	102
macOS Configuration File Location	102
<i>Disable update check on startup for Windows</i>	102
<i>Disable update check on startup for macOS</i>	102
Folder: Create, Edit, Move, Delete	103
Create a New Folder	103
Edit a Folder	103
Move a Folder	104
Delete a Folder	104
Log Files	106
Windows Log File Location	106
<i>Changing the Log Level</i>	106

Windows Log File Location	106
MacOS Log File Location	106
<i>Changing the Log Level</i>	106
Using SSH Session Groups	107
Creating and Naming an SSH Group	107
Sending Commands to the SSH Group	109
Options for Displaying SSH Sessions on the Group Tab	110
Building an SSH Group	111
Closing an SSH Group	111
Secrets with Workflows	112
Troubleshooting	113
General	114
What are the default locations for the Connection Manager application and log files?	114
Is there a local session timeout for sessions within Connection Manager (CM)?	114
I'm seeing a Connection failed error message while trying to connect to SS	114
Is there a way to refresh the SS connections?	114
Where and how is the data for Connection Manager stored?	114
Is there a way to push scripted code out to multiple SSH sessions at one time for updates or commands?	114
What happens if the SS Heartbeat fails?	114
Is there any current performance data for Connection Manager? Including: general memory, amount of space needed, number of open connections that can be made at one tie, etc.	114
While recording a session, if a user isn't on tab, what's the behavior? Do we reduce what we record and send? Or does it stay the same? How can we tell if it's the "focus"?	114
Application Crash when Editing Existing Secret Server Connection	116
Issue	116
Reason	116
Workarounds	116
<i>Workaround 1</i>	116
<i>Workaround 2</i>	116
Resolution	117
AVBlock Error with Session Recording	118
Problem	118
Workaround	118
Host Names	119
Invocation Error when Connecting to Secret Server	120
Issue	120
Reason	120
Resolution	120
Future Releases	120
Encryption	121
Licenses	122

Does a current customer drop in the platinum trial license key into their current Secret Server instance to receive the Connection Manager feature?	122
Does it matter, if Connection Manager is working with a different Secret Server instance than the one aligned with the trial key?	122
Is it okay to add trial license to production server? Will it overwrite or add to the current license?	122
<b>CM Crashing When Offline and Checking Certificates</b>	123
Issue	123
Resolution	123
<b>Generate Additional Log Entries</b>	124
<b>Manually Cleaning the Connection Manager File System</b>	125
Remove files and folders	125
Clear entries from the Registry	125
<b>Related Resources</b>	126
<b>Release Notes</b>	127
Connection Manager Version Compatibility with Secret Server	127
Release Notes History	127
<b>1.9.0 Release Notes</b>	128
Features	128
General Improvements	128
Security Improvements	128
Bug Fixes	128
<i>iOS Specific</i>	128
<b>Changelog</b>	129
Connection Manager Version Compatibility with Secret Server	129
August 2022	129
April 2022	129
November 2021	129
August 2021	129
July 2021	129
March 2021	129
March 2021	129
December 2020	129
August 2020	130
July 2020	130
June 2020	130

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

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

## 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 procedures below:

- [System Requirements](#)
- [Windows Installation](#)
- [MacOS Installation](#)
- [Command line Arguments to Create a Secret Server Connection on Install](#)

In order to install or uninstall Connection Manager, users must have administrator privileges.

### Version 1.8.0

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

- SHA1 e4989e93fc2d1a3f5d0bc92a298b99be2cd0ce1e
- SHA256 d5352367df30e254678026c6724a80bb2761b96c726b78b11ef61a556c59e44b

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

- SHA1 da39a3ee5e6b4b0d3255bfef95601890afd80709
- SHA256 e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

### Version 1.7.1 Hashes

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

- SHA1 c0e269a41fc8ac974f445d6769ae28b9bd2008ff
- SHA256 22387c20a1620938a642906f2c103b43ea5c608975722d8a1f1a0db4d30d9cc5

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

- SHA1 4ede9f06111d11fc77900427e416b8f7a0cf0c25
- SHA256 088aa3c6ec903e04ced12871198a40d0dfc1a2028c7f8bcc21dc916786986ef2

### Version 1.7.0 Hashes

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

- SHA1 343c82d10b79abcf9302b7b1772f4caa8637047
- SHA256 3cf0ed060bc2b9d2639b779dd6e9c90c48adcd268646b9c3408726eac5bb1d05

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

- SHA1 9ae109074bffade9e2e3e0bca241db23457e0c50
- SHA256 b04fa74e41f522c3f13913b05194026b17ef329ba470e0200318cabf84b4962b





## System Requirements

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

Connection Manager does not support Windows Server 2003.

For Unicode characters, Connection Manager supports UTF-8 encoding.

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>). Delinea recommends upgrading clients to Windows 10.
- Macintosh Installation: OS X 10.12x (High Sierra) or later, 8GB RAM, M1 chipsets are also supported

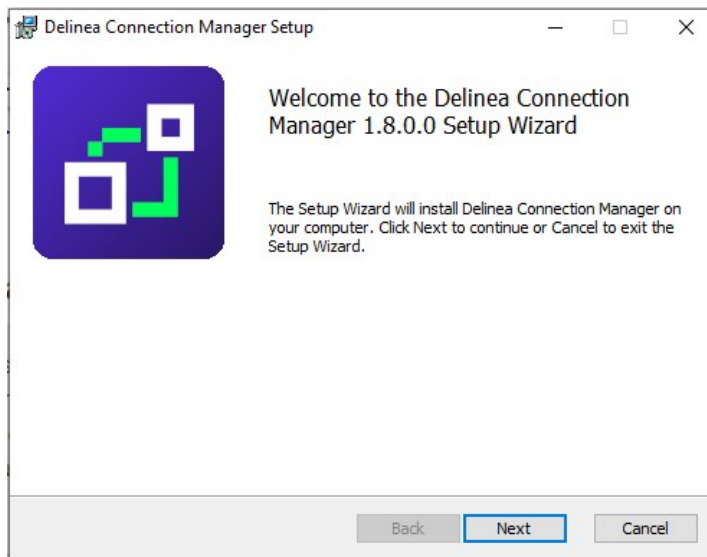
Minimum requirements for connectivity to Secret Server(s):

- Secret Server Installation: 10.7 or later

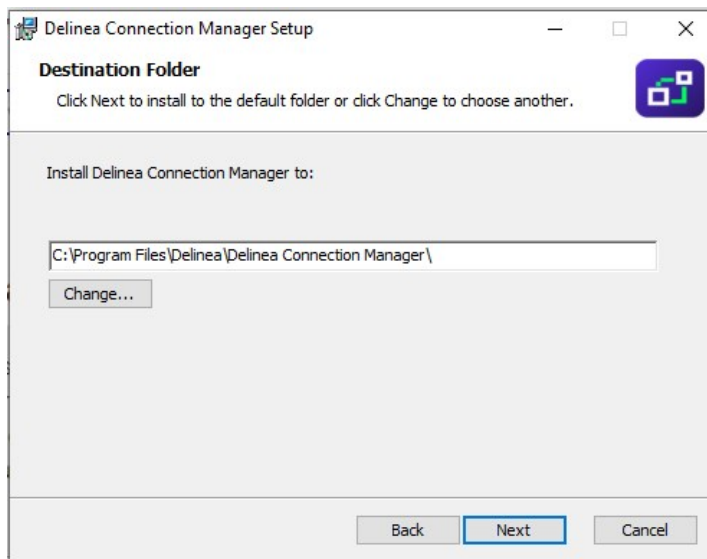
## Windows Installation

**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.

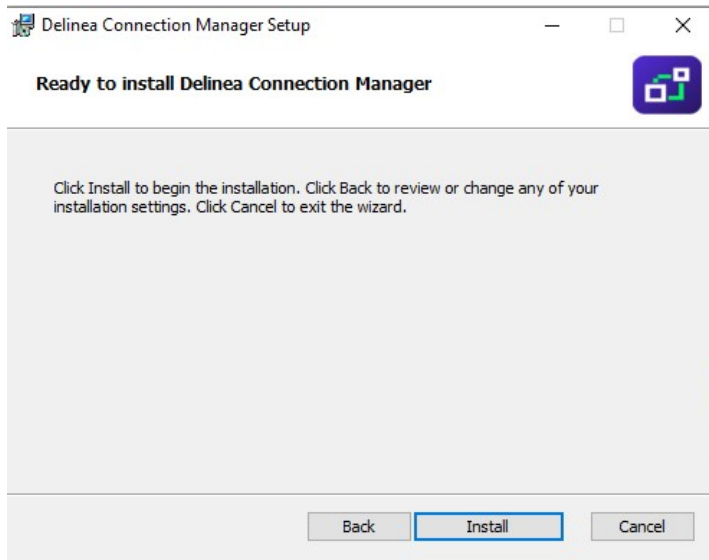
1. Download the MSI [Windows Installer File \(MSI\)](#) for Connection Manager.
2. Double-click the MSI file to start the install process.



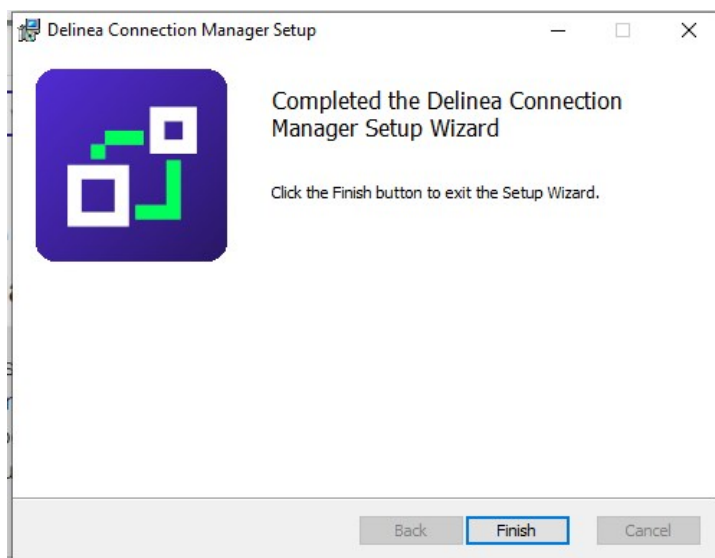
3. Click **Next** to continue.



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



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



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?

Remind me later

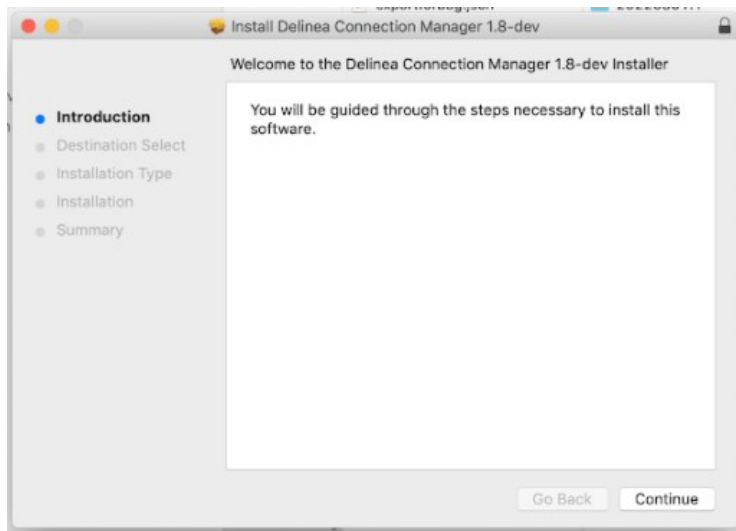
Update

## MacOS Installation

1. Download the PKG file from Delinea's [Macos download](#) page.
2. A PKG file will download to your system.

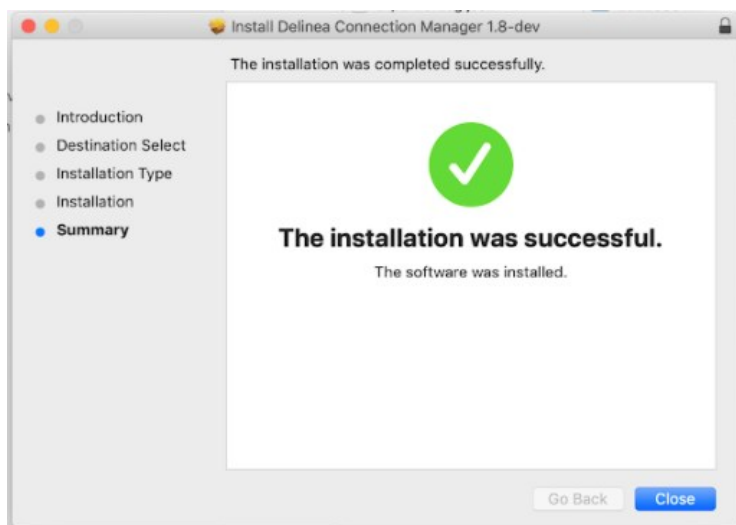
**Note:** The file extension is a .pkg starting with release 1.2.0.

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 Delinea Connection Manager logo to the Applications folder. The installation begins.



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

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



## Enabling Screen Recording and Input Monitoring

Some functions in Connection Manager for Mac require access to Screen Recording and Input Monitoring.

macOS 11 Big Sur introduced the capability for Mobile Device Management (MDM) profiles to give a standard user access to these functions. macOS does not provide this access automatically. You must configure the access by using an MDM Privacy Preferences Policy Control (PPPC) profile following the steps below.

1. Navigate to **System Preferences > Security and Privacy > Privacy** tab.
2. In the left-hand panel select **Input Monitoring**.
3. In the right-hand panel check the box next to **Delinea.ConnectionManager**.
4. In the left-hand panel select **Screen Recording**.
5. In the right-hand panel check the box next to **Delinea.ConnectionManager**.

Inside your MDM, create a PPPC profile using the settings below:

- **Identifier:** com.Delinea.ConnectionManager

- **Identifier Type:** Bundle ID

- **Code Requirement:**

identifier "com.Delinea.ConnectionManager" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /\* exists \*/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /\* exists \*/ and certificate leaf[subject.OU] = UJDHBB2D6Q

- **Services and Key Values:**

- **ScreenCapture:** AllowStandardUserToSetSystemService
- **ListenEvent:** AllowStandardUserToSetSystemService

## Command Line Arguments

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

- -disablelocalvault
- -logo
- -logocollapsed
- -ssauth
- -ssname
- -ssurl

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

**Important:** /quiet mode installation works only with Administrative privileges. If a user without administrator privileges runs the MSI with /quiet mode, nothing happens.

Use this argument to disable the local vault on installation:

-disablelocalvault

### Example

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

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

-logo, -logocollapsed

### Example

```
Thycotic.ConnectionManager.WindowsInstaller.msi /quiet RUNCM=runCM KEYS="-logo "/Library/Application Support/Thycotic2/Connection Manager/Resources2/logo.png" -logocollapsed "/Library/Application Support/Thycotic2/Connection Manager/Resources2/logo_collapsed.png"
```

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

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

Two files are necessary to use custom logos:

1. Logo.png - 50 x 250 pixels
2. Logo\_collapsed.png - 50 x 100 pixels

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

-ssurl, -ssname, -ssauth

### Local Connection

#### Example

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



local"

## Web Connection

### Example

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

## 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.

Data File Location\*  [Browse](#)

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

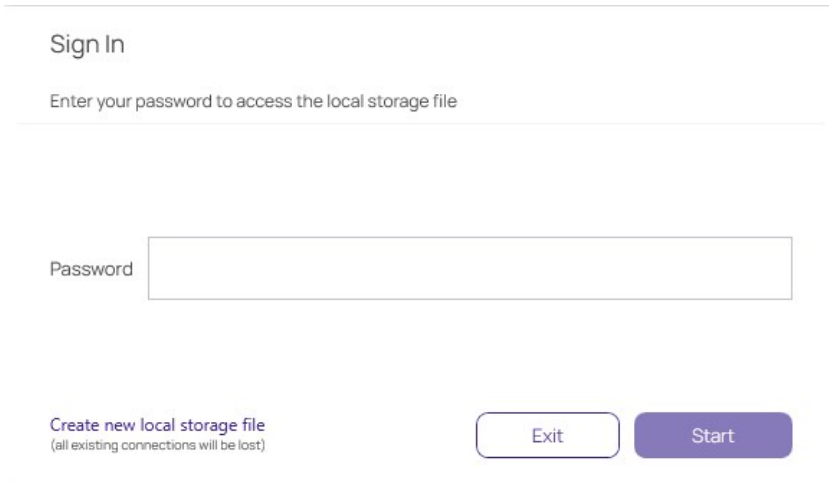
Confirm Password\*

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

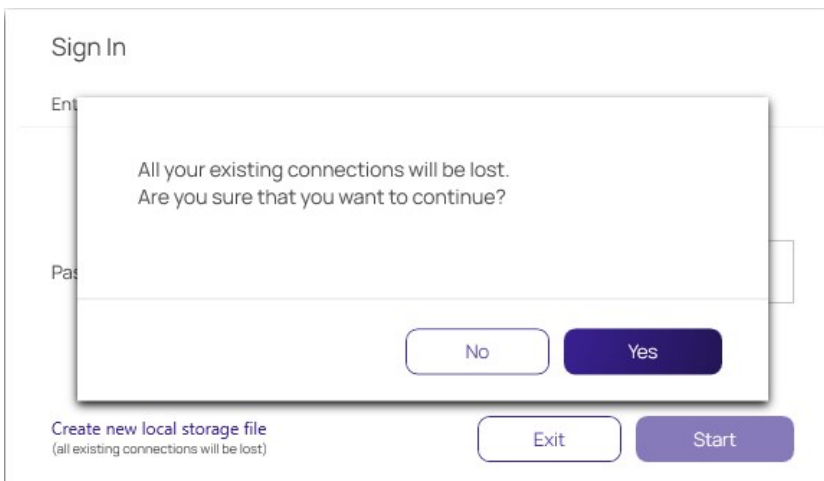
Password

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

Exit Start

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

Password

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

Exit Start

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

No Yes

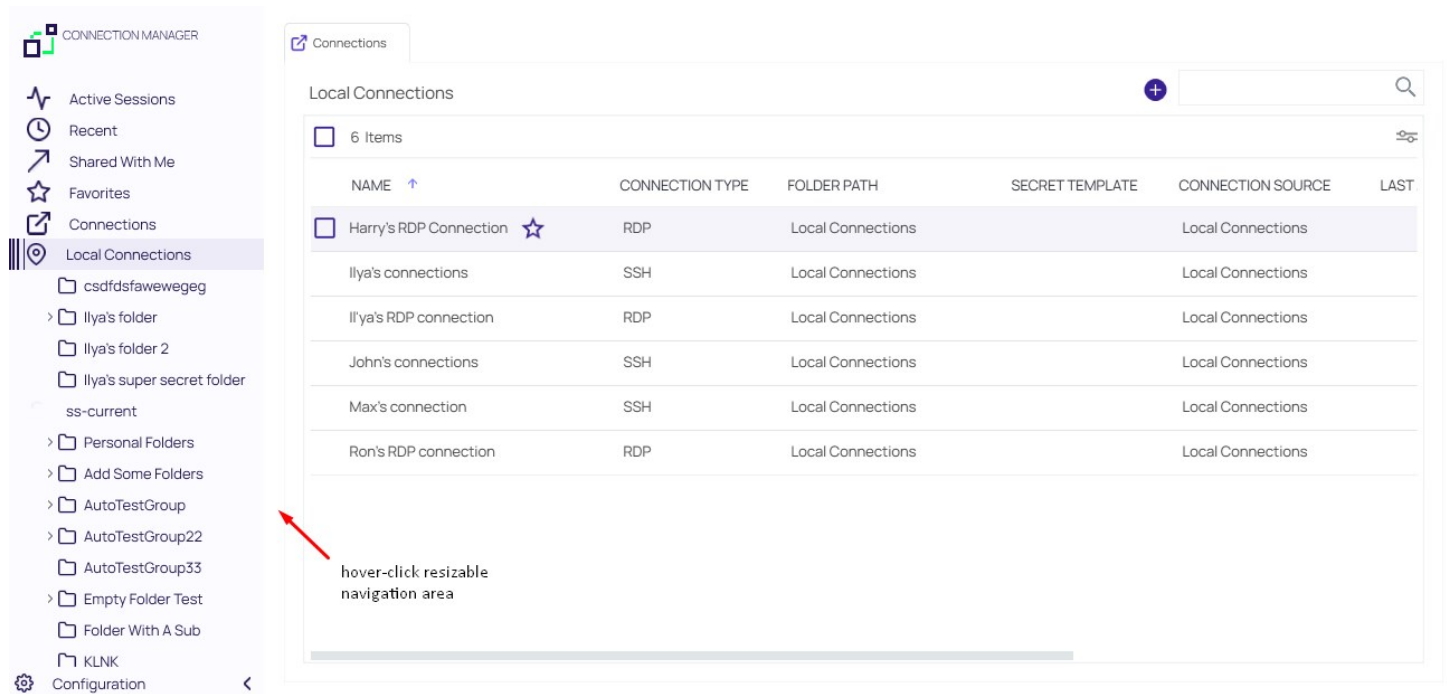
Users of Secret Server's modern interface will find Connection Manager's interface and functionality to be similar in look and feel. The interface takes advantage of some client-side functionality such as right-click menus, double-click menus, and others.

- [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.

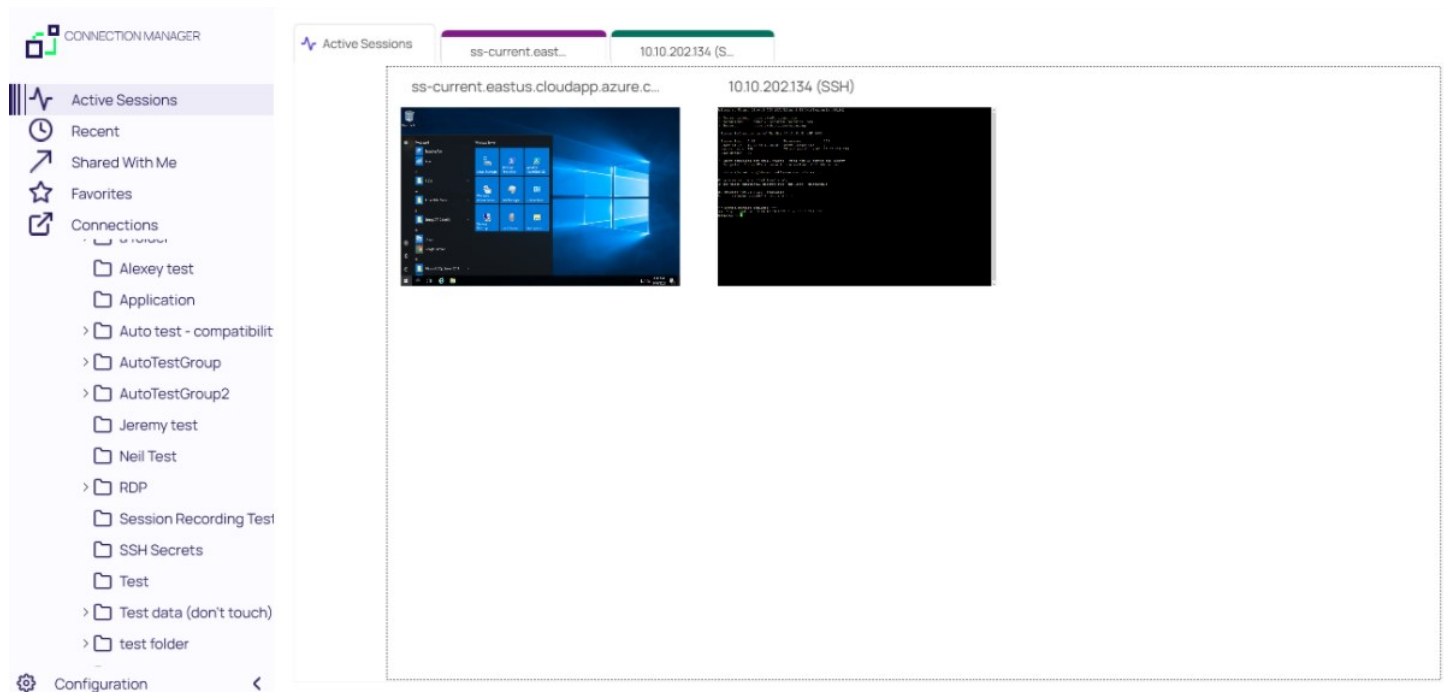
The two sections work in concert with each other.



The navigation area is hover-click resizable.

## Active Sessions

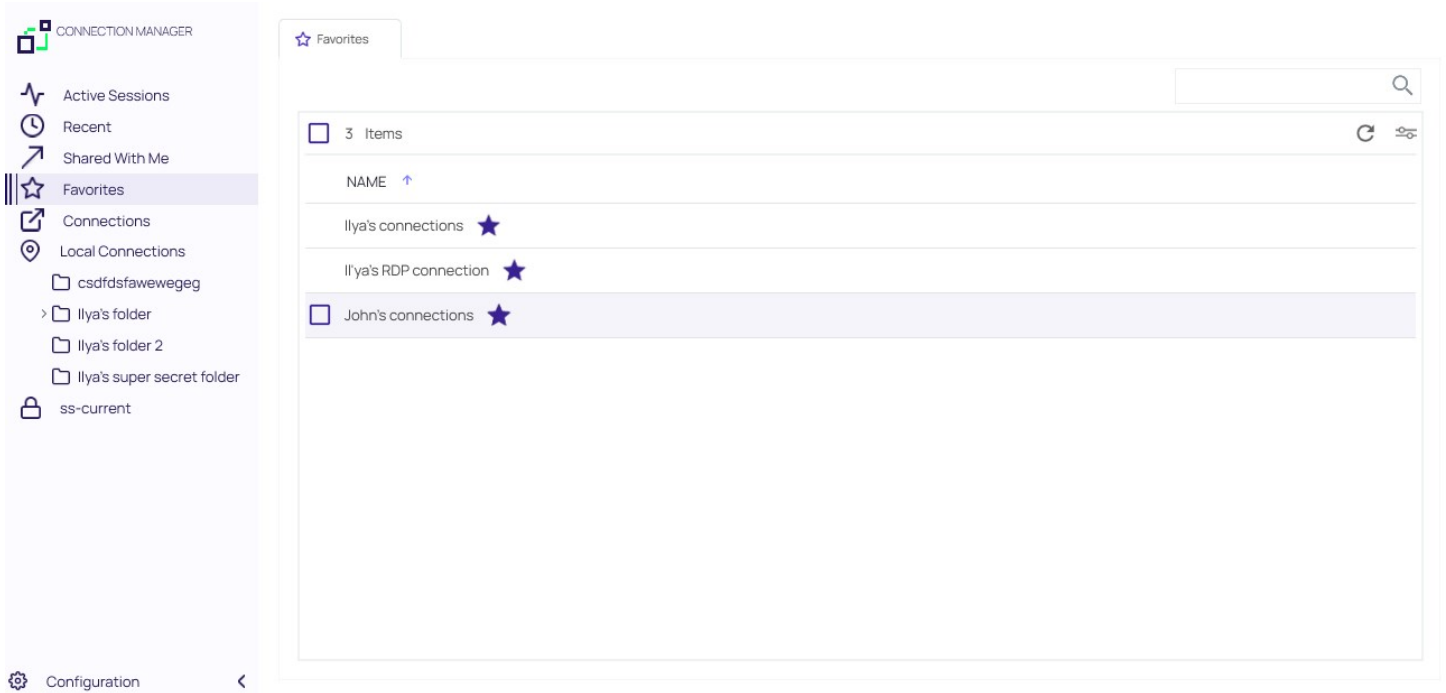
Select to view all active sessions.



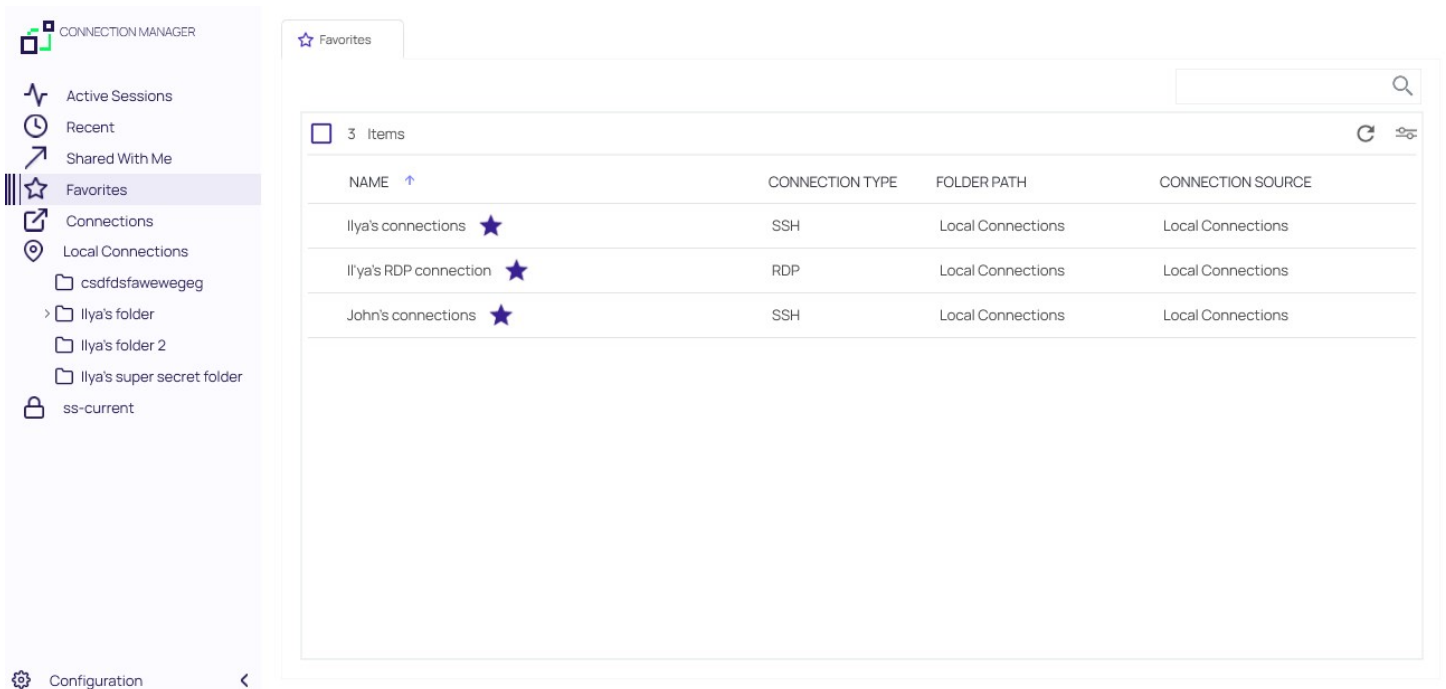
## Favorites

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:



Favorites page showing local and Secret Server connection favorites:



## Shared With Me

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



CONNECTION MANAGER

- Active Sessions
- Recent
- Shared With Me
- Favorites
- Connections
- Local Connections
  - csdfsfawewegeg
  - Ilya's folder
  - Ilya's folder 2
  - Ilya's super secret folder
- ss-current
- Personal Folders
  - Max
  - Add Some Folders
  - AutoTestGroup
  - AutoTestGroup22
  - AutoTestGroup33
  - Empty Folder Test
  - Folder With A Sub
- Configuration

Shared With Me

16 Items

NAME	CONNECTION TYPE	FOLDER PATH	CONNECTION SOURCE
AD IBM 10.7	Active Directory Acc...		ss-current
ibm 7.2	Windows Account		ss-current
permissions - edit	Windows Account	ss-current/Personal Folders/Ma	ss-current
permissions - list	Windows Account	ss-current/Personal Folders/Ma	ss-current
permissions - view	Windows Account	ss-current/Personal Folders/Ma	ss-current
Request Access secret	Unix Account (SSH)	ss-current/Personal Folders/Ma	ss-current
Require Approval for MAX	Unix Account (SSH)		ss-current
Require aproval	Active Directory Acc...		ss-current
restricted SSH	Unix Account (SSH)	ss-current/Personal Folders/Ma	ss-current
Root folder secret	Active Directory Acc...	ss-current	ss-current

Double clicking on these Secrets will launch sessions.

## Recent

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

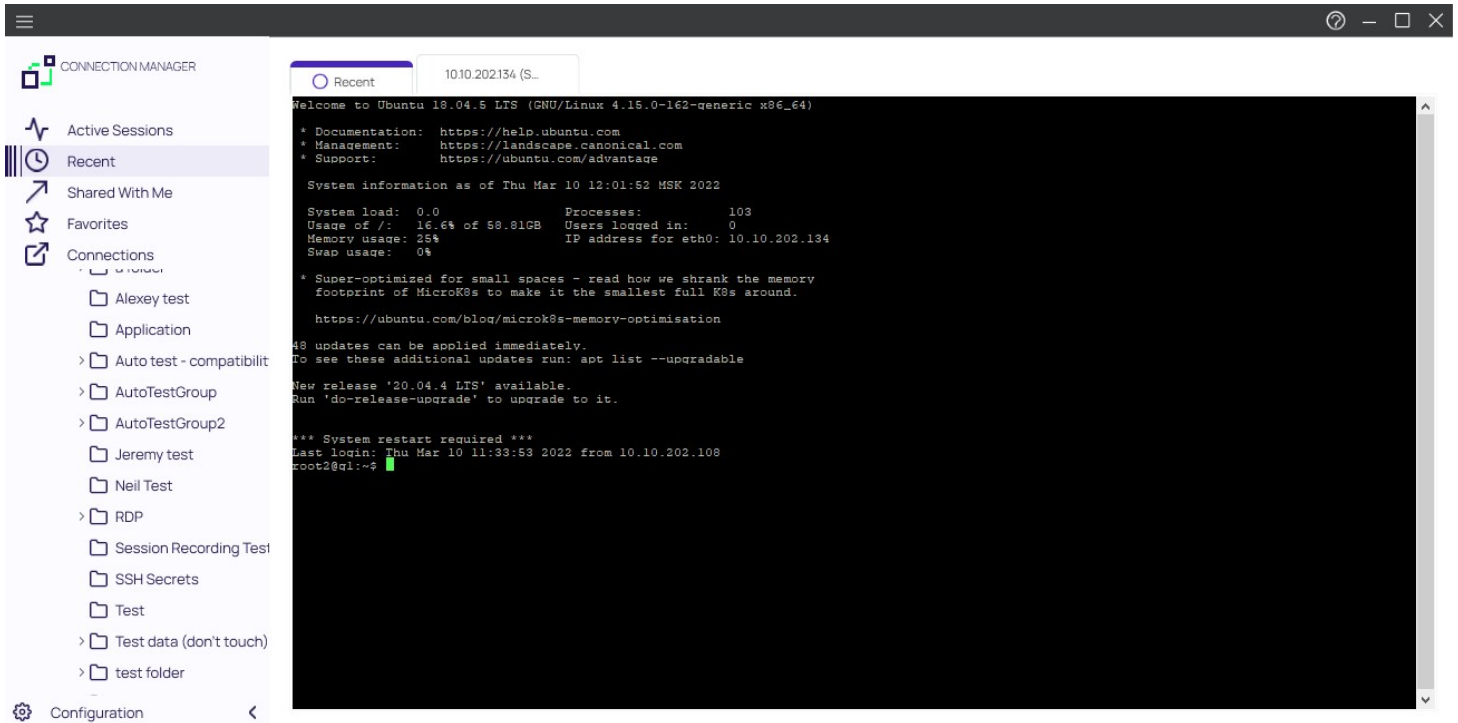
CONNECTION MANAGER

- Active Sessions
- Recent
- Shared With Me
- Favorites
- Connections
- Local Connections
  - csdfsfawewegeg
  - Ilya's folder
  - Ilya's folder 2
  - Ilya's super secret folder
- ss-current
- Personal Folders
  - Max
  - Add Some Folders
  - AutoTestGroup
  - AutoTestGroup22
  - AutoTestGroup33
  - Empty Folder Test
  - Folder With A Sub
- Configuration

Recent

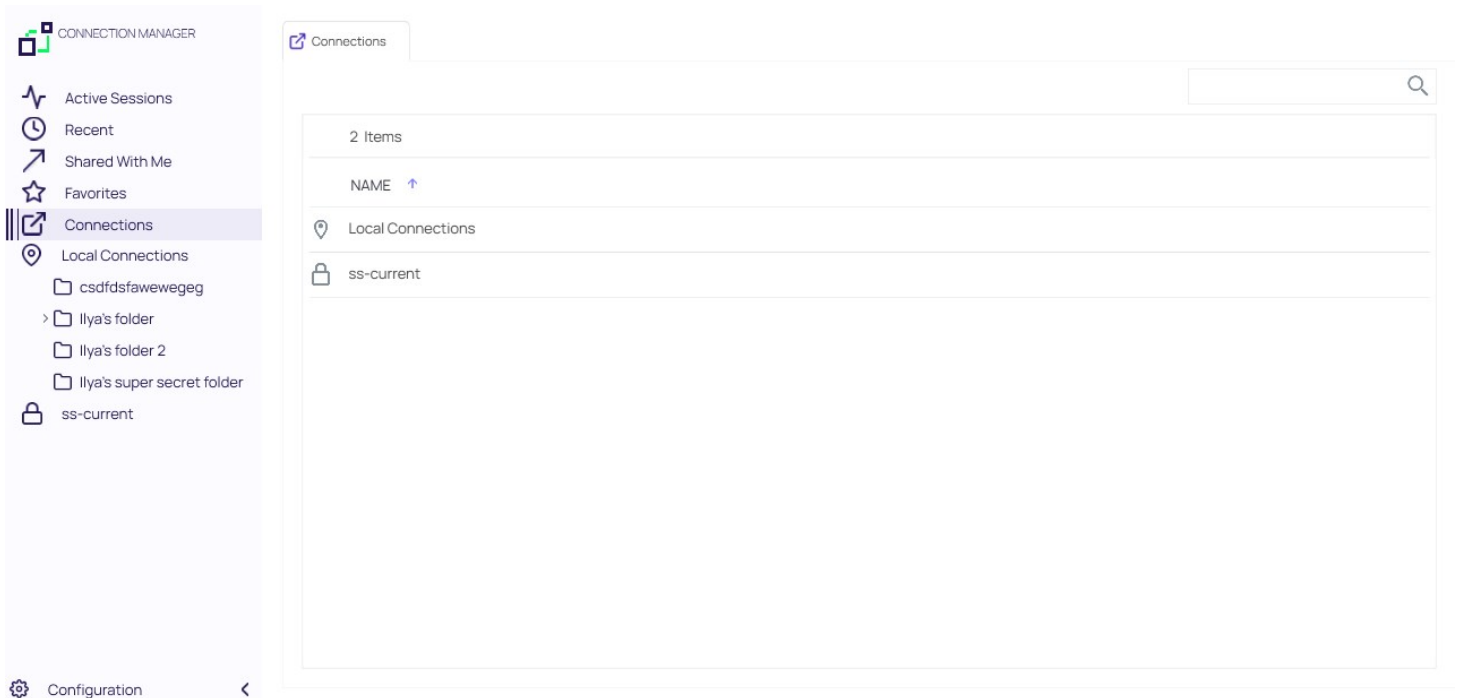
NAME	CONNECTION SOURCE	CONNECTION TYPE	LAST ACCESS
RDP	ss-current		49 seconds ago
SSH	ss-current	Unix Account (SSH)	31 minutes ago
SSH - recording session	ss-current	Unix Account (SSH)	34 minutes ago
RDP Proxy	ss-current	Windows Account	35 minutes ago
Harry's RDP Connection	Local Connections	RDP	19 hours ago
Ilya's connections	Local Connections	SSH	19 hours ago
Ilya's RDP connection	Local Connections	RDP	19 hours ago
Ron's RDP connection	Local Connections	RDP	19 hours ago
John's connections	Local Connections	SSH	19 hours ago

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

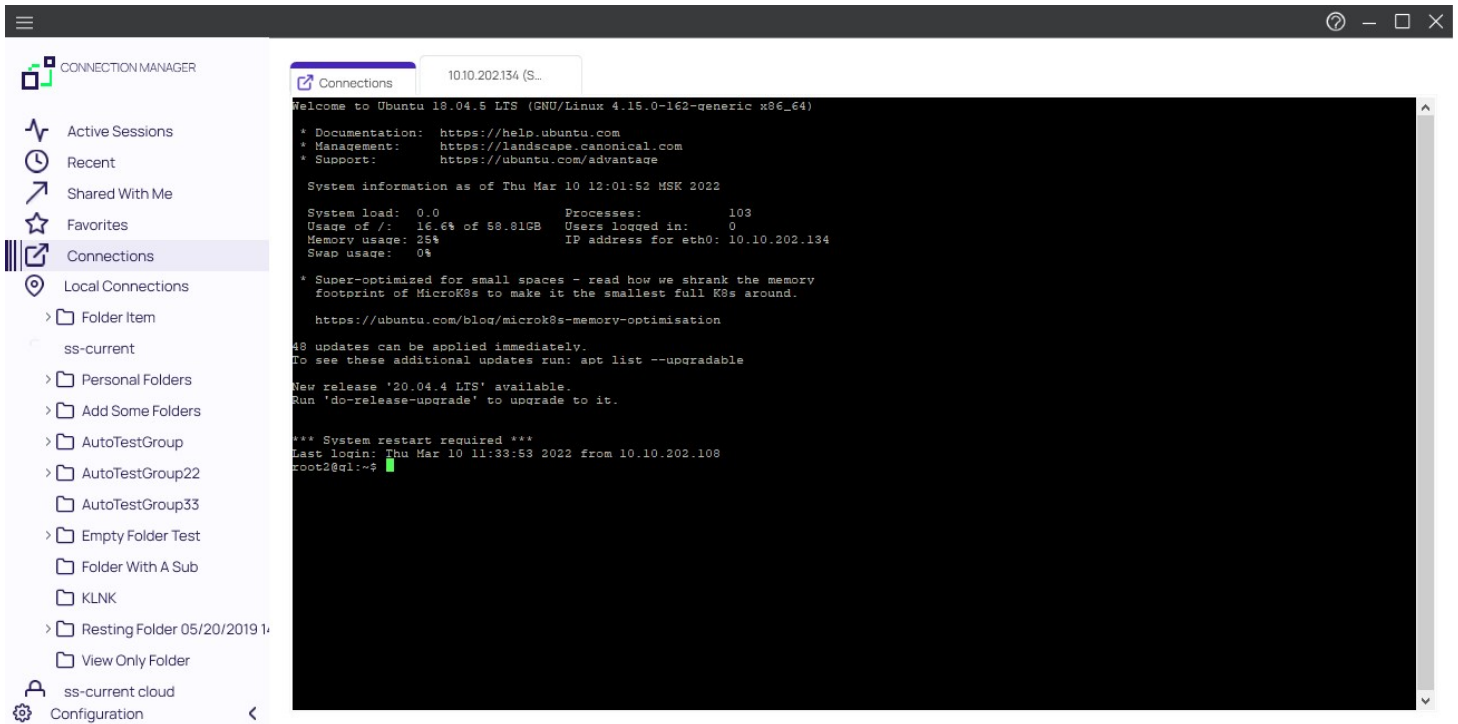


## Connections

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



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



## Local Connections

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

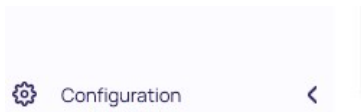
## Shared with me

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

## Configuration

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

- Secret Server Connections and
- Global Configurations.



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

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.

The screenshot displays the 'Connections' interface. The breadcrumb path is 'ss-current > Personal Folders > Max > Test data (don't tou...'. The main area shows a table with 16 items. The selected item, 'shared SSH', has its properties displayed in a side panel.

NAME	SECRET TEMPLATE	FOLDER PATH	CONNECTION SO
test for SS update		ss-current/Personal Folders...	
RDP	Windows Account	ss-current/Personal Folders...	ss-current
RDP (1920x1080)	Windows Account	ss-current/Personal Folders...	ss-current
RDP - recording session	Windows Account	ss-current/Personal Folders...	ss-current
RDP for SSH Tunneling with SSH...	Windows Account	ss-current/Personal Folders...	ss-current
RDP Proxy	Windows Account	ss-current/Personal Folders...	ss-current
shared SSH	Unix Account (SSH)	ss-current/Personal Folders...	ss-current
SSH	Unix Account (SSH)	ss-current/Personal Folders...	ss-current
SSH - recording session	Unix Account (SSH)	ss-current/Personal Folders...	ss-current
SSH Proxy	Unix Account (SSH)	ss-current/Personal Folders...	ss-current

The properties panel for 'shared SSH' includes:

- Machine:** 10.10.202.134
- Username:** root2
- Password:** [Redacted] [Show](#)
- Launchers:**
  - PuTTY-SSH
  - putty X11 forwarding

**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

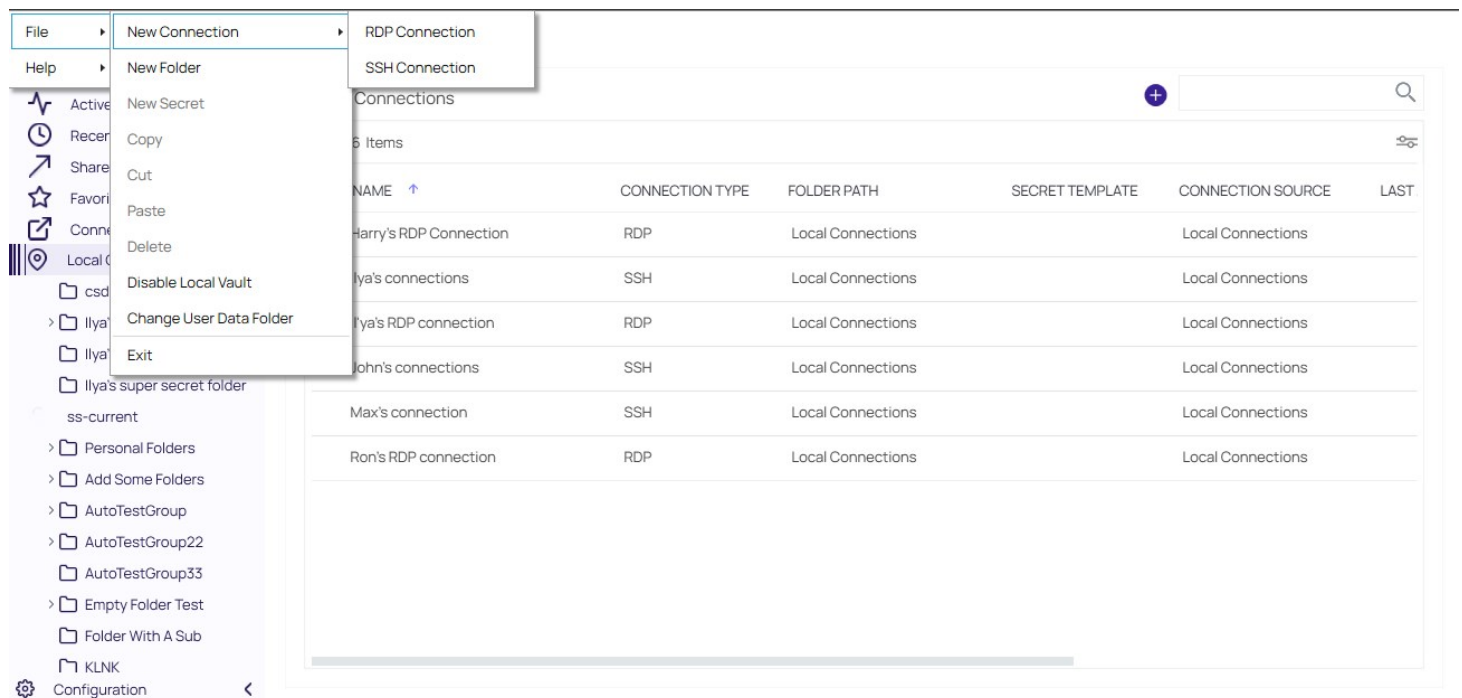
The menu at the top left of the application allows you to select File and Help.



### File

Under File you can do the following:

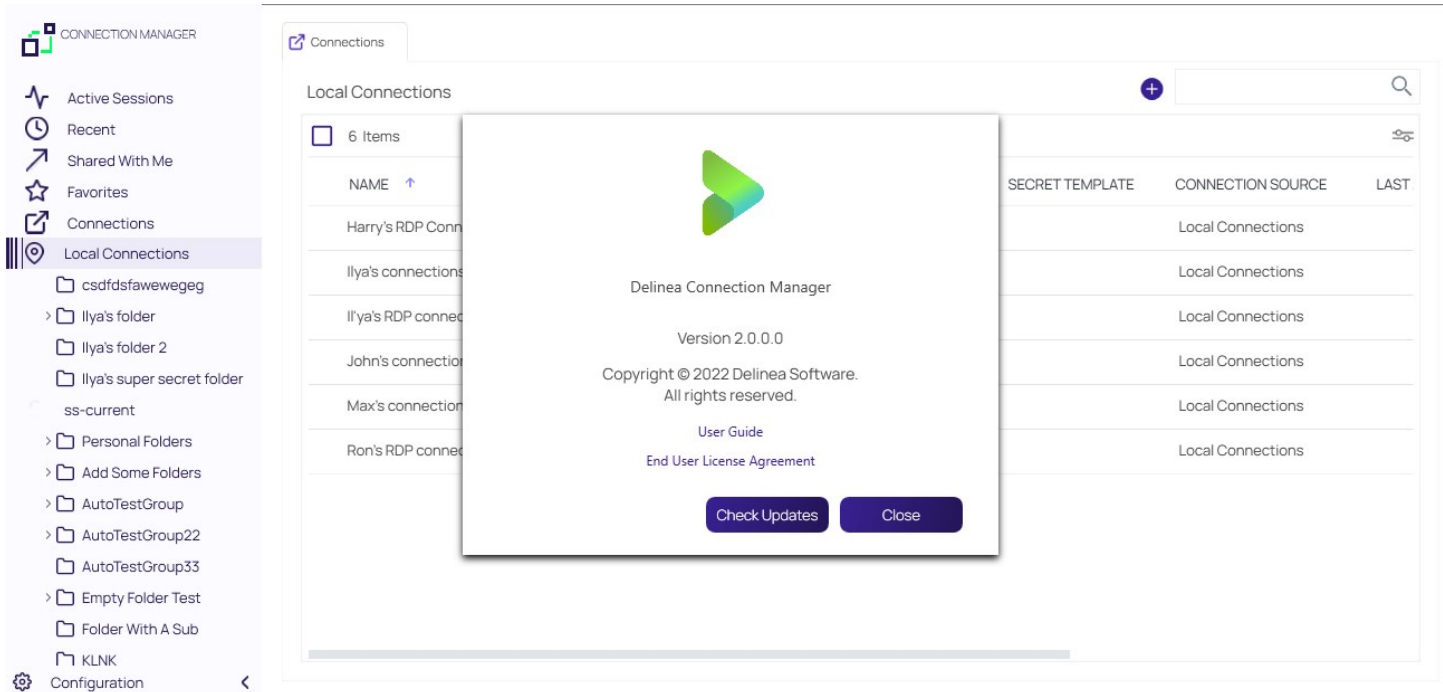
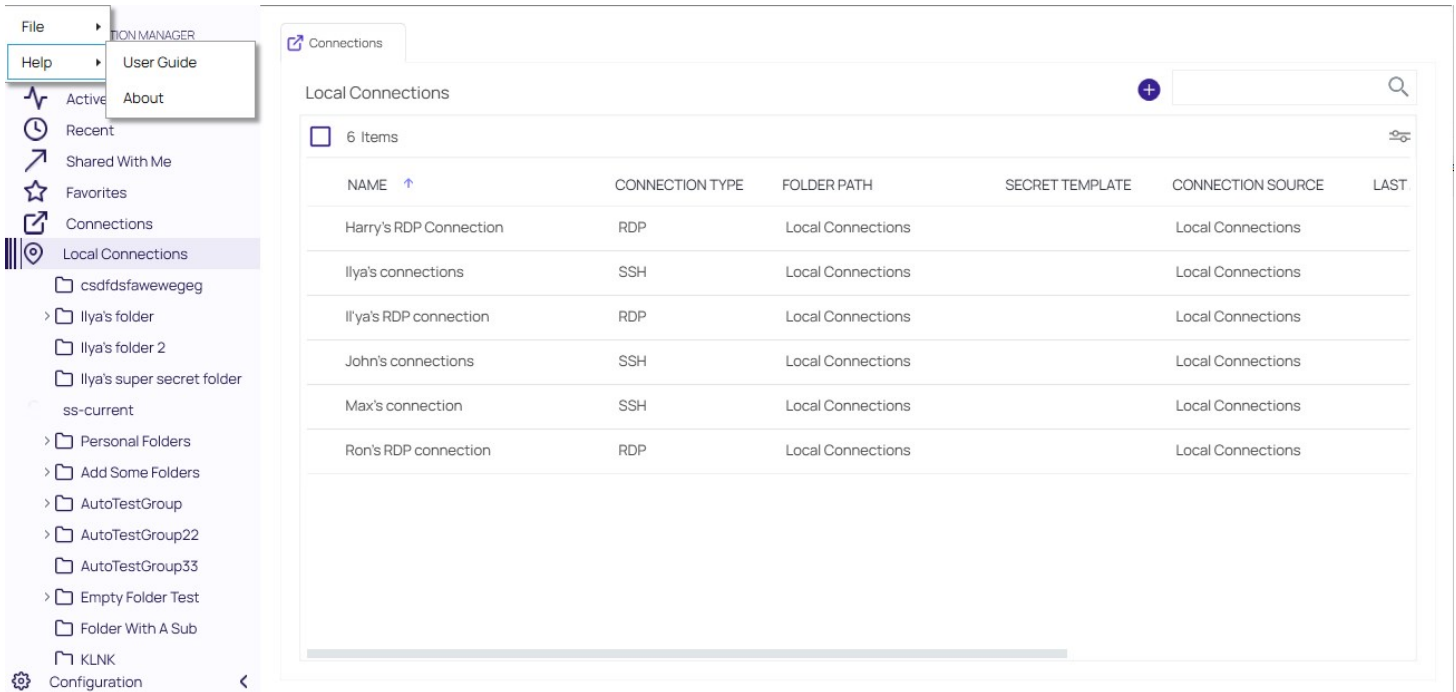
- Create new connections (RDP or SSH)
- Create new folders
- Delete folders/connections
- Exit the application



**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:



## 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 REST APIs
- 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.

### Create a Secret Server Connection

Step 1 of 3: Please, enter Secret Server parameters

---

Secret Server Name\*

Secret Server URL\*

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** or **Web Login**

Click **Next**.

3. On the Step 2 of 3 dialog complete:

## Create a Secret Server Connection

Step 2 of 3: Please, enter your credentials

Username*	<input type="text"/>
Password*	<input type="password"/>
Domain	<input type="text"/>
Two Factor:	Select two factor authentication that applies: <input checked="" type="radio"/> None <input type="radio"/> Pin Code <input type="text"/> <input type="radio"/> Duo Push <input type="radio"/> Duo Phone Call
Remember me:	<input type="checkbox"/> Store credentials locally
Launch automatically	<input type="checkbox"/>

- **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.

## Create a Secret Server Connection

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

6 Selected

- Active Directory Account
- Active Directory Account - Resticted Launch
- Active Directory Account alternate
- AD - List Launch
- 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

Back

Cancel

Finish

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](#)



ss-current

[Edit](#)

https://connmanagerss.thycotic.net/ss-current

[Remove](#)

[Close](#)

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 lose your internet connection to Secret Server, Connection Manager retains your authentication for several minutes and displays the dialog, **Attempting to Auto-reconnect to [Secret Server name]**, with options to Cancel the attempt or to manually Reconnect. After more than three minutes of unsuccessful attempts to reconnect, the dialog closes and the Connect dialog opens.

If you are using SAML, follow these steps:

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

## Create a Secret Server Connection

Step 1 of 3: Please, enter Secret Server parameters

---

Secret Server Name\*

Secret Server URL\*

Authentication Type:  Local Username/Password  
 Web Login

Cancel

Next

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. In the dialog **Step 2 of 3**, select the login method: Gamma (AAD) or Com Man Okta. Your login method will be the same as the method your administrator used to create your account and cannot be changed.

## Create a Secret Server Connection

Step 2 of 3: Please, enter your credentials

 **Secret Server**  
Log in using Identity Provider

-  Gamma (AAD)
-  Com Man SS Okta (Current)

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.

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

## Create a Secret Server Connection

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

Search for Template Name

6 Selected

- Active Directory Account
- Active Directory Account - Resticted Launch
- Active Directory Account alternate
- AD - List Launch
- 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

Back

Cancel

Finish

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



## Secret Server Connections

[Add a Connection](#)



ss-current

[Edit](#)

<https://connmanagerss.thycotic.net/ss-current>

[Remove](#)

[Close](#)

Customers using Secret Server version 11.2 and newer can create a new Secret Server connection via an external browser.

**Note:** Connection via external browser is only available to customers using Connection Manager version 1.9 and newer.

1. Select **External Browser** from the dropdown menu


## Create a Secret Server Connection

Step 1 of 1: Summary text

Secret Server Name \*

Secret Server URL \*

Authentication Type

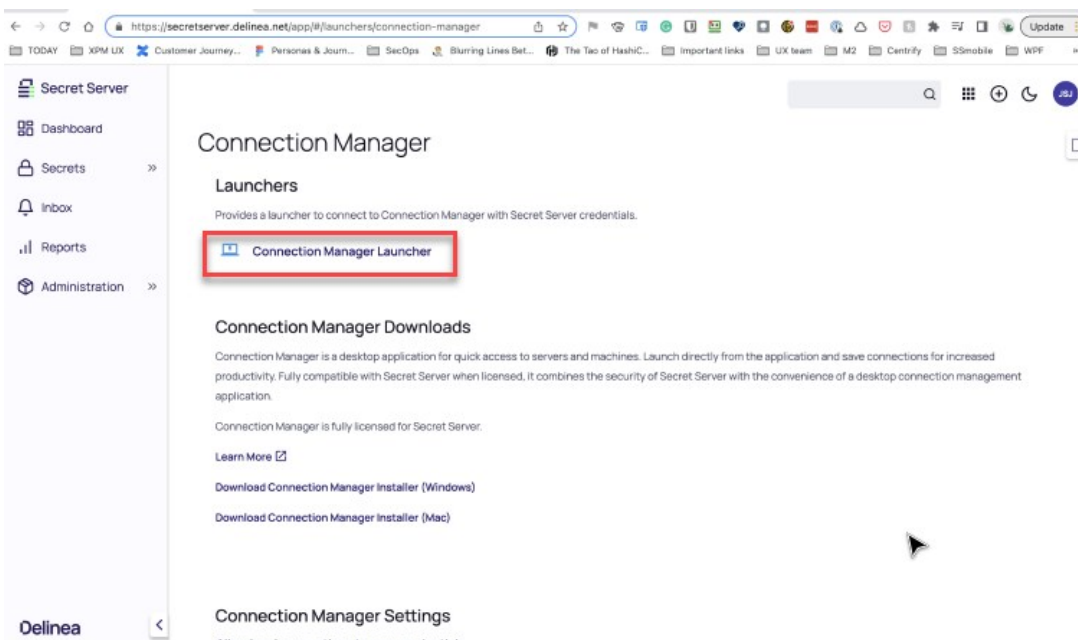
 To continue, set Connection Manager as your default protocol handler for Secret Server.  
[Set as default](#)

Cancel

Next

**Note:** To continue, Connection Manager must be set as your default protocol handler for Secret Server

- Input the Secret Server Name and URL and click **Next**. Your browser will then open Secret Server and you will be prompted to login, unless you have already done so.
- Once you are signed in, the browser will then redirect you to the Connection Manager page where you will need to click **Connection Manager Launcher**.



Secret Server

Dashboard

Secrets >

Inbox

Reports

Administration >

### Connection Manager

#### Launchers

Provides a launcher to connect to Connection Manager with Secret Server credentials.

**Connection Manager Launcher**

#### Connection Manager Downloads

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.

Connection Manager is fully licensed for Secret Server.

[Learn More](#)

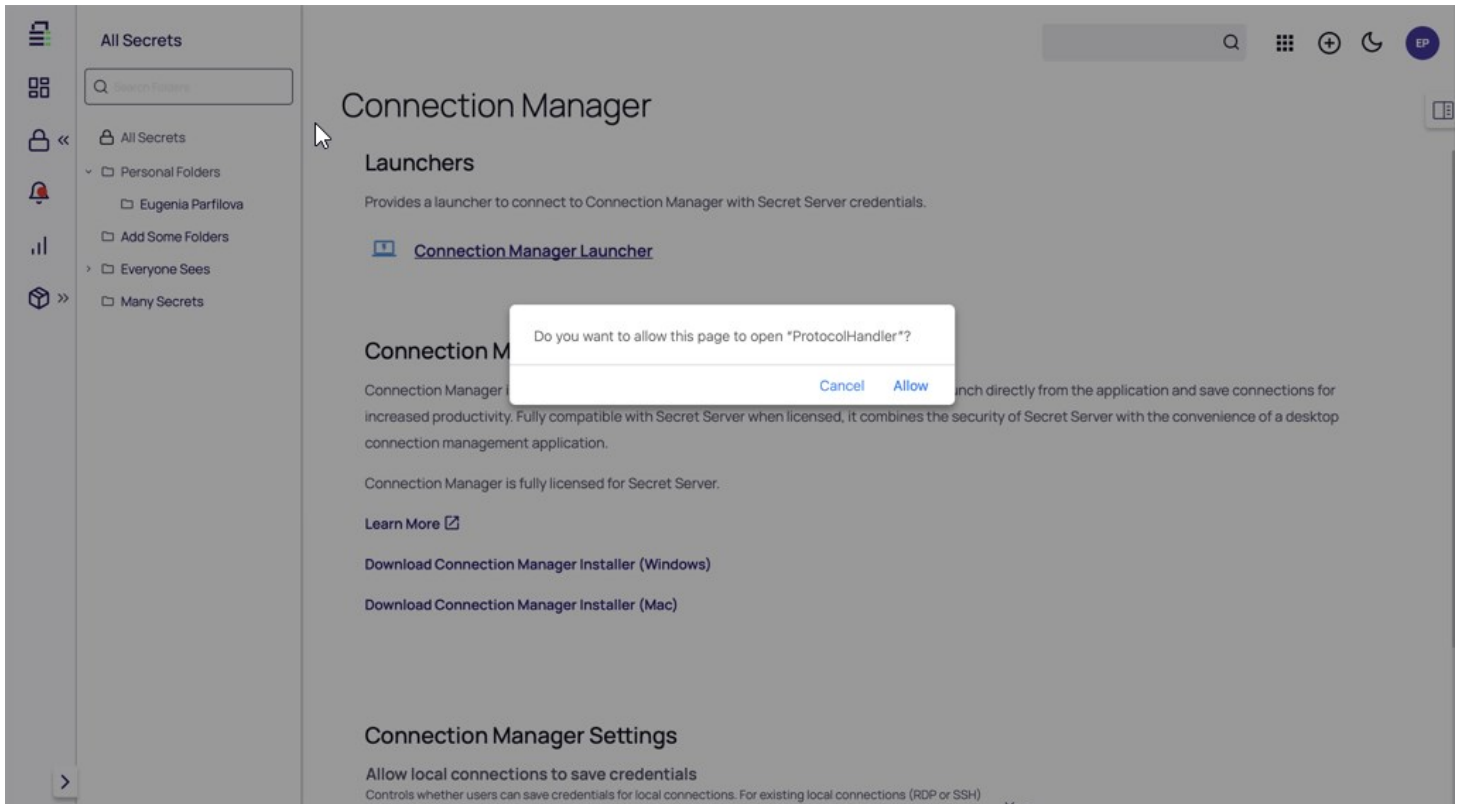
[Download Connection Manager Installer \(Windows\)](#)

[Download Connection Manager Installer \(Mac\)](#)

Connection Manager Settings

Delinea

4. Click **Allow** to open the Protocol Handler.



5. A loading page will be displayed as a connection to Secret Server is created.




Back

Cancel

Reload

6. You will be taken back to Secret Server to complete your connection.

Create a Secret Server Connection  
Step 2 of 3: Summary text

 **Must be on Secret Server Version XX.XXX**  
If you are on a lower version, please change versions in the previous step.

Go to browser to complete login  
Not seeing the browser tab? Click "Reload" below.

[Back](#) [Cancel](#) [Reload](#)

## 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 Secret Server Connection

Step 1 of 3: Please, enter Secret Server parameters

---

Secret Server Name\*

Secret Server URL\*

Authentication Type:  Local Username/Password  
 Web Login

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

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

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

## Edit Secret Server Connection

Step 2 of 3: Please, enter your credentials

---

Username*	<input type="text" value="max"/>
Password*	<input type="password" value="•"/>
Domain	<input type="text"/>
Two Factor:	Select two factor authentication that applies: <input checked="" type="radio"/> None <input type="radio"/> Pin Code <input type="text"/> <input type="radio"/> Duo Push <input type="radio"/> Duo Phone Call
Remember me:	<input checked="" type="checkbox"/> Store credentials locally
Launch automatically	<input type="checkbox"/>

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

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

## Edit Secret Server Connection

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

Search for Template Name

6 Selected

- Active Directory Account
- Active Directory Account - Resticted Launch
- Active Directory Account alternate
- AD - List Launch
- 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

Back

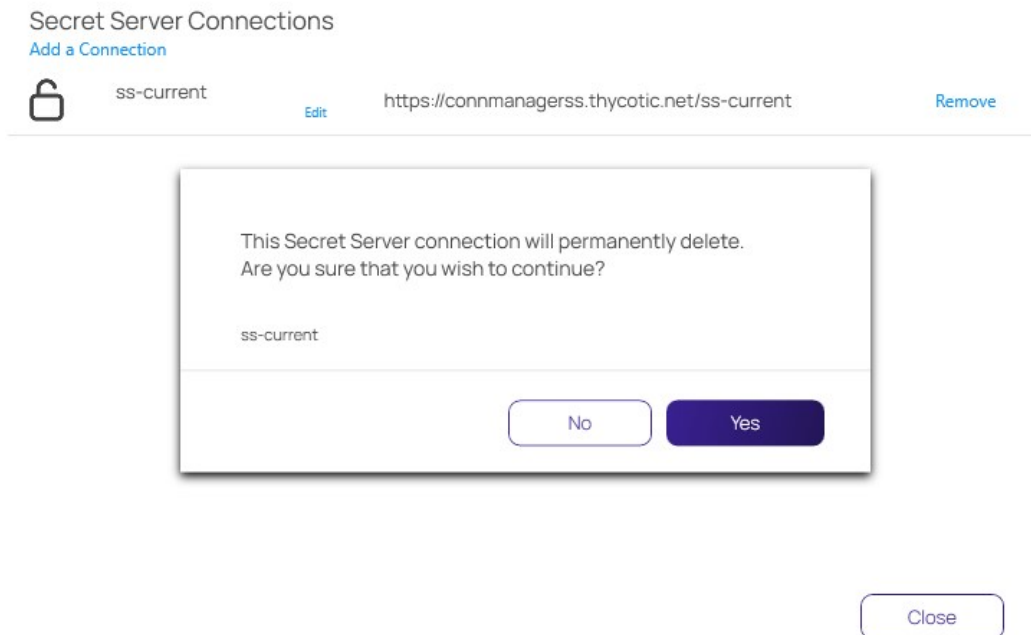
Cancel

Finish

## 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.



3. Click **Yes** to confirm.



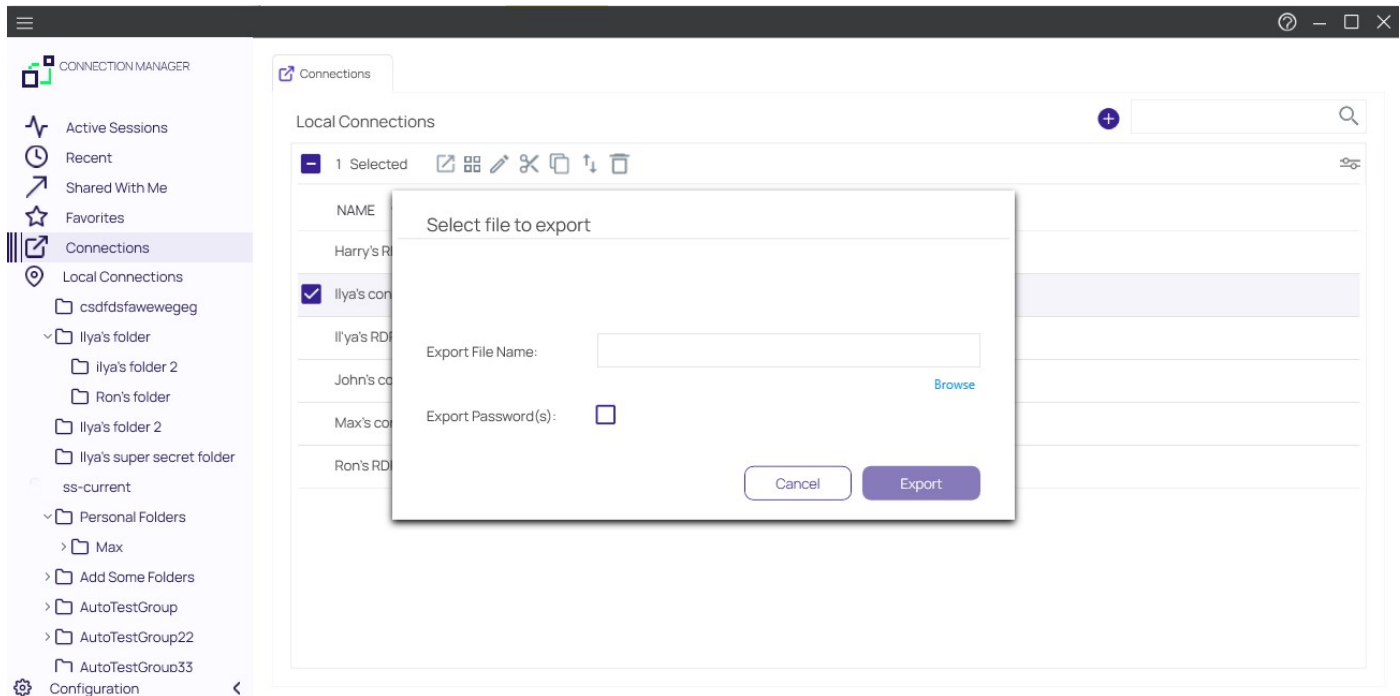
The following topics are available:

- [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.



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"
  },
]
}
```

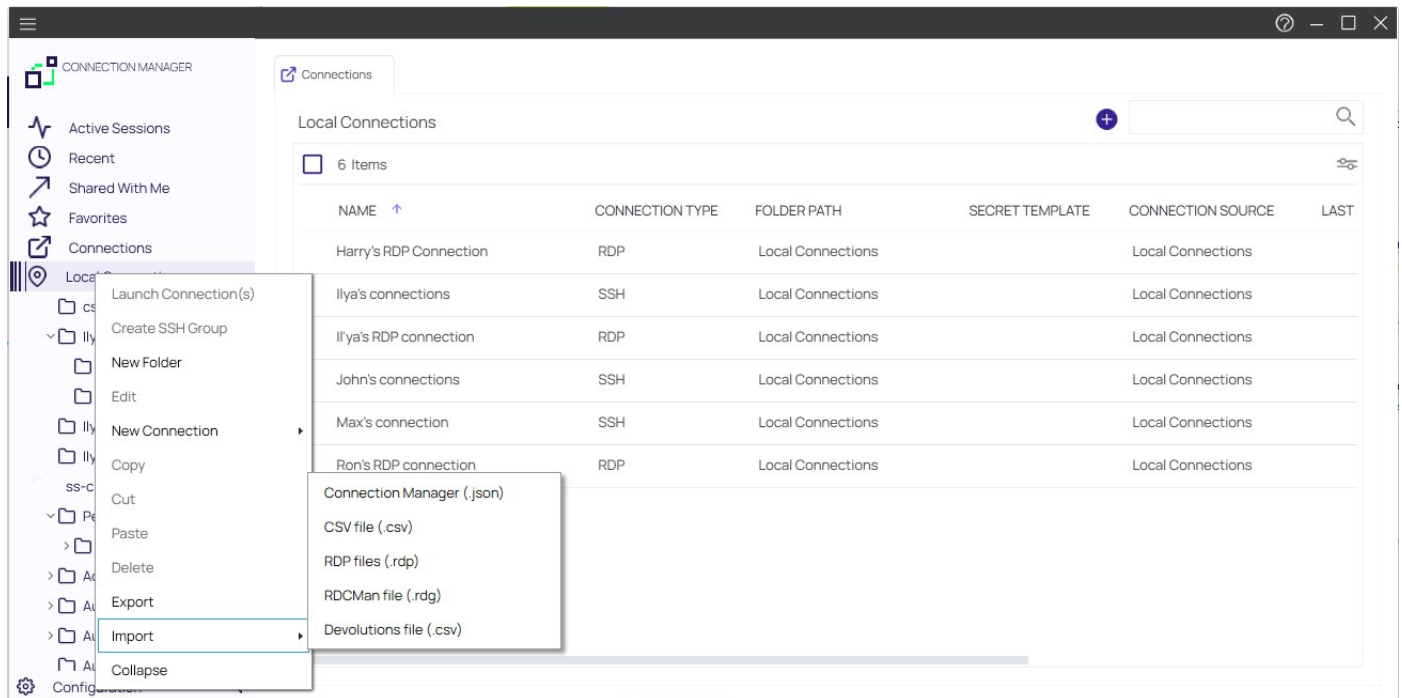
**Note:** The red text for the password field indicates that this part of the JSON file will only be included if the Export Password(s) option is used.



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\*  [Browse](#)

Connection Type\*

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	3
Computer Name *	Host name	3
Port	Port	3389
Credentials	Unmapped	
User Name	Username	EAM05\administrator
User Domain	Unmapped	
Password	Password	pbdaemon2005
Desktop Width	Custom width	1600
Desktop Height	Custom height	1200
Auto Expand	Auto expanding	False

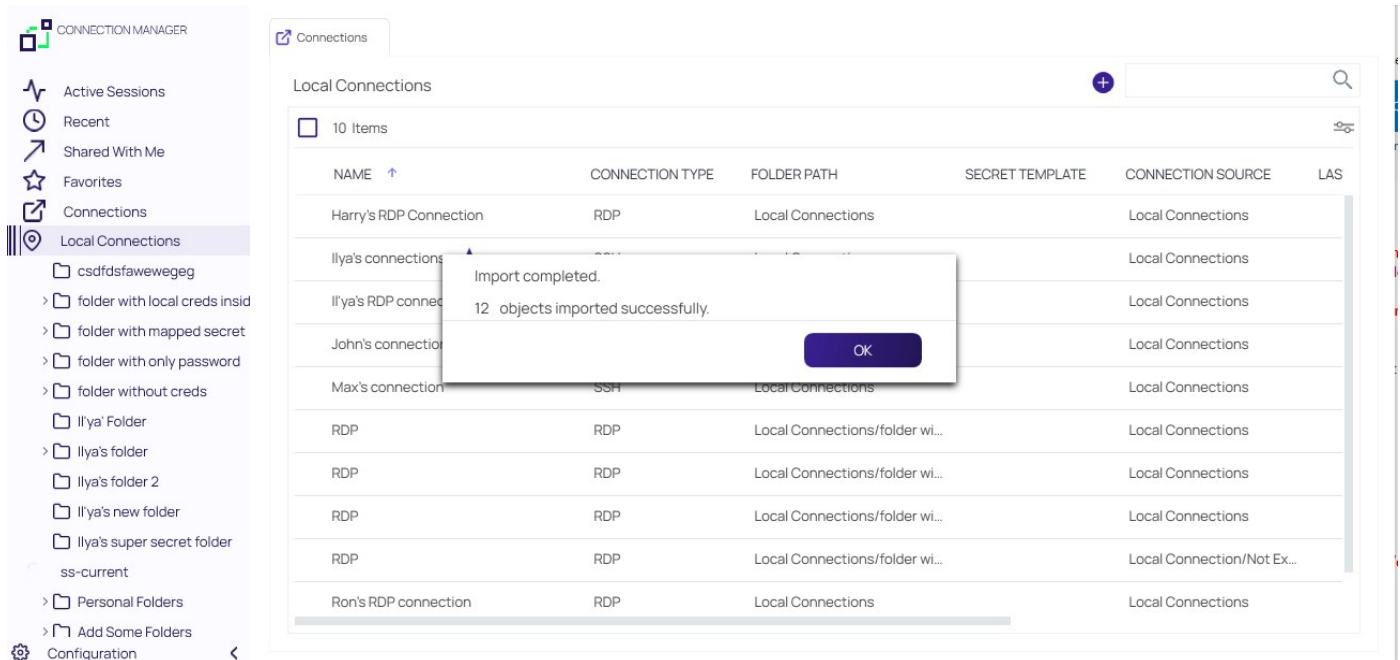
Back

Cancel

Finish

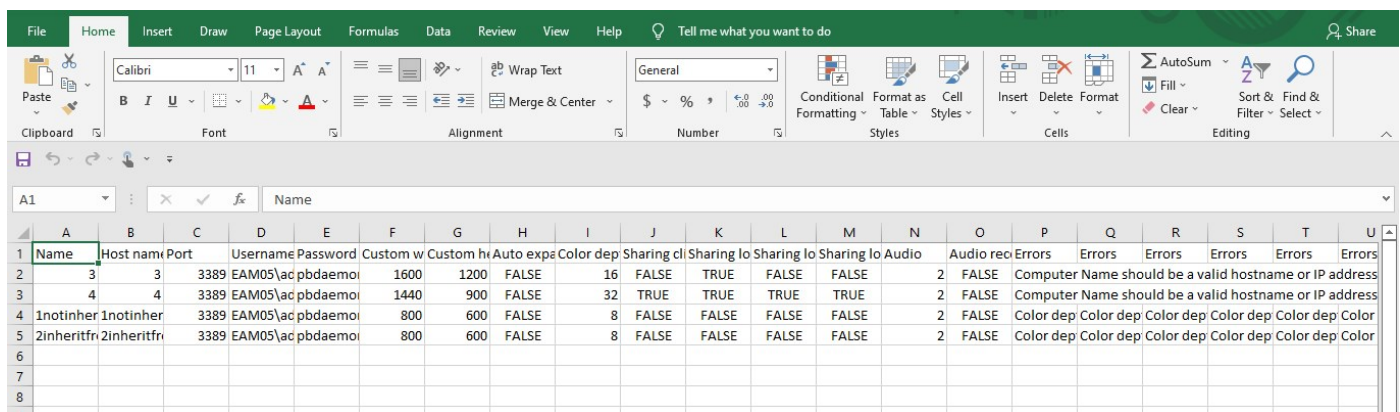
By default Connection Manager maps the data from the import file to field mappings for the local connection information. Any data not recognized/mapped is indicated as unmapped and duplicate mappings are highlighted red. These potential errors can be fixed prior to the import.

3. Click **Finish**.



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

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



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

- 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 *	URI	SS Con 1
Computer Name *	URI	SS Con 1
Port	Port	27
Credentials	Unmapped	
User Name	Unmapped	
User Domain	Unmapped	
Password	Unmapped	
Desktop Width	Unmapped	
Desktop Height	Unmapped	
Auto Expand	Unmapped	

Back

Cancel

Finish

## Field Values and Types

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

Field Name	Type	Supported Protocols	Options
<b>Connection Name</b> (required)	String	RDP, SSH	
<b>Computer Name</b> (required)	String	RDP, SSH	
<b>Port</b>	Number	RDP, SSH	1 - 65535
<b>Credentials</b>	Enumeration: 0,1,2	RDP, SSH	0 - None 1 - Inherited 2 - Embedded
<b>User Name</b>	String	RDP, SSH	
<b>User Domain</b>	String	RDP, SSH	

<b>Password</b>	String	RDP, SSH	Cleartext
<b>Desktop Width</b>	Number	RDP	
<b>Desktop Height</b>	Number	RDP	
<b>Auto Expand</b>	Boolean	RDP	TRUE FALSE Or 1 0
<b>Color Depth</b>	Number	RDP	15 16 24 32
<b>Run As Admin</b>	Boolean	RDP	
<b>Clipboard</b>	Boolean	RDP	
<b>Drives</b>	Boolean	RDP	
<b>Printer</b>	Boolean	RDP	
<b>Smart Cards</b>	Boolean	RDP	
<b>Audio Playback</b>	Enumeration: 0,1,2	RDP	0 - Use local computer 1 - Disabled 2 - Use remote computer
<b>Audio Recording</b>	Boolean	RDP	
<b>Remote Character Set</b>	String	SSH	
<b>Font</b>	String	SSH	
<b>Font Size</b>	Number	SSH	1-72
<b>Connection Type</b>	Enumeration: 1 - RDP, 2 - SSH		1 - RDP 2 - SSH

## Desktop Size

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

### //4:3 resolutions

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

- 1920x1440
- 2048x1536

## //16:10 resolutions

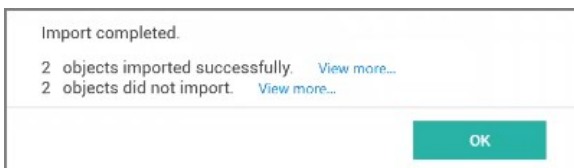
- 1280x800
- 1440x900
- 1680x1050
- 1920x1200
- 2560x1600
- 2880x1800

## //16:9 resolutions

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

## Import Completed Reports

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



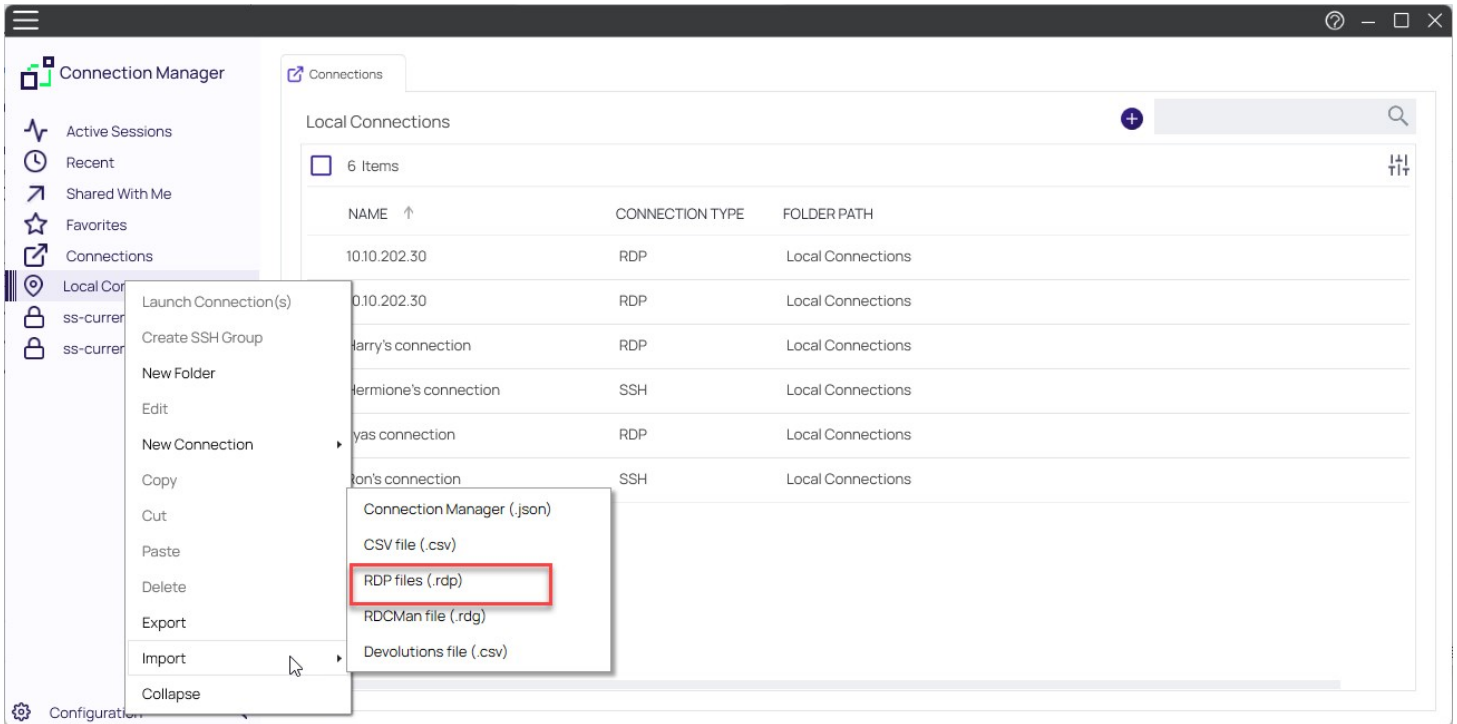
- Successful: This report lists all objects that have been successfully imported.
- Not imported: This report lists all objects that failed to import. The report can be used to remediate the import issue(s) and the remaining connections can be reimported.

## CSV Import Differences

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

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

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



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

## Import RDP files (.rdp)

Select RDP files



Browse

Cancel

Finish

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

## Import RDP files (.rdp)

Select RDP files

---

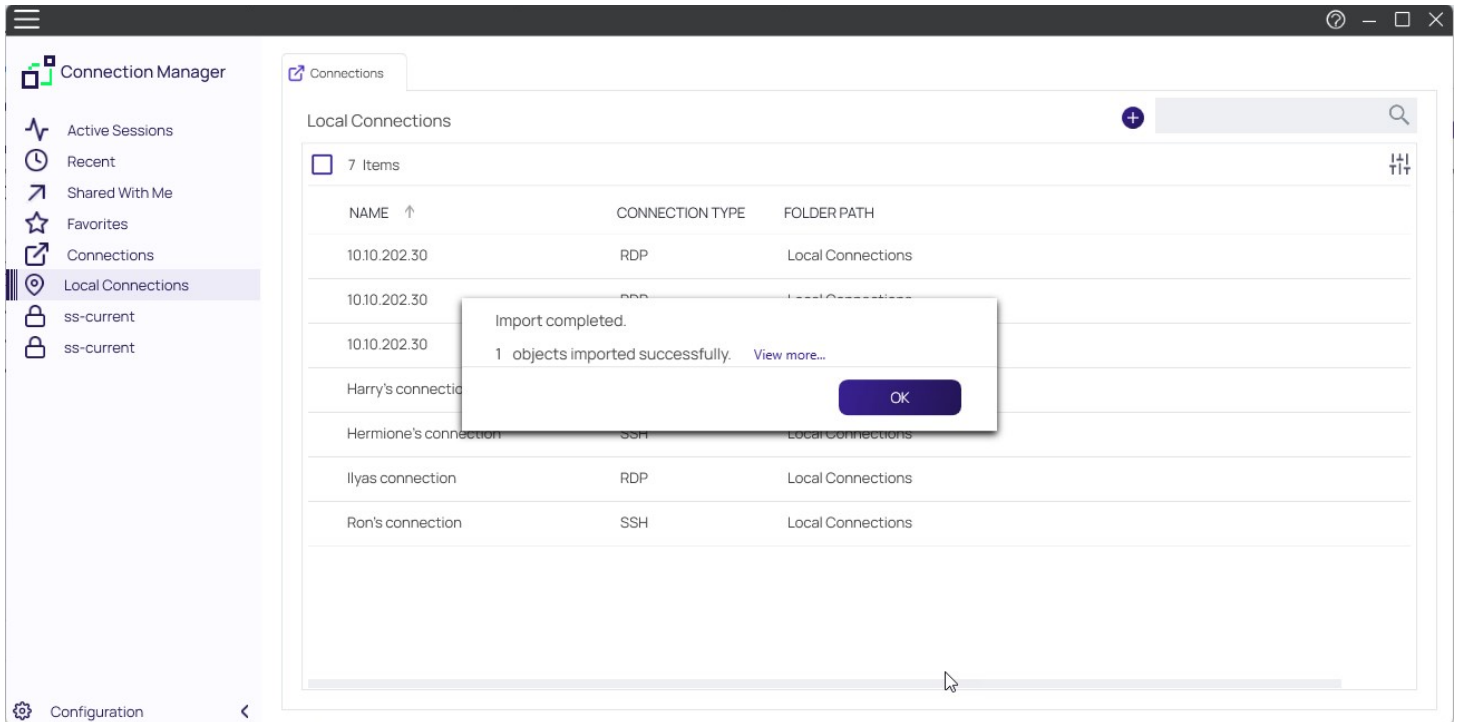
C:\Users\lilyus\Downloads\RDP Test.rdp	Remove
--	--------

Browse

Cancel Finish

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

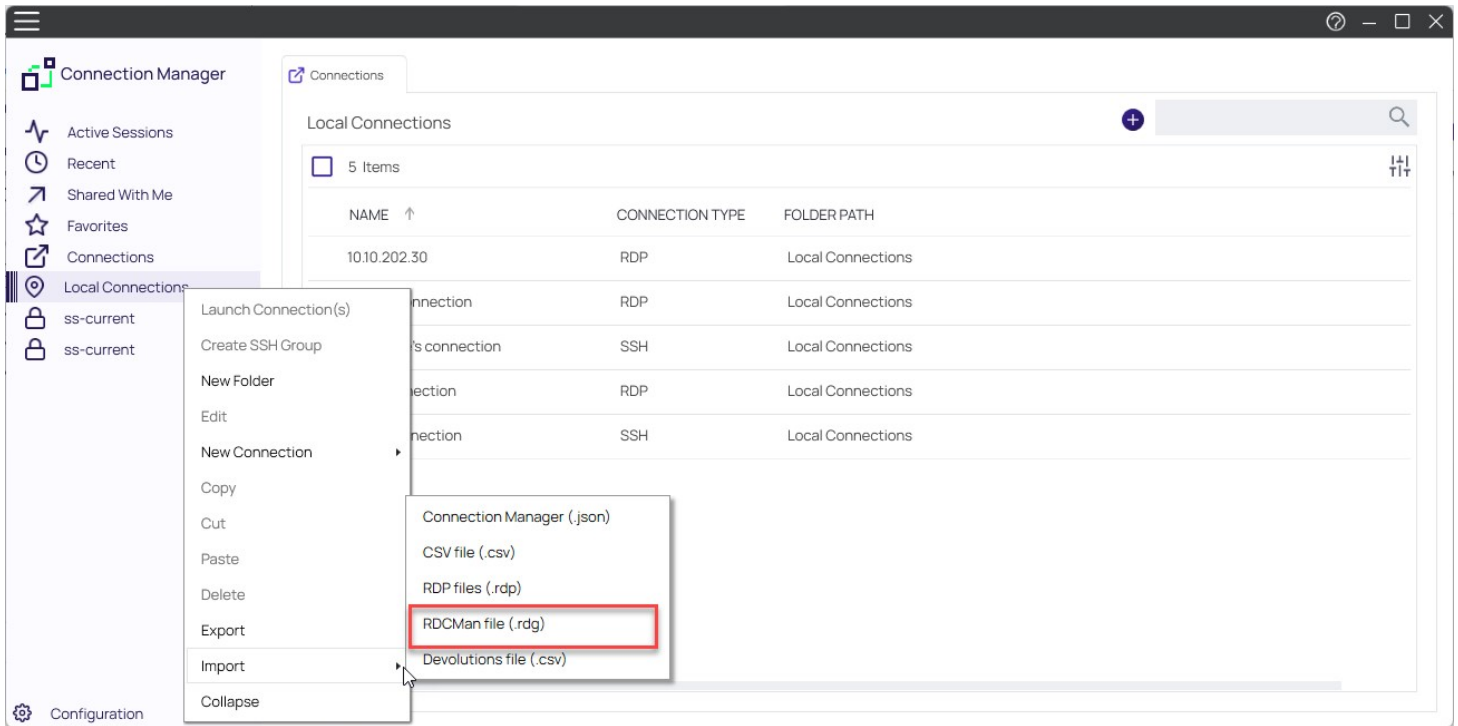
---



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

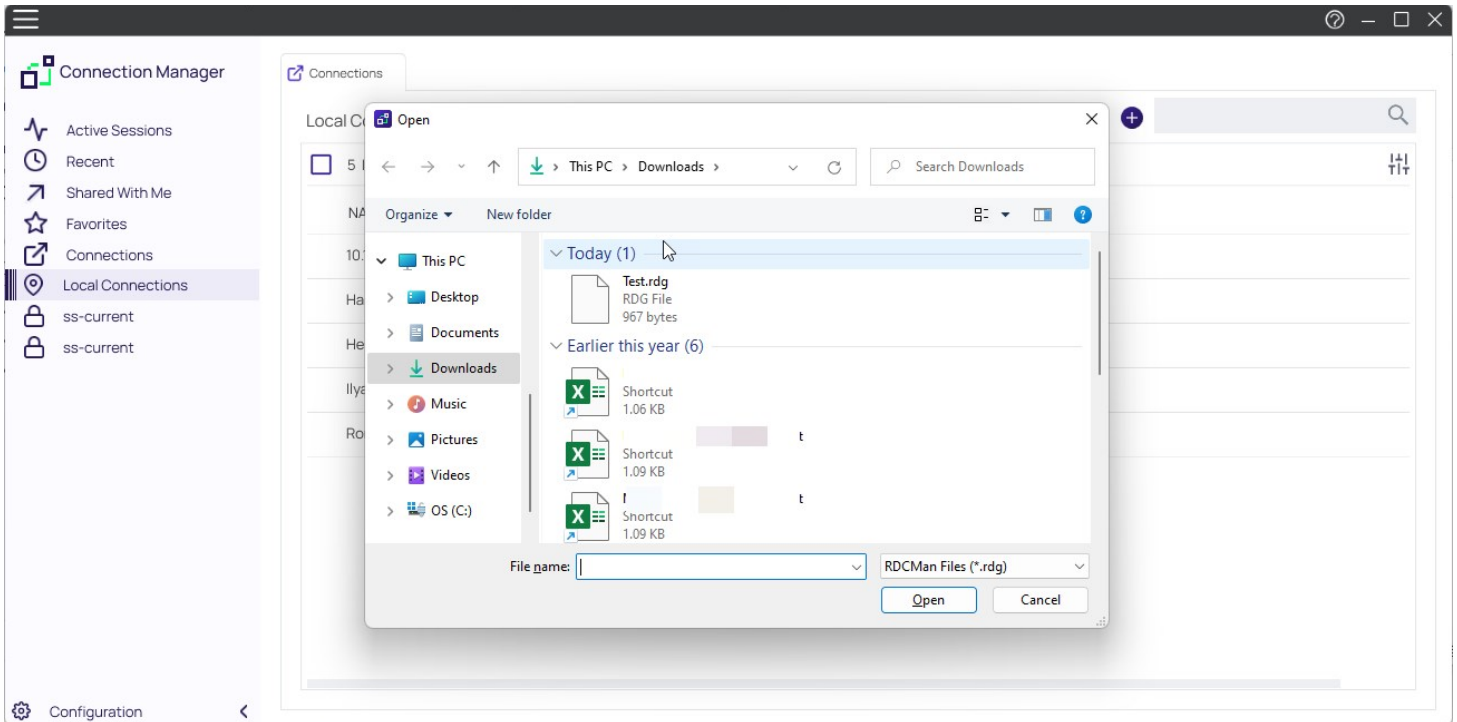
Connection Manager supports the import of RDG files. To import an RDG file:

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

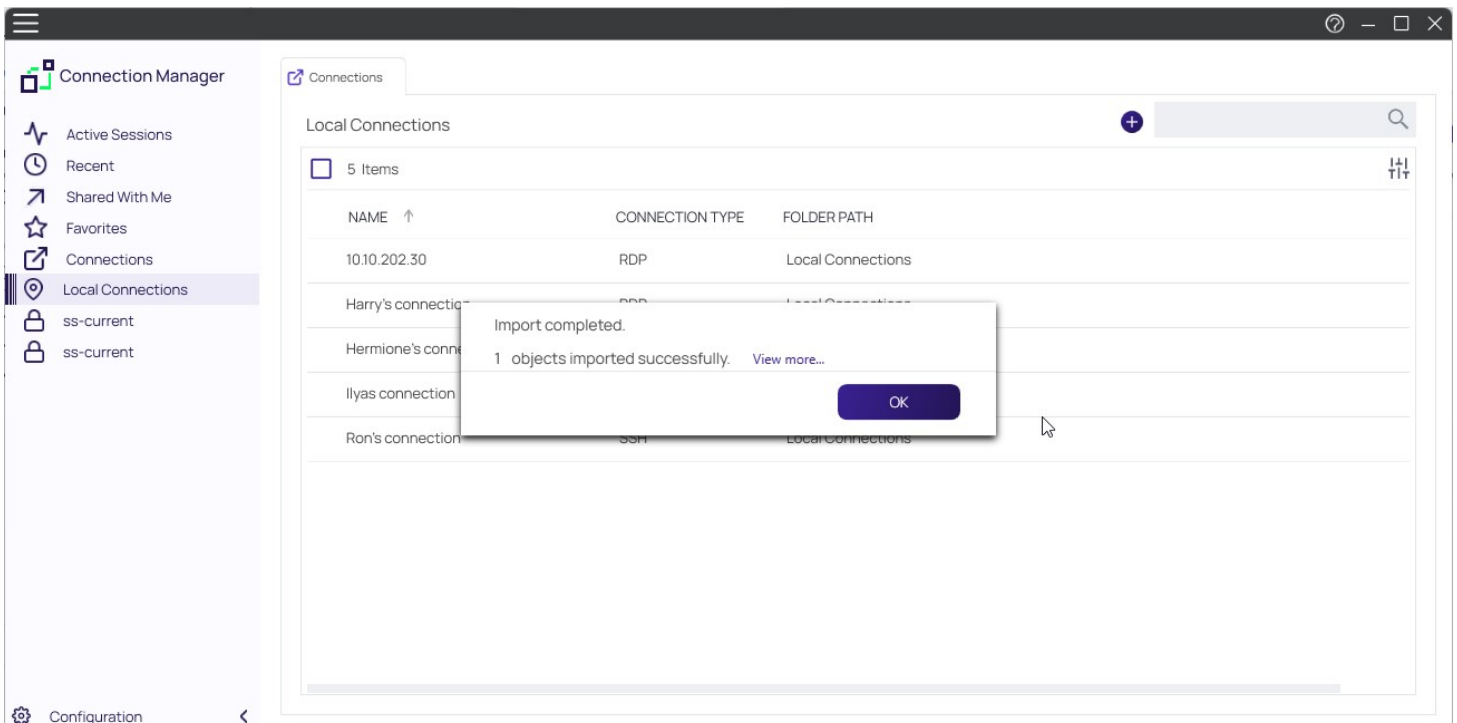


2. A dialogue window will appear. Select the files you would like to import.





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



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

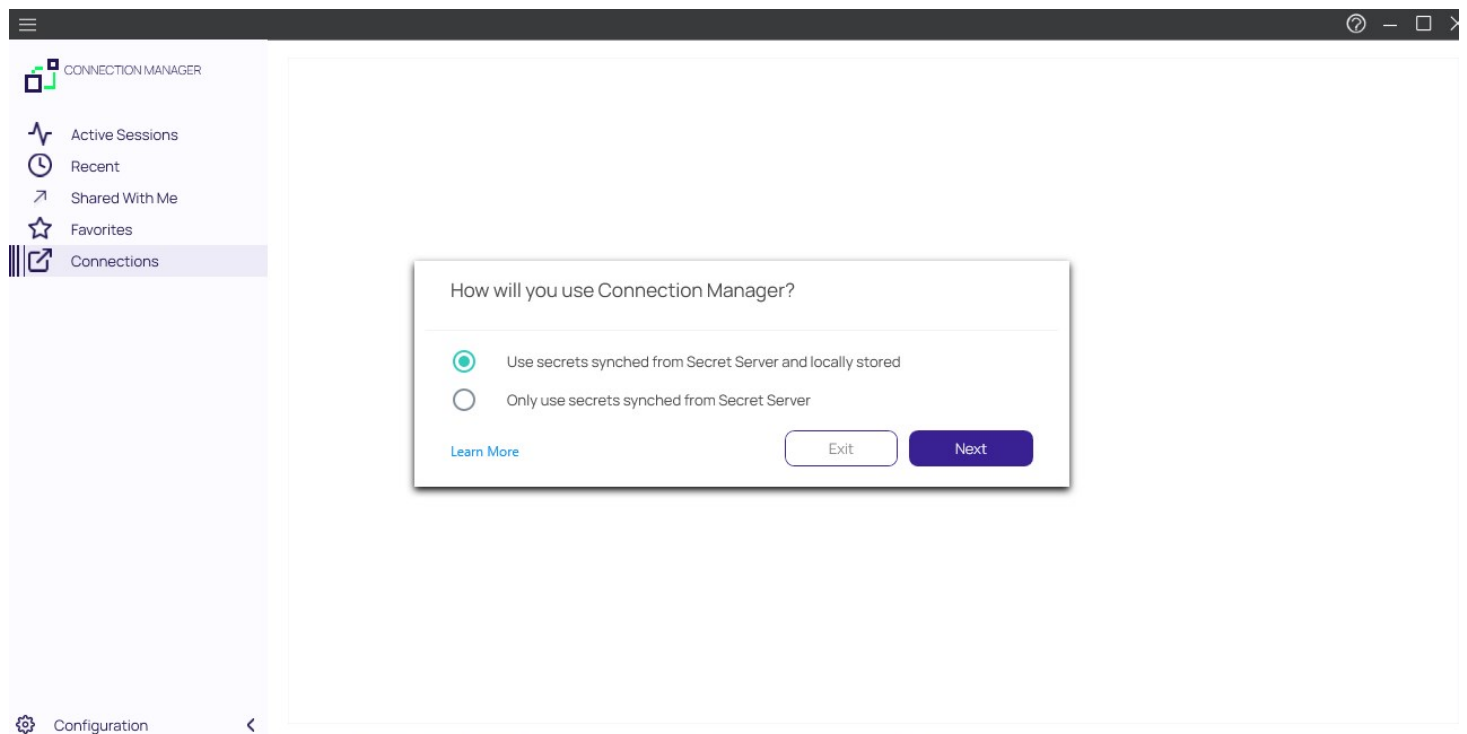
## Local Data Vault

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

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

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

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



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

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

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

follows:

## Windows

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

## Mac

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

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

---

Connect to Secret Server

---

Username\*

Password\*

Domain

Two Factor: Select two factor authentication that applies:

None

Pin Code

Duo Push

Duo Phone Call

Remember me:  Store credentials locally

Launch automatically

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

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

2. Click **File**.
3. Click either **Enable Local Data Vault** or **Disable Local Data Vault**.

## Global Configuration Settings

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

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

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

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

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

The **Windows Shortcuts** field offers three choices, listed below with their meanings:

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

The screenshot shows the 'Global Configurations' dialog box with the 'RDP Global Settings' tab selected. The settings are as follows:

- Desktop Size:** Auto
- Auto Expand:**
- Use Multiple Displays:**
- Color Depth:** True Color (24 bit)
- Run as Admin:**
- Local Devices:** Select resources to use in remote session:
  - Clipboard
  - Drives Specify Drives...
  - Printer
  - Smart Cards
- Audio Playback:** This Computer
- Windows Combinations:** On This Computer
- Audio Recording:**

Buttons: Cancel, Save

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

## Global Configurations

RDP Global Settings **SSH Global Settings** Preferences Launcher Settings

Remote Character Set

Font

Font Size

Color Presets

Background Color  Bold Color

Foreground Color

A color selection dialog box is open over the foreground color field. It has two tabs: 'Standard' (selected) and 'Advanced'. The 'Standard Colors' section displays a grid of 24 color swatches. Below the grid are several grayscale swatches. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

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

Global Configurations

RDP Global Settings   SSH Global Settings   Preferences   Launcher Settings

Protocol Handler

Secret Server Launcher

Connection Manager

Secret Server Launcher

Cancel   Save

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 I See All**.
2. Select **Tools & Integrations**.

What are you looking for?

Search for an admin option

Simple View

- Actions**  
Features that perform important jobs
- Setup & System Maintenance**  
Setup your system and keep it running with Licensing, Backups, Imports, Networking options, and more
- Users, Roles, Access**  
These features help you organize users & permission settings
- Diagnostics, Logs, Security**  
Reference options for diagnostics, logs, and security features
- Tools & Integrations**  
Find tools and other product integrations here

TOOLS & INTEGRATIONS

- Launcher Tools**
- Connection Manager**
- SDK Client Management
- Privilege Manager
- Privileged Behavior Analytics
- DevOps Secrets Vault
- Slack Integration
- Platform Integration

Unlimited Admin Mode

These options are by default enabled:

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

Admin > Connection Manager Settings

## 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.

Connection Manager is fully licensed for Secret Server.

[Learn More](#)

[Download Connection Manager installer \(Windows\)](#)

[Download Connection Manager installer \(Mac\)](#)

#### Allow local connections to save credentials

Controls whether users can save credentials for local connections. For existing local connections (RDP or SSH) where credentials already exist, turning this setting off will remove the credentials from those local connections. This setting does not remove local connections. They are still there and can be used, but the user has to enter credentials each time they connect.



#### Save Secret Server Credentials

Controls whether users can save credentials used to connect to Secret Server (this switch has no impact on the Local Connections).





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 Windows Mode Local Resources

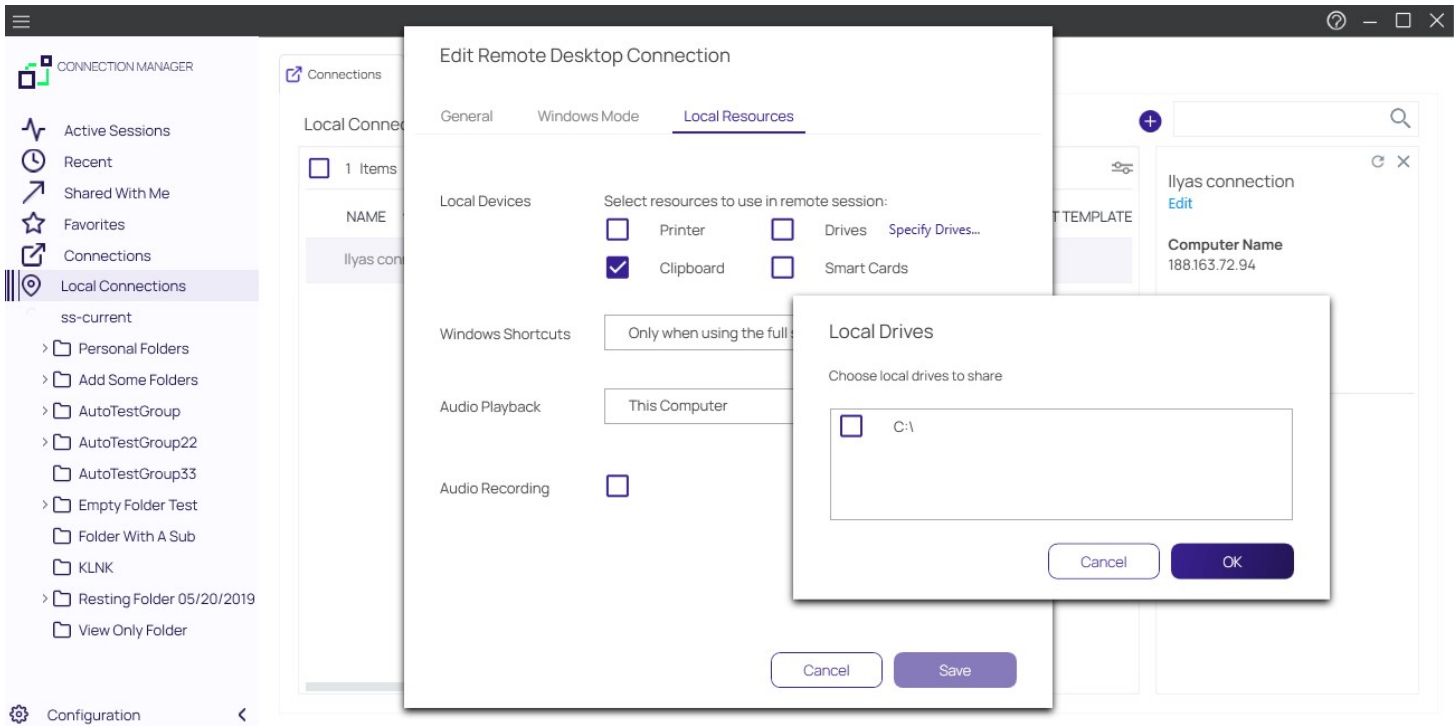
### GENERAL CONNECTION INFORMATION

Connection Name*	<input type="text"/>
Computer Name*	<input type="text"/> <small>Enter a computer name or IP address</small>
Port*	<input type="text" value="3389"/>
Credentials*	<input type="text" value="None"/>

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

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

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



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

## Manual Procedure

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

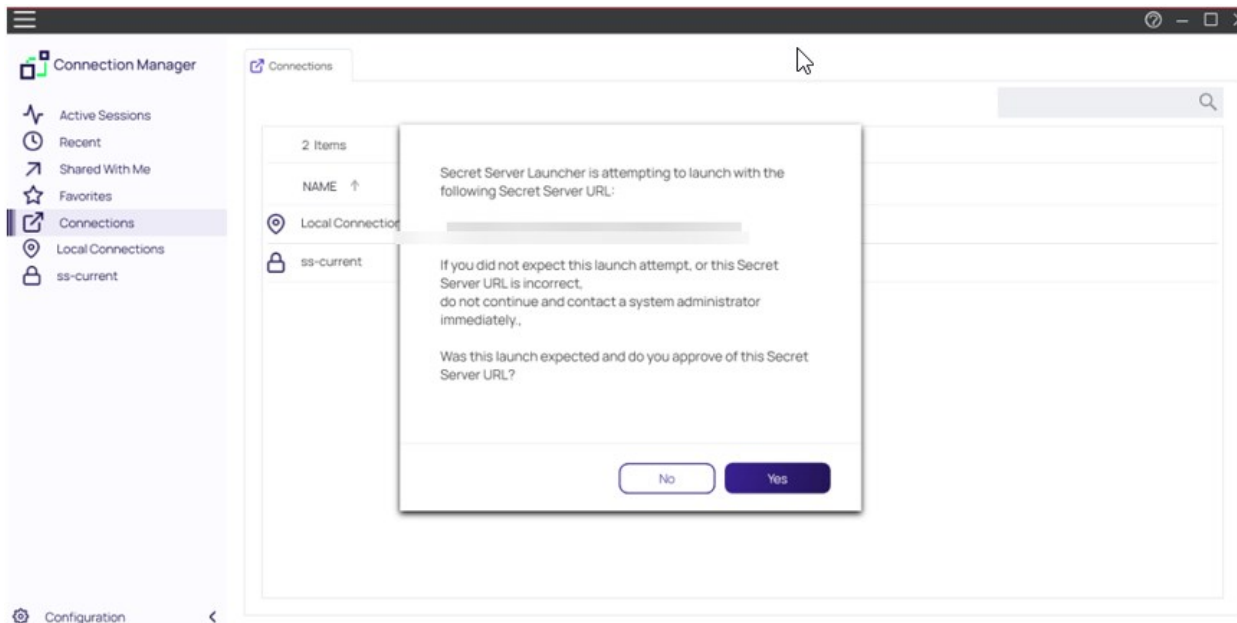
## Command Line Procedure

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

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

## Protocol Handler Approved URLs

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



Connection Manager will not run secret from denied SS URLs. If the user denied the SS url by mistake, and wants to fix this issue, they should delete the ApprovedSsUriStorage.dat file located in the application's data folder (reload application).

## Desktop Size and Auto Expand

In the Global RDP Settings, users are able to select either a fixed desktop size or an automatic one.

### Global Configurations

RDP Global Settings   SSH Global Settings   Preferences   Launcher Settings

Desktop Size	<div style="border: 1px solid #ccc; padding: 2px;"><div style="border-bottom: 1px solid #ccc; padding: 2px;">Auto</div><div style="border: 1px dashed #ccc; padding: 2px;">Auto</div><div style="padding: 2px;">Size 640x480</div><div style="padding: 2px;">Size 800x600</div><div style="padding: 2px;">Size 1024x768</div><div style="padding: 2px;">Size 1280x720</div><div style="padding: 2px;">Size 1366x768</div></div>
Auto Expand	
Color Depth	
Run As Admin	<input type="checkbox"/>
Local Devices	Select resources to use in remote session: <input type="checkbox"/> Printer <input type="checkbox"/> Drives <a href="#">Specify Drives..</a> <input checked="" type="checkbox"/> Clipboard <input type="checkbox"/> Smart Cards
Windows Shortcuts	<div style="border: 1px solid #ccc; padding: 2px;">Only when using the full screen</div>
Audio Playback	<div style="border: 1px solid #ccc; padding: 2px;">This Computer</div>
Audio Recording	<input type="checkbox"/>

Cancel

Save

## Global Configurations

RDP Global Settings    SSH Global Settings    Preferences    Launcher Settings

Desktop Size

**Auto Expand**

Color Depth

Run As Admin

Local Devices  Printer     Drives [Specify Drives..](#)  
 Clipboard     Smart Cards

Windows Shortcuts

Audio Playback

Audio Recording

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

Auto	Yes	Fill CM window	No rescale, border	Rescale image, no scrollbars
Auto	No	Fill CM window	No rescale, border	No rescale, scrollbars
Fixed	Yes	Fixed size, border	Fixed size, border	Rescale image, no scrollbars
Fixed	No	Fixed size, border	Fixed size, border	No rescale, scrollbars

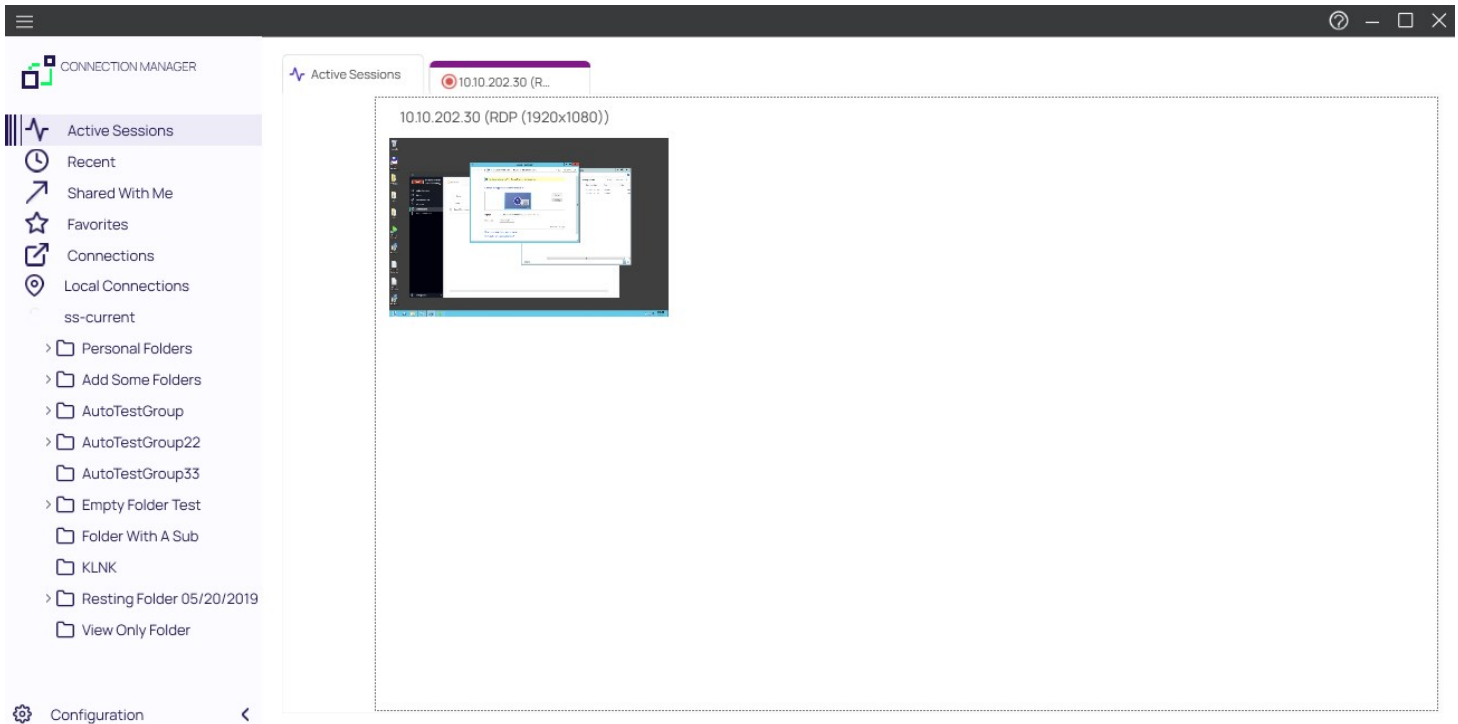
**Note:** If RDP proxy is ON, no reconnect will be attempted because RDP proxy requires a one time password and it is impossible to reuse the same credentials to reconnect.

## 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.

The screenshot displays the Connection Manager application window. On the left is a navigation sidebar with options like Active Sessions, Recent, Shared With Me, Favorites, Connections, Local Connections, and a folder tree. The main area shows a list of connections under the path 'ss-current > Personal Folders > Max'. A table lists various connection entries with columns for Name, Secret Template, Folder Path, and Connection SO. The 'UniXASSH' entry is selected and highlighted. On the right, a details panel for 'VM1-node0' is open, showing machine information, username, password, and a list of available launchers such as Remote Desktop, PuTTY-SSH, Powershell Launcher, WinWord Proce..., SQL Server Launcher, new name for Notepad, and cmd+ RMW.

NAME	SECRET TEMPLATE	FOLDER PATH	CONNECTION SO
T3 - test andy - secret	Active Directory Acc...	ss-current/Personal Folders...	ss-current
T3-andy	Windows Account	ss-current/Personal Folders...	ss-current
T3-XXX-andy - T3	Active Directory Acc...	ss-current/Personal Folders...	ss-current
test	Active Directory Acc...	ss-current/Personal Folders...	ss-current
TestADSecret	Active Directory Acc...	ss-current/Personal Folders...	ss-current
TestingEventSubscription	Active Directory Acc...	ss-current/Personal Folders...	ss-current
testss	Active Directory Acc...	ss-current/Personal Folders...	ss-current
UniXASSH	Unix Account (SSH)	ss-current/Personal Folders...	ss-current
VM1-node0	Windows Account	ss-current/Personal Folders/Max	ss-current
W1W1	Windows Account	ss-current/Personal Folders...	ss-current



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.

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

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

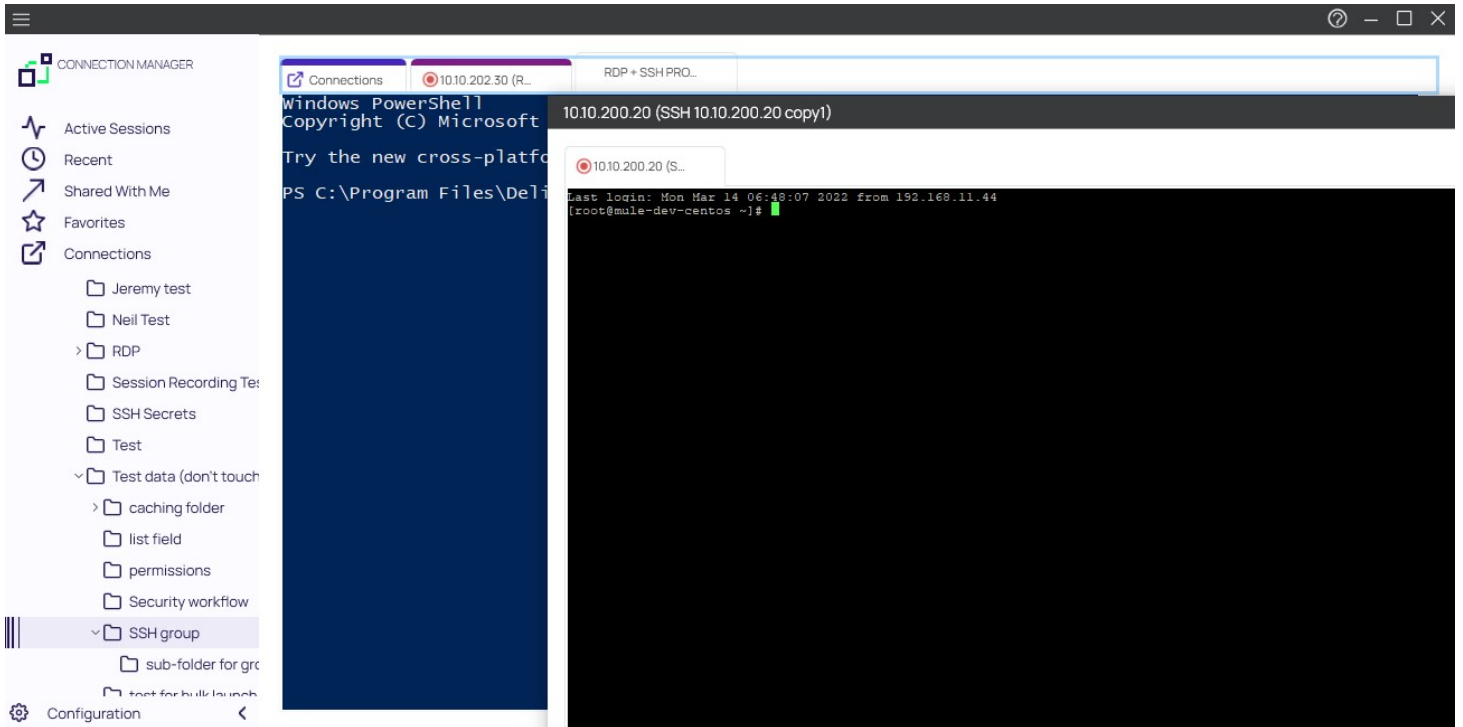
When a session is connecting through a proxy, the tab label displays the identity of the remote host.

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

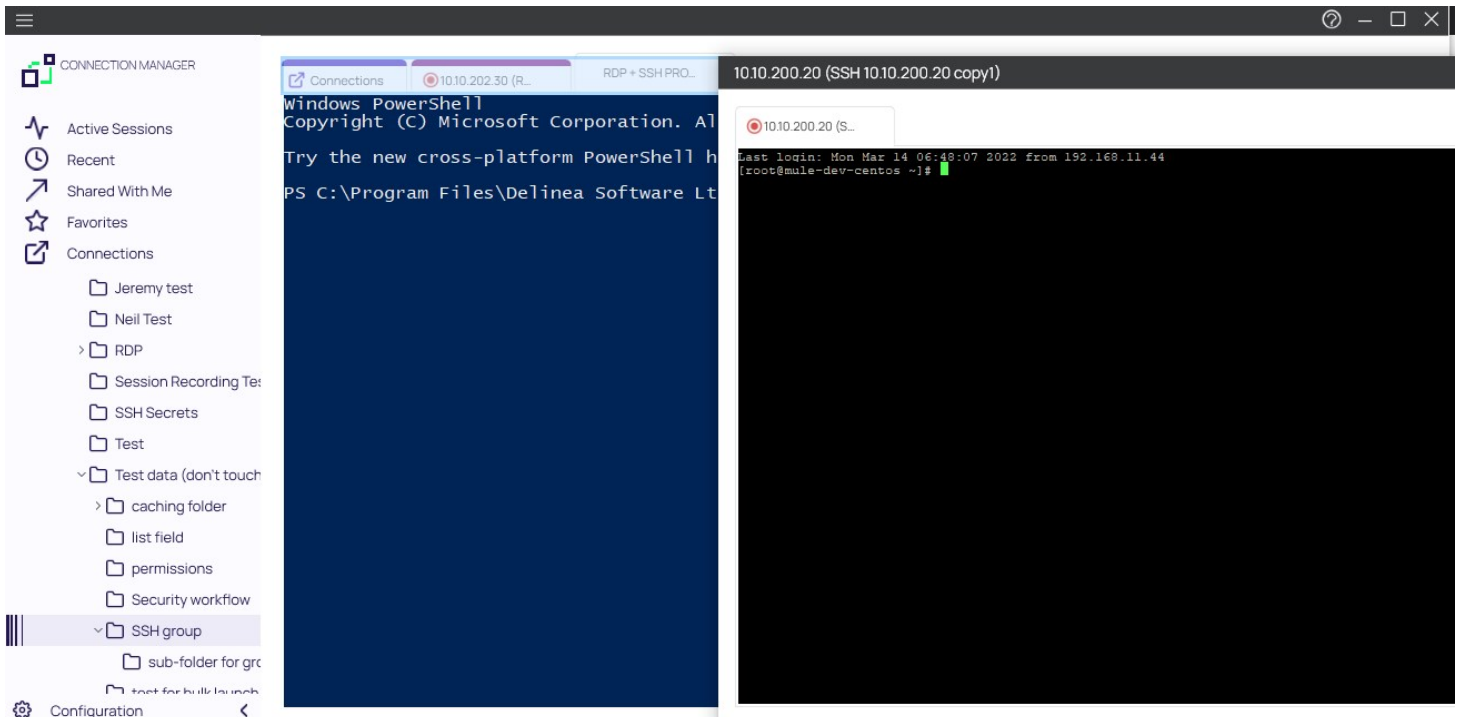
You can undock, move, and redock session tabs and windows in Connection Manager. To undock a session window, click the session tab and drag it out of the tab dock area. The tab becomes a standalone session window, which you can drag to another monitor or to another location on your desktop.



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



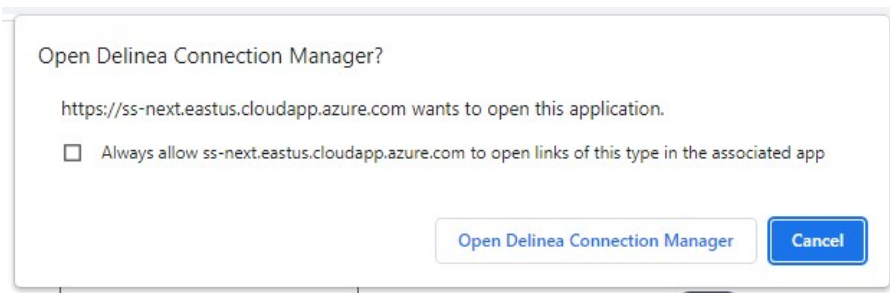
When you drag the window onto the tab dock, the dock turns light blue to indicate that you can drop the window:



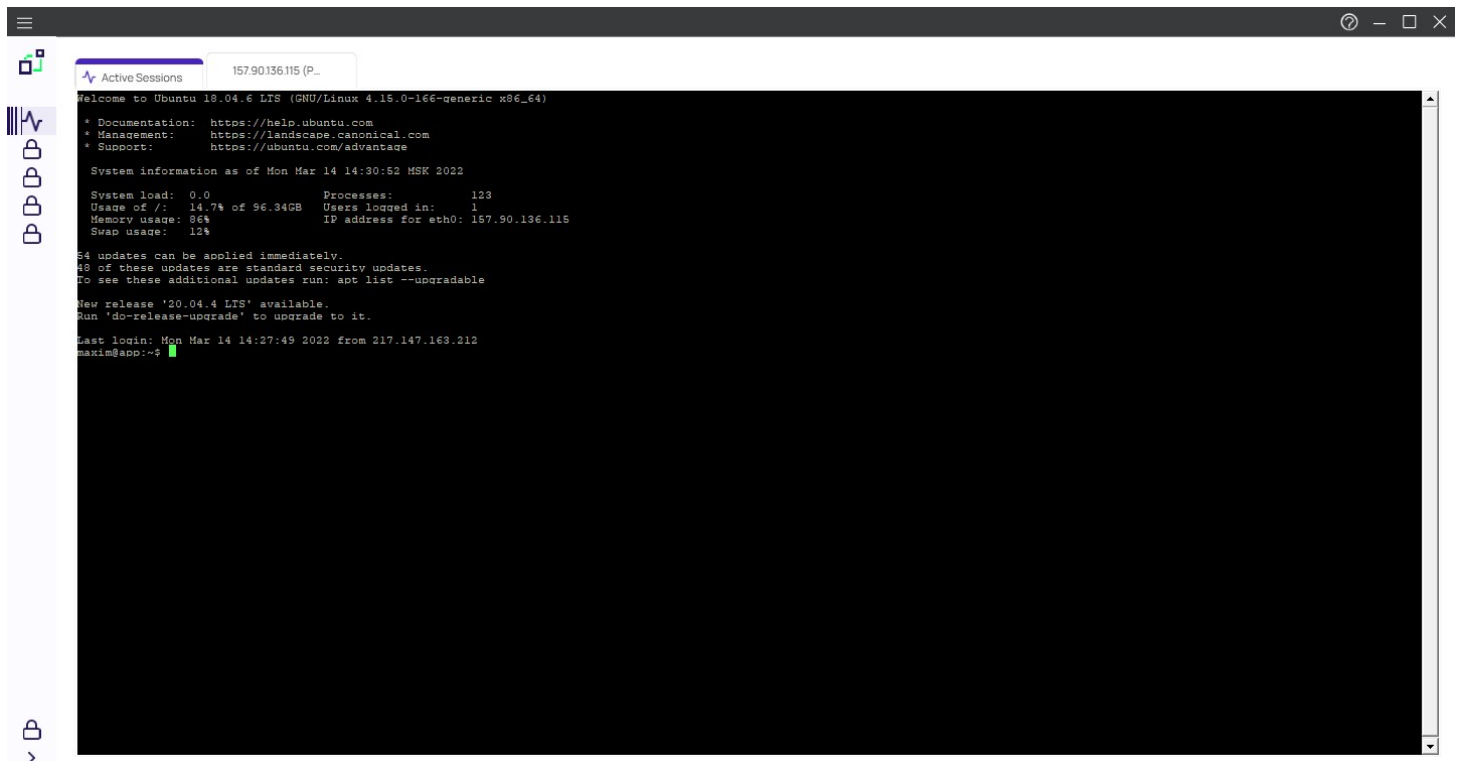
If session recording is configured to run only on the primary secret, only the primary session will be recorded. If the secret is configured to record multiple windows, Connection Manager honors the setting and all sessions started from the initial session are also recorded.

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 Connection Manager?** modal opens:



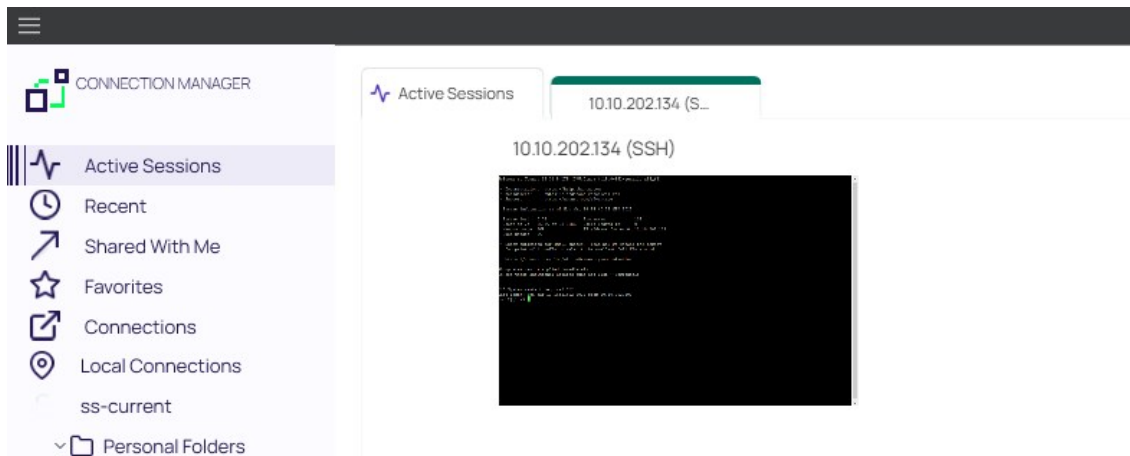
Click **Open Connection Manager** and an active session is launched in Connection Manager:



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

from the originally launched application will be tracked.

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



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

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

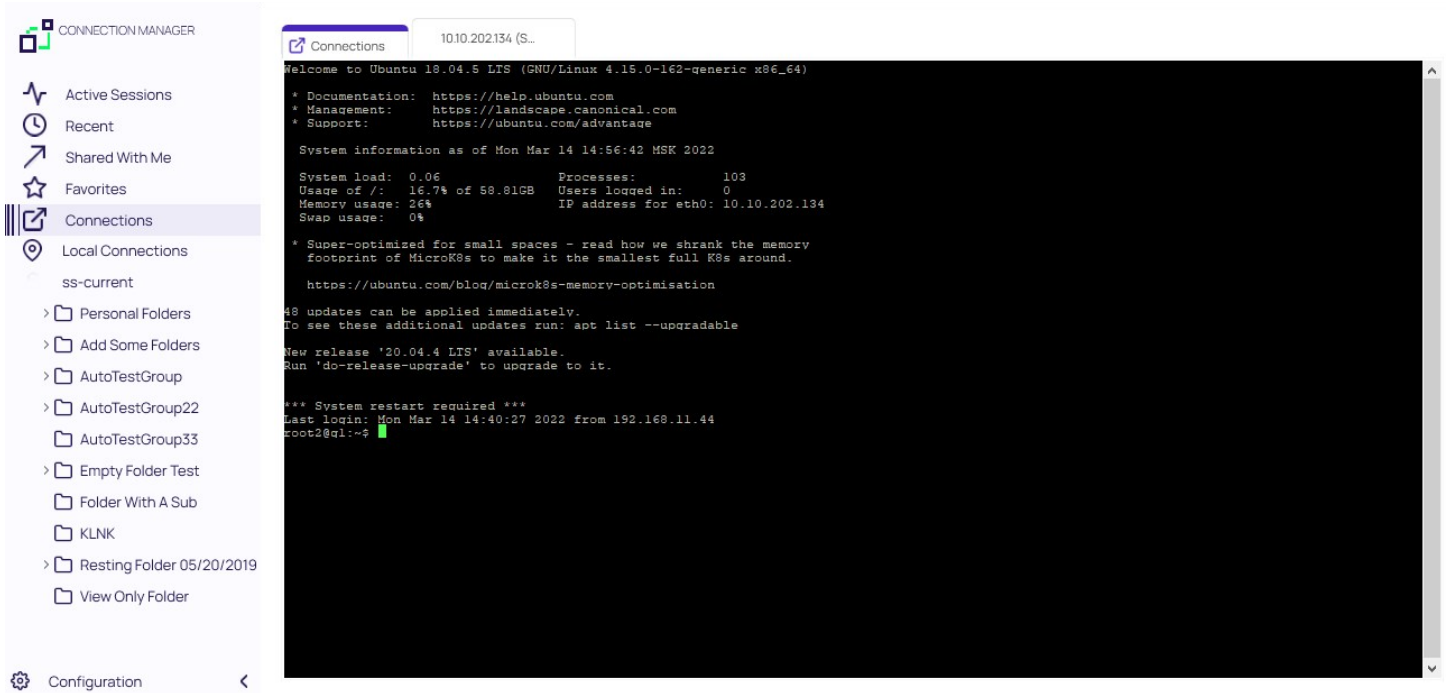
1. From the hamburger menu, select **File | Sign in** or right-click on Active Session and select **Sign in**.

The 'Sign In' dialog box prompts the user to 'Enter your password to access the local storage file.' It features a 'Password' label and an empty text input field. At the bottom, there is a link for 'Create new local storage file (All existing connections will be lost)', a 'Cancel' button, and a 'Sign In' button.

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

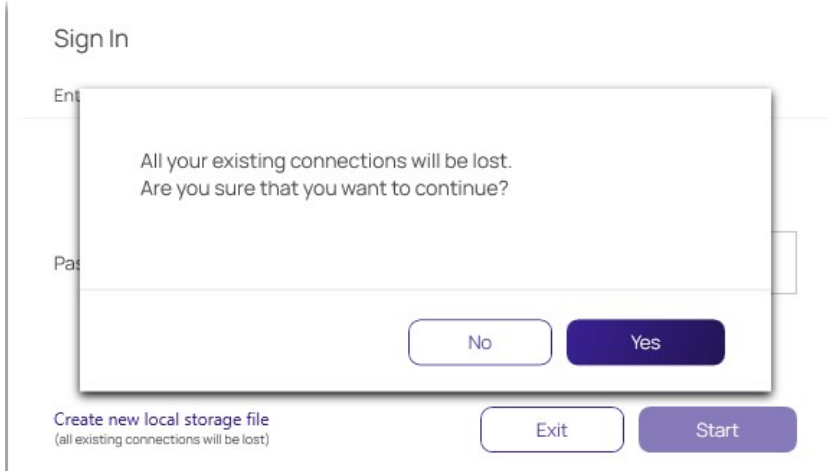
Once signed in, the user has access to all connections and all Connection Manager functionality is unlocked.

---



## 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:



**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.

- [Folder Editing](#)
- [Connection to Remote Systems](#)
- [Integrated Connections](#)
- [Re-authenticate to Secret Server](#)
- [Log File Location](#)

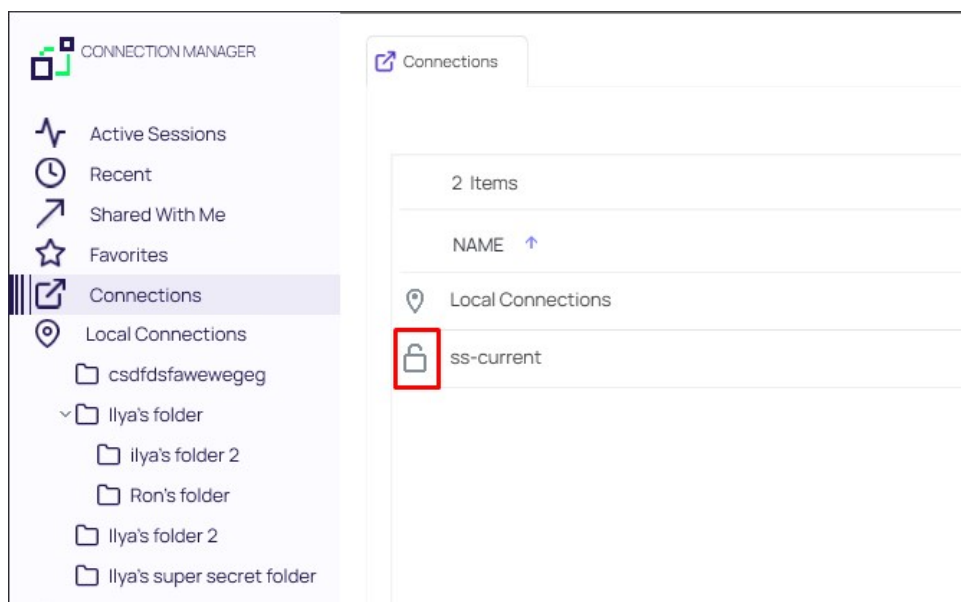
The following Connections related topics are available:

- [Re-authenticate](#)
- [Remote connections](#)
- [Integrated connections](#)

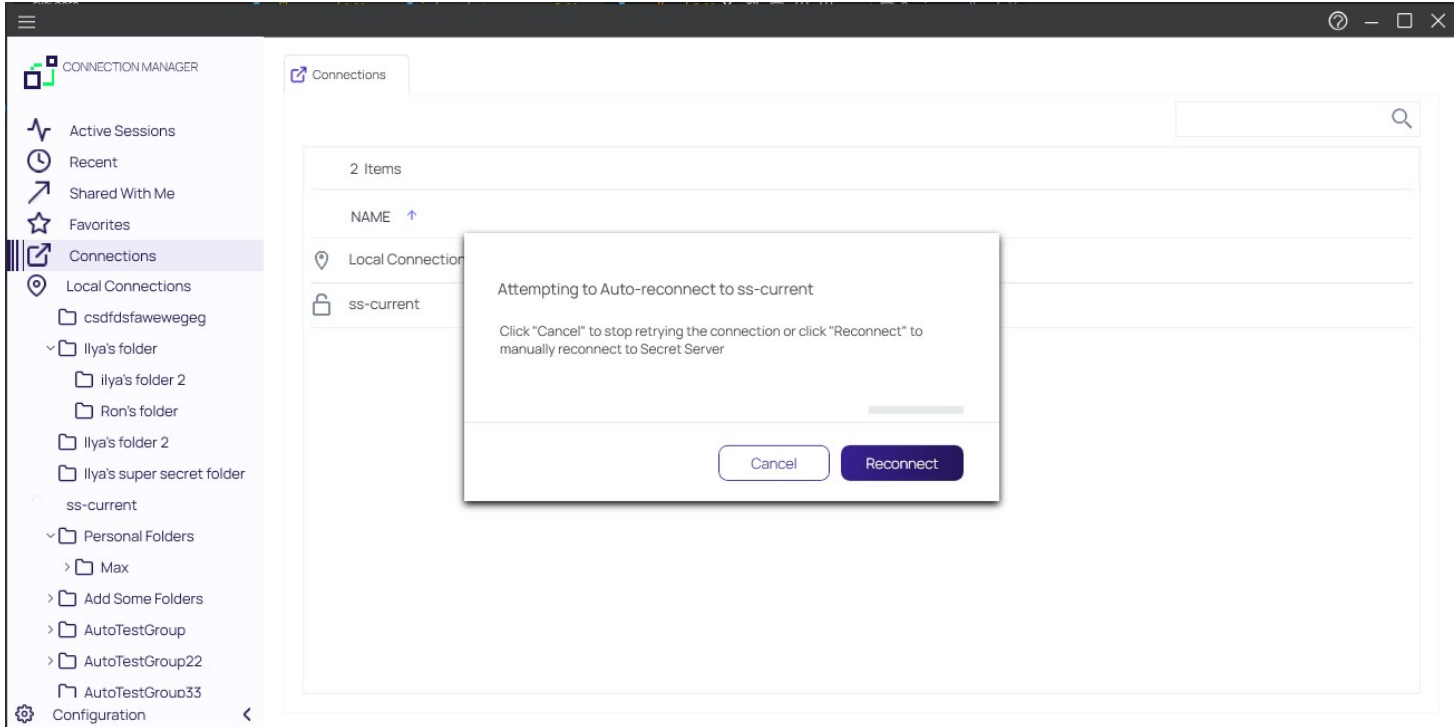
When Connection Manager starts, the configured Secret Server connection are displayed under the Connections tab, but they are **not** connected.

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**.



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





## 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.

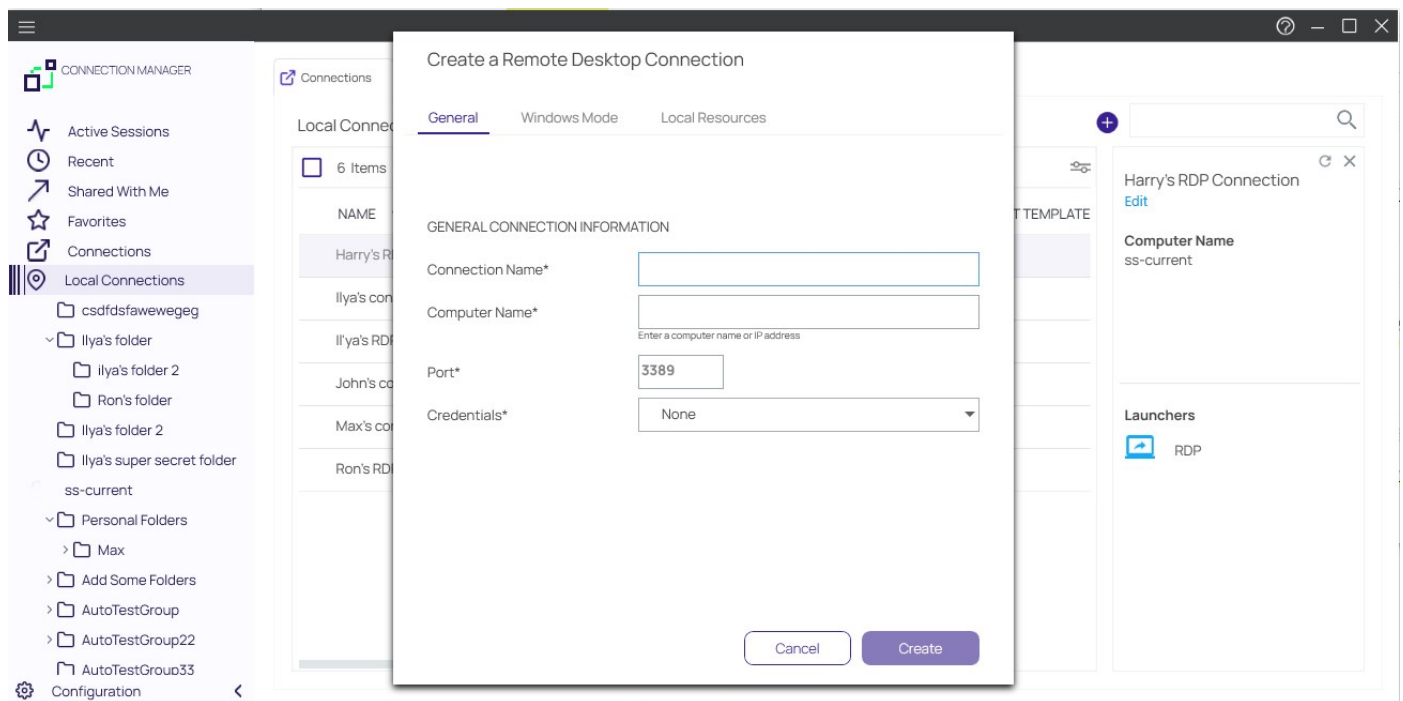
All required fields and the appropriate optional fields must be filled out. If you choose not to enter a username and password, you will be prompted to enter this information when connecting. Many of the fields will have default values pre-entered. You may keep these values or modify them as appropriate.

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

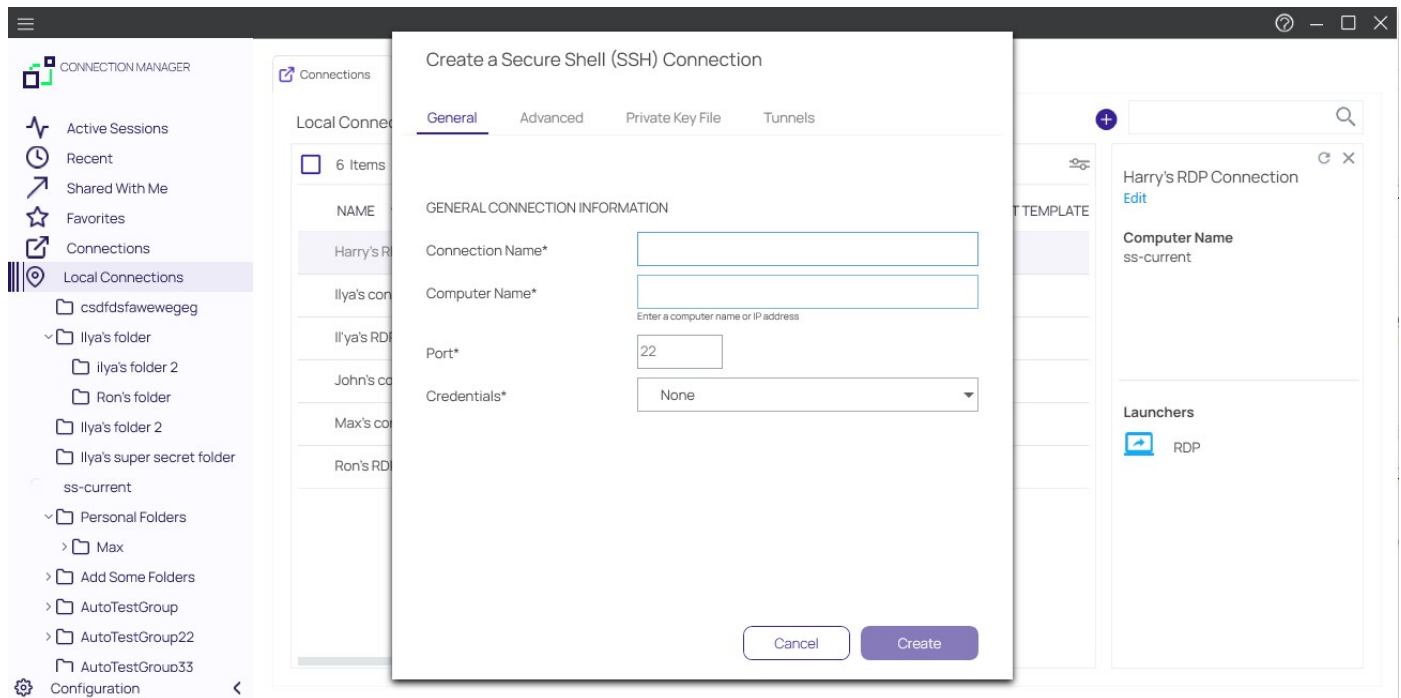
- **Connection Name:** Enter a friendly name for the new connection.
- **Computer Name:** Enter the unique identifier for the computer name or IP address.
- **Port:** Enter the port number for the connection or leave default.
- **Credentials:** Select the appropriate credential for the new connection.



### SSH Connection

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

- **Credentials:** Select the appropriate credential for the new connection.

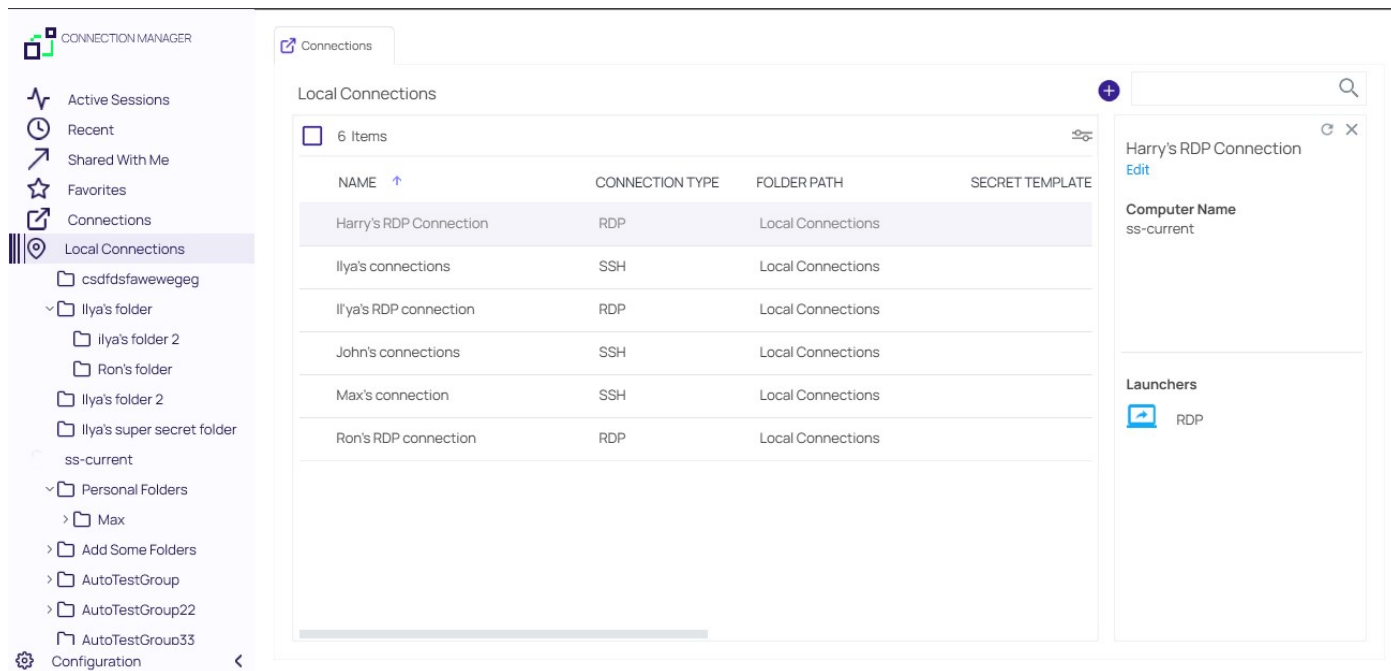


**Note:** The default value settings may be modified under the Configuration option.

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

## Edit Connections to Remote Systems

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



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

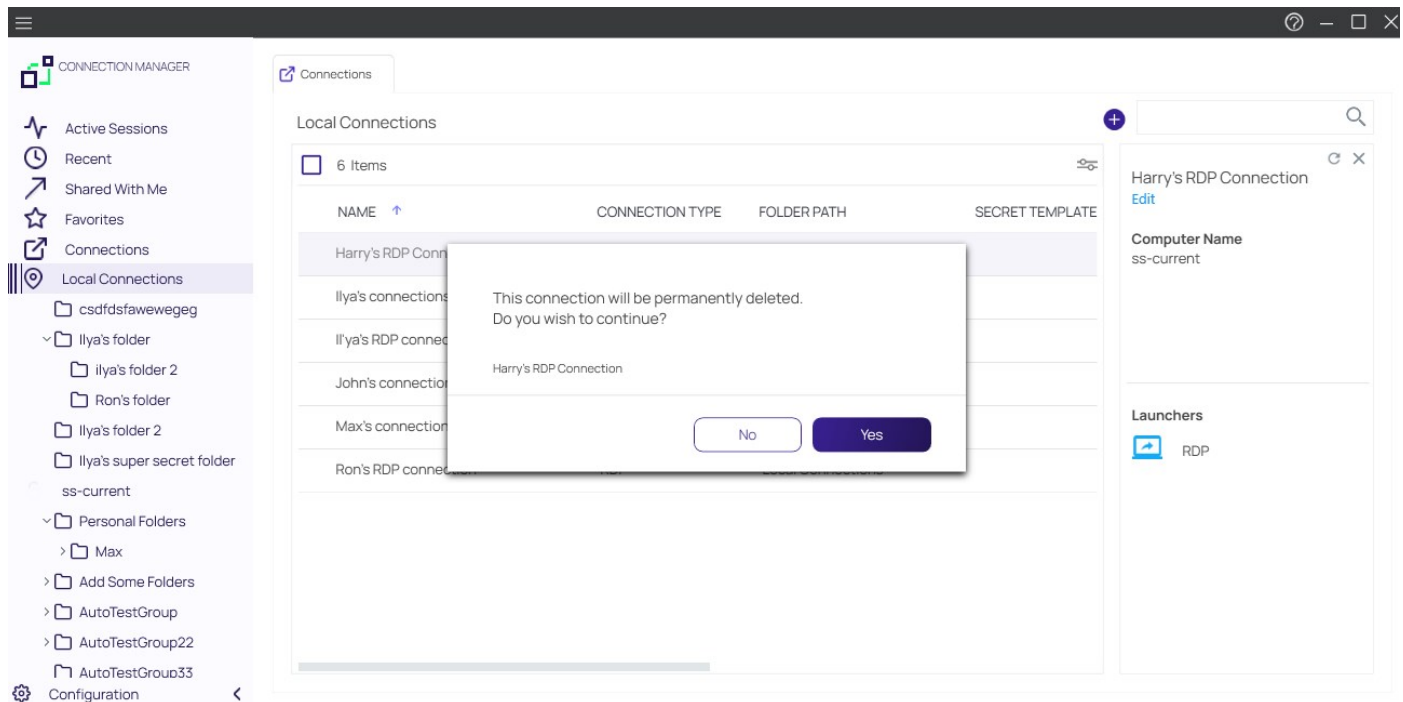
1. Modify the fields as desired. (Most values in a local connection may be edited, except the required fields and the username field.)
2. Click **Save** when finished.

## 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.



"Confirm connection delete")

3. Click **Yes** to confirm.

## Open a Remote Connection

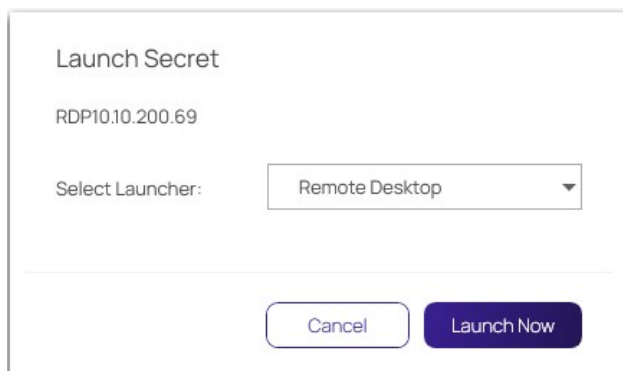
The process of connecting to a Local connection or to a Secret from Secret Server is essentially the same.

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.

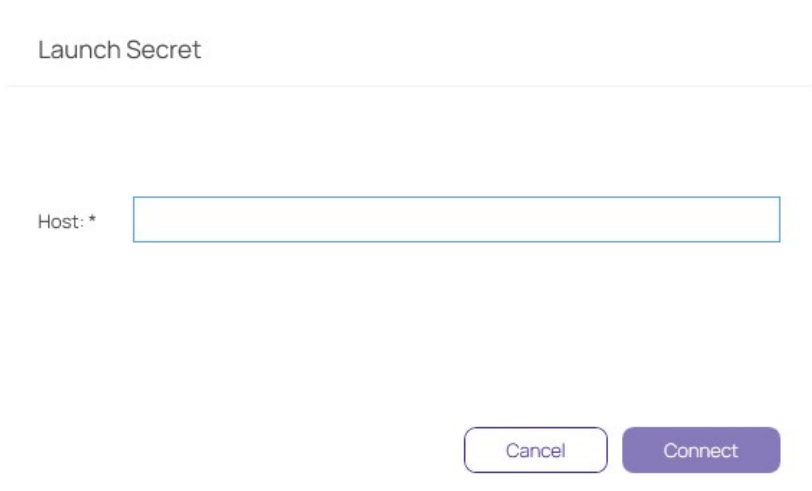
**Note:** When connecting to a Secret with an Allowed List, users will be prompted to enter a text value if the list is empty.

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



Click **Launch Now**.

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



Click **Connect**.

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

Please enter user name and password

User Name\*

Password

Cancel

Continue

Click **Continue**.

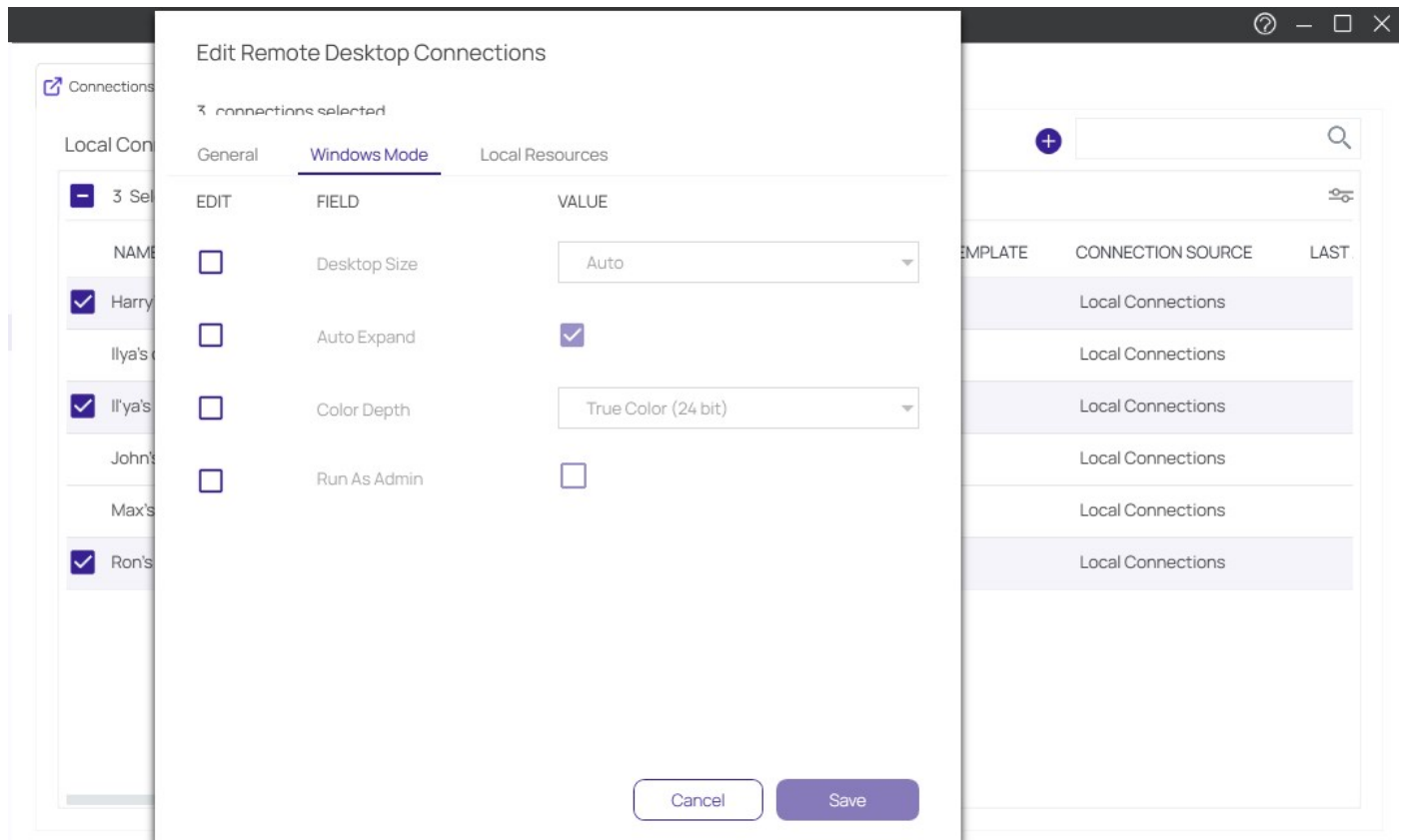
## Batch Edit Local Connections

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

### Batch Edit Local Connections Using Multi-select

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

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

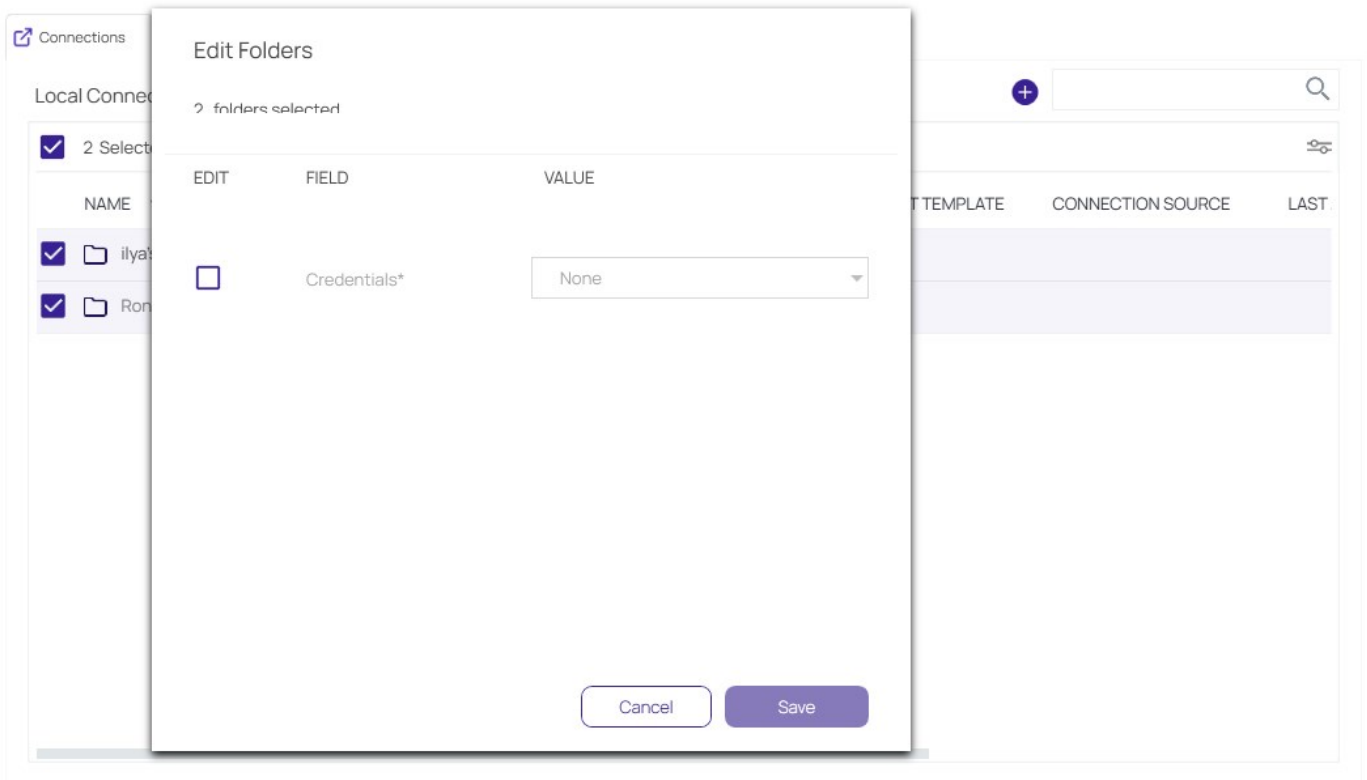


2. In the toolbar click the **Edit** icon.
3. Edit the settings you wish to apply to all of your selected connections and click **Save**.

### Batch Edit Credentials for All Connections in One or More Folders

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

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



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



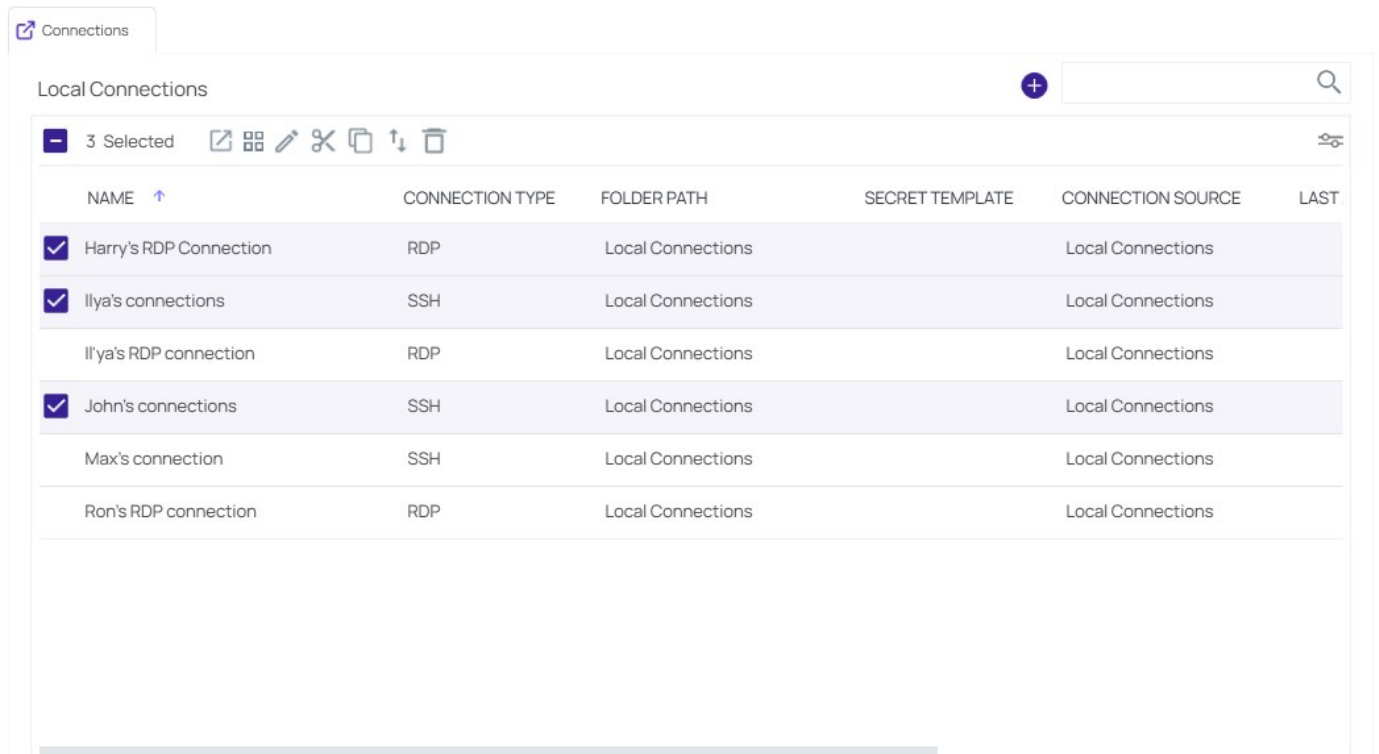
## Batch Open Connections

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

### Batch Open Connections Using Multi-select

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

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

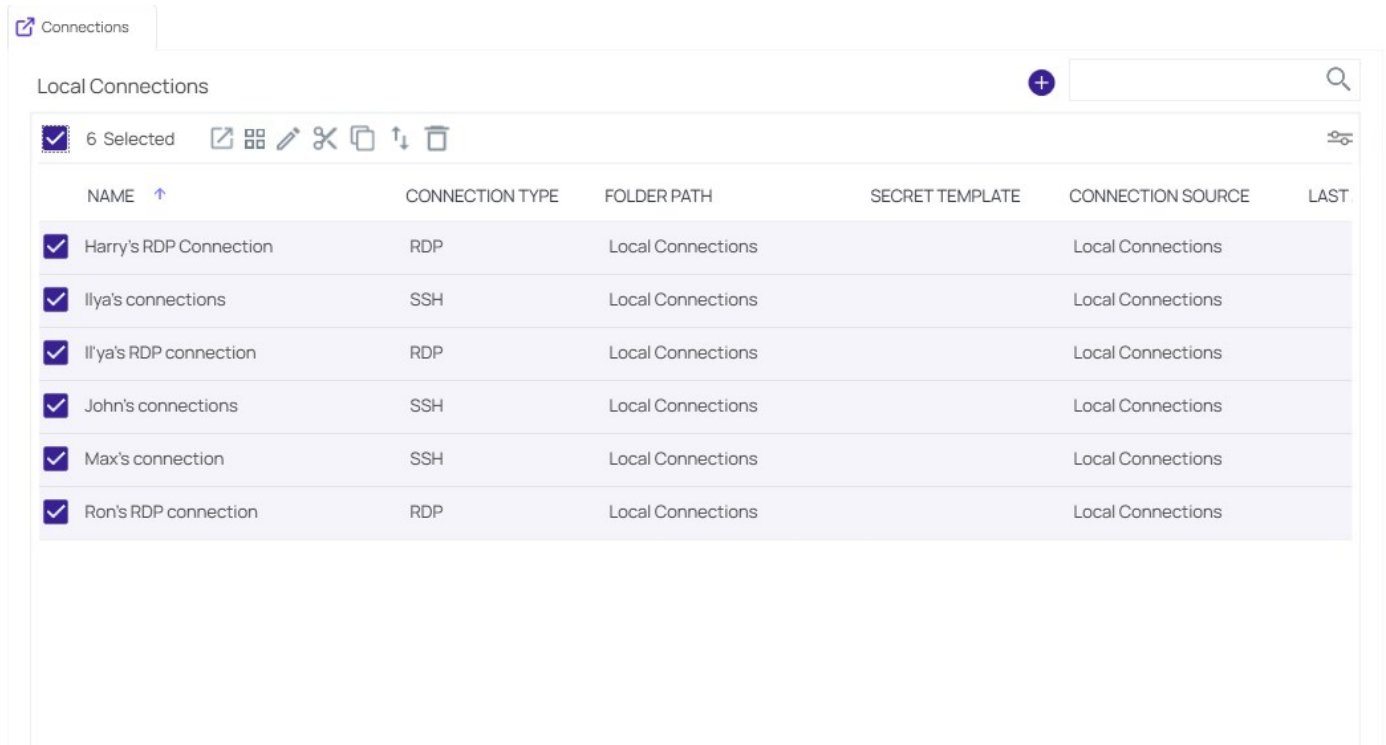


2. In the toolbar click the **Connect** icon.

### Batch Open All Connections in a Folder

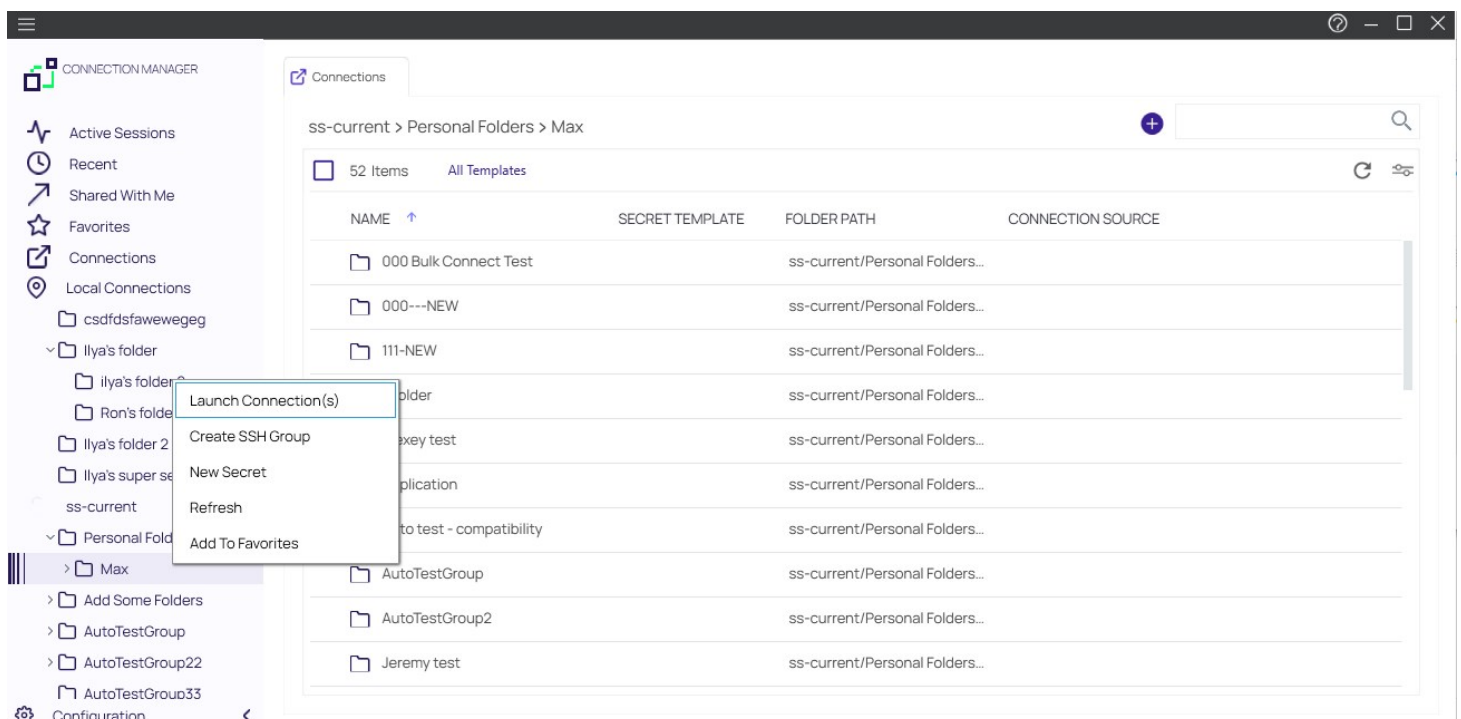
You can batch open all connections in a folder, at the folder level.

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



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

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



## Duplicate Remote Connection

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

## 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/If ya's new folder

Credential

harry.potter

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

#### CONNECTION CREDENTIALS

Secret\*

[Select Secret](#)

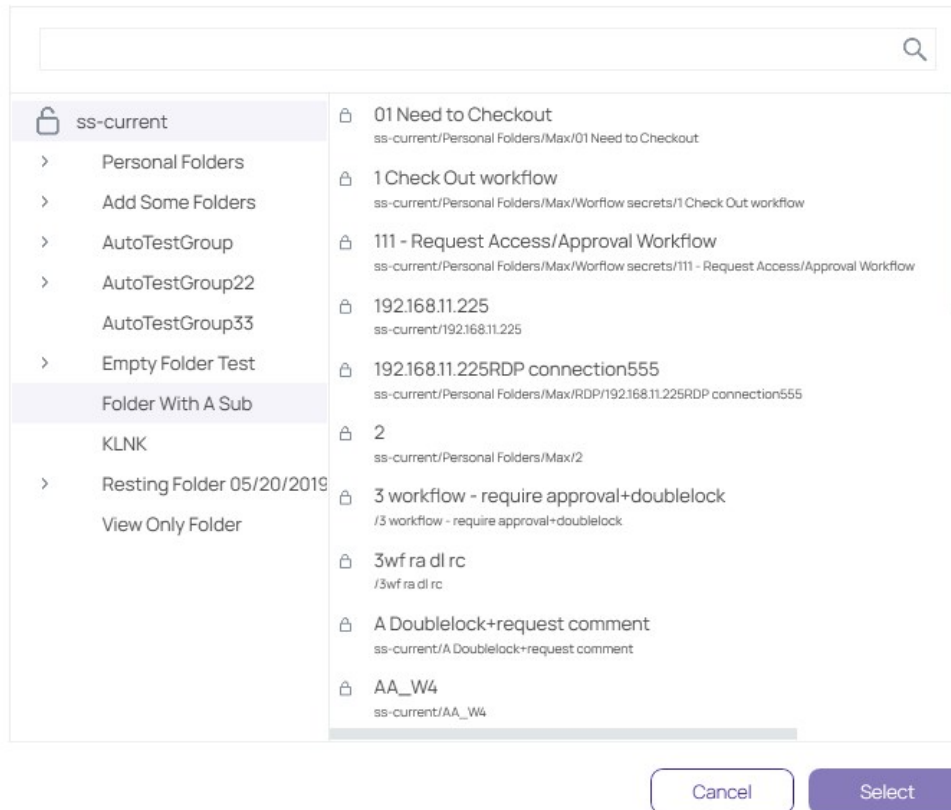
### Map a Secret to a Folder

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



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.

- 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

User Name

Password

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

## Configuration File

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

C:\Program Files\Thycotic Software Ltd\Thycotic Connection Manager\Thycotic.ConnectionManager.exe.config for Windows

/Users/<yourusername>/Library/Preferences/com.Thycotic.ConnectionManager.plist

### Disable update check on startup for Windows

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

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

### Disable update check on startup for macOS

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

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

## Folder: Create, Edit, Move, Delete

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\*

Parent Folder: Local Connections

Credentials\* None ▼

- None
- Local Credentials
- Inherit from Folder
- Map Secret

Cancel Create

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

Credentials\*

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

View the [Integrated Connections](#) section for additional information on credentials.

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

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 folder and its contents will permanently delete.  
Are you sure that you wish to continue?

Local Connections/Ilya's folder



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\Delinea\Connection Manager
```

### Changing the Log Level

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

```
</configSections>  
<appSettings>  
  <add key="UpdateOnStartup" value="true" />  
</appSettings>  
<log4net>  
  <root>  
    <level value="INFO" />  
    <appender-ref ref="LogFileAppender" />  
    <appender-ref ref="TraceAppender" />  
  </root>
```

```
C:\Program Files\Delinea Software Ltd\Delinea Connection Manager
```

```
~/Library/Application Support/Delinea/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 typing:

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

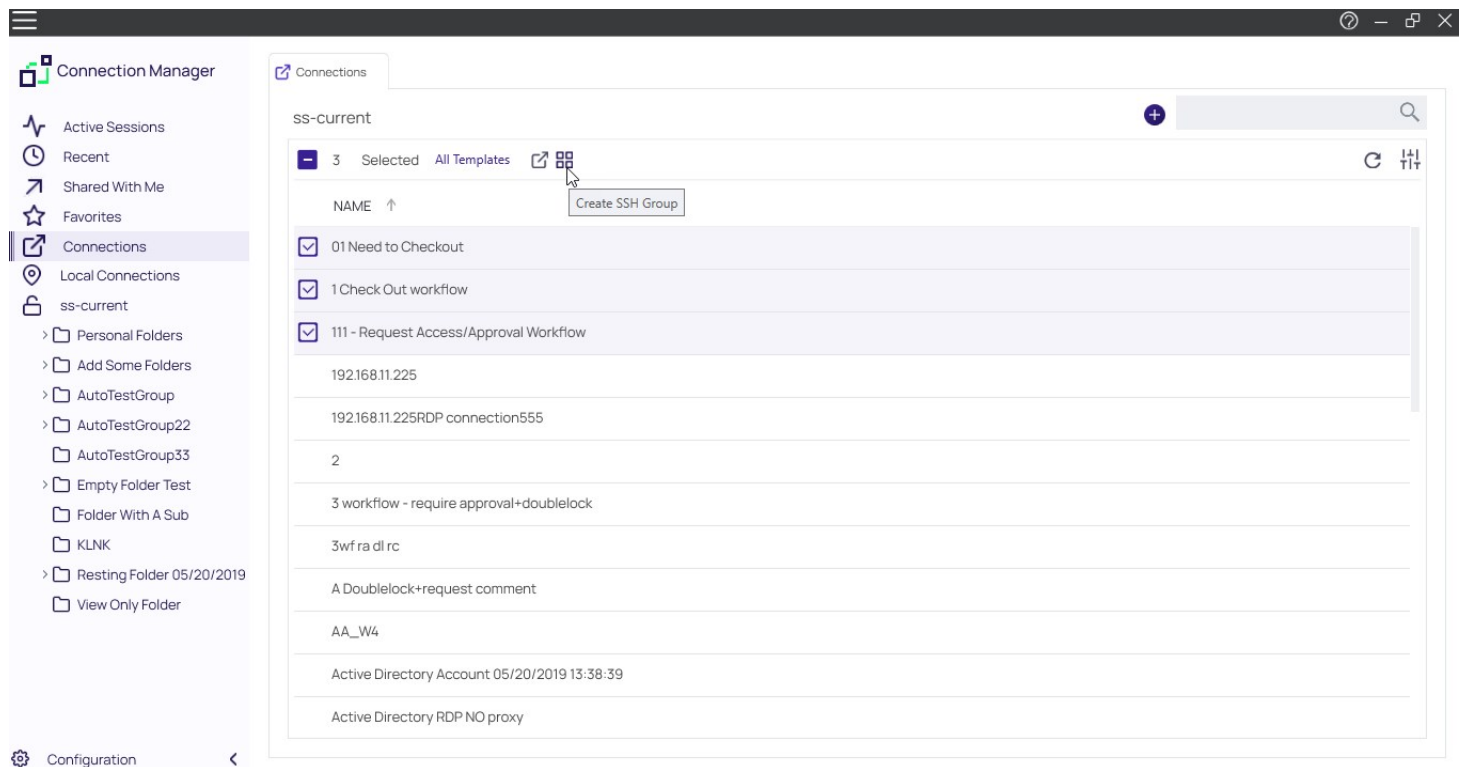
**Note:** For Connection Manager versions 1.7 and older, the directory names will use *Thycotic* instead of *Delinea*

## Using SSH Session Groups

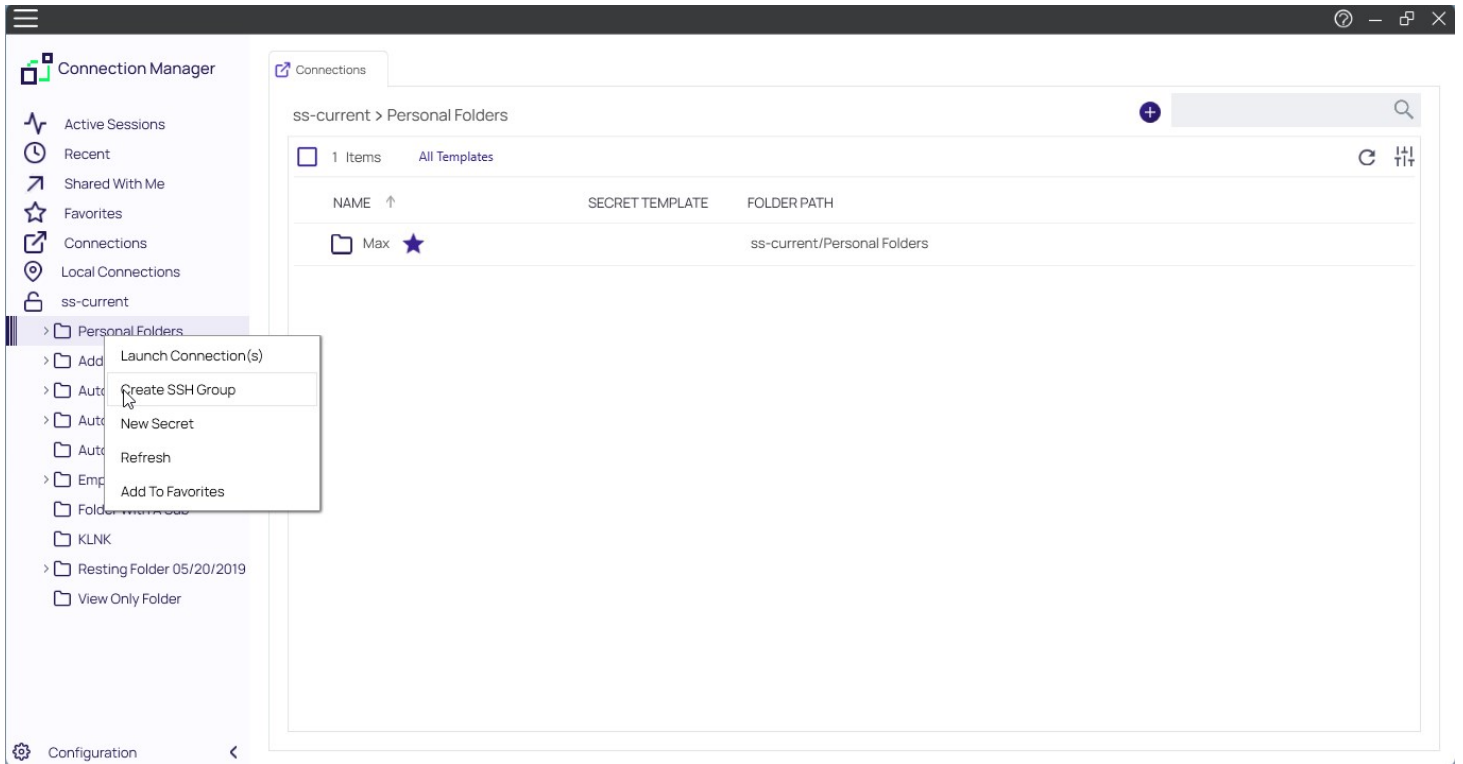
Users can now create one or more groups of active SSH sessions, then send a command or a series of commands in bulk to all active sessions in the group.

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

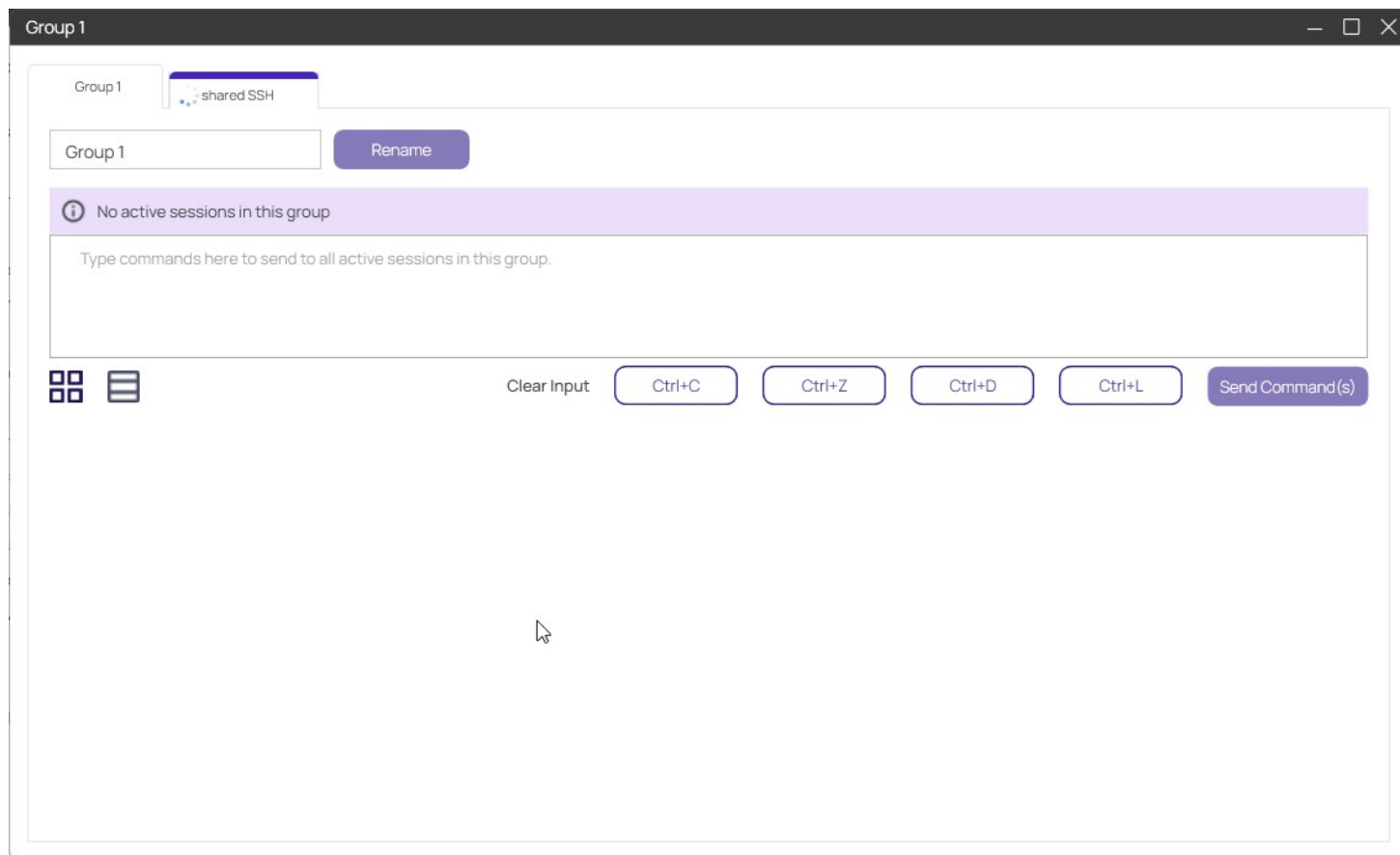
1. Select the sessions you want to include in the group
2. Click the **Create a Group** toolbar icon.



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

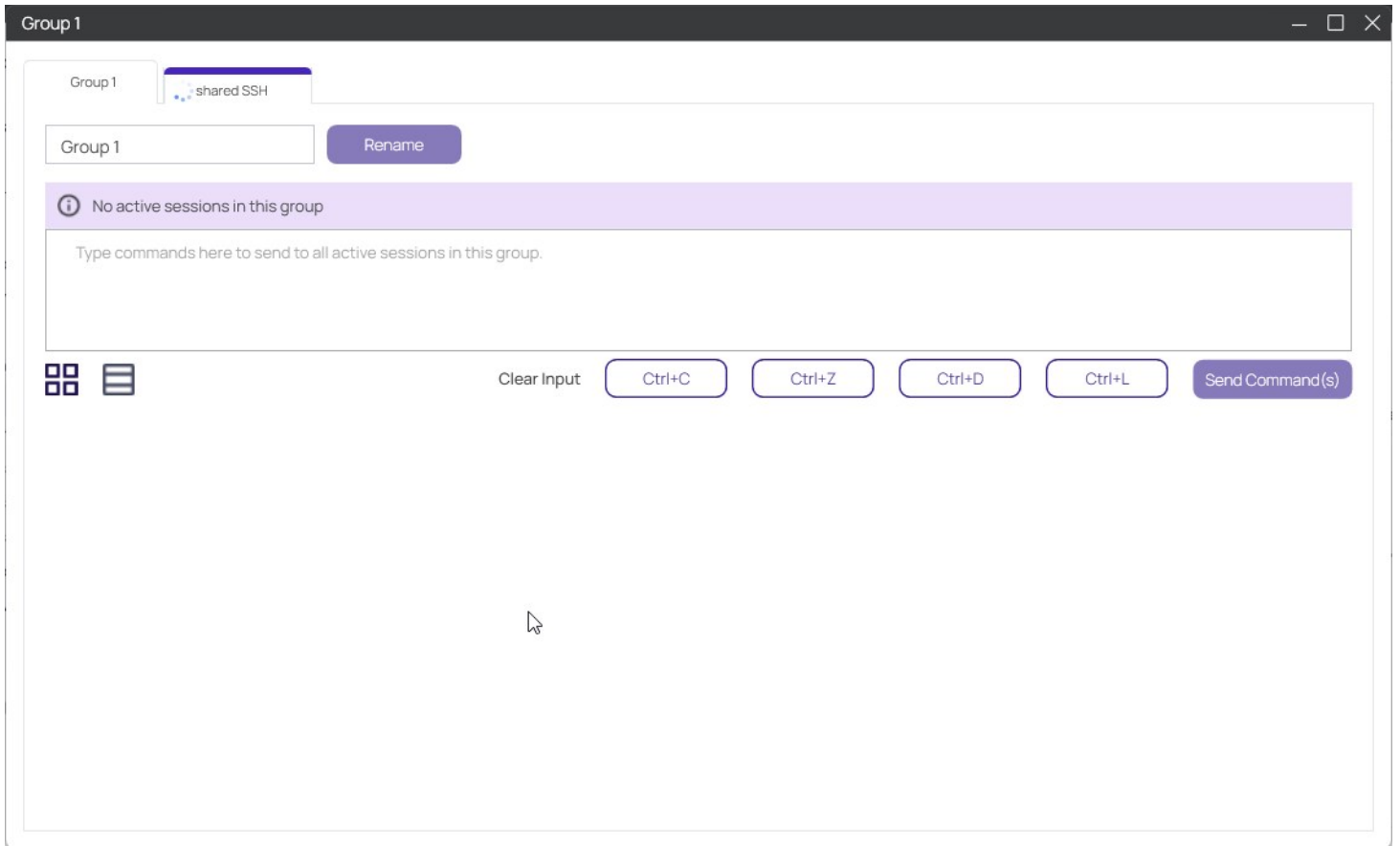


When the SSH Group is created, it opens in its own window with a special Group tab followed by the individual tabs for each SSH session in the group.



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

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



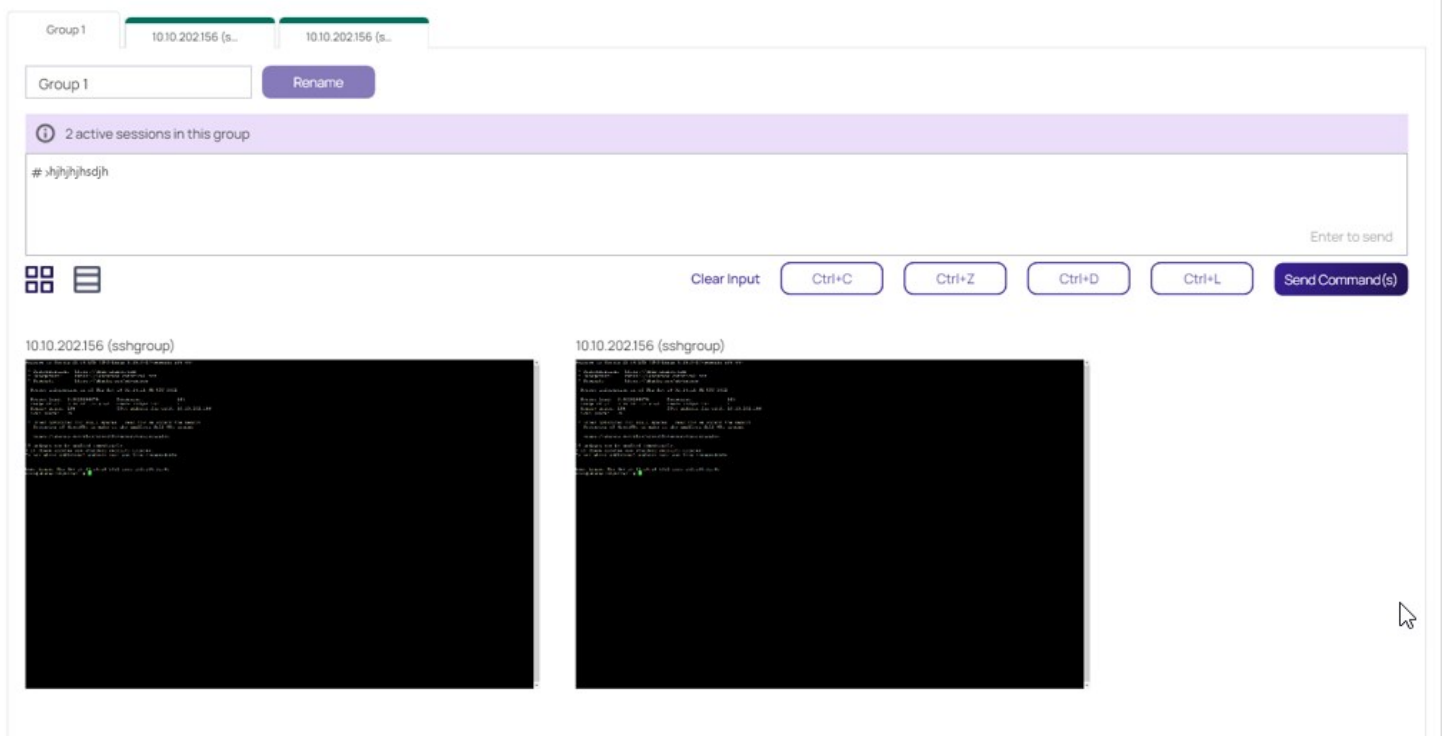
The four commands listed below are built into the user interface as individual buttons:

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

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

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





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

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

## 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 Secret Workflows](#).

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](#)
- [Generate Additional Log Entries](#)
- [Related Resources](#)

## General

Windows, application file: C:\Program Files\Delinea Software Ltd\Delinea Connection Manager on Windows

Windows, log file: C:\Users\AppData\Roaming\Delinea\Connection Manager

macOS, application file: Applications/delinea/Connection Manager.app

macOS, log file: users/<username>/library/application support/delinea/Connection Manager

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\Delinea\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.

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

## 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.



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](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.

## CM Crashing When Offline and Checking Certificates

If a Connection Manager end user is using untrusted certificates in their environment while they are offline, CM will try to reach out to an MS DNS to confirm the certificate. This happens even after a DNS sinkhole is set on that domain through the host file. But because there is no outbound internet connection, CM pauses while waiting indefinitely for a confirmation that will never come, eventually freezing and crashing.

To resolve this issue, edit the local group policy using the information in the article, [An Automatic Updater of Untrusted Certificates for Windows](#).

## Generate Additional Log Entries

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

1. Open the `Delinea.ConnectionManager.exe.config` file

Windows default location: `C:\Program Files\Delinea Software Ltd\Thycotic Connection Manager`

macOS default location: `Applications/Delinea/Connection Manager.app`

2. Find the snippet below and change INFO to DEBUG.

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

Before:

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

After:

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

## Manually Cleaning the Connection Manager File System

To manually clean up the Connection Manager file system, you need to remove files and folders specified below, and then clear Registry entries specified below.

Remove the specified files and folders at the following paths:

- C:\Users\UserName\AppData\Roaming\Thycotic (folder **Delinea** must be deleted)
- C:\Users\UserName\AppData\Local\Thycotic\_Software\_Ltd (folder **Thycotic\_Software\_Ltd** must be deleted)
- C:\Program Files\Thycotic Software Ltd (folder **Delinea Software Ltd** must be deleted)

Clear entries from the registry as specified below:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\ssllauncher
- HKEY\_CURRENT\_USER\Software\Thycotic
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Thycotic Software Ltd
- HKEY\_CURRENT\_USER\Software\Classes\ssllauncher
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version Vector
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version Vector

In addition, run regedit, search for and remove all registry keys that contain "thycotic" as part of a key name.

## Related Resources

- [Secret Server Secret Workflows](#)
- [Supported Characters for Machine Host Name](#)

## Release Notes

Your Connection Manager version is compatible with any Secret Server version released within the 12 months preceding the Connection Manager release.

Example: For Connection Manager Version 1.6.2 - Released August 2021, the oldest Secret Server Version compatible would be 10.9.000000, released in August 2020.

The following Connection Manager release notes are available:

- [1.9.0 - Release Notes](#)

Previous versions:

- [1.8.0 - Release Notes](#)
- [1.7.1 - Release Notes](#)
- [1.7.0 - Release Notes](#)
- [1.6.2 - Release Notes](#)
- [1.6.1 - Release Notes](#)
- [1.6.0 - Release Notes](#)
- [1.5.0 - Release Notes](#)
- [1.4.1 - Release Notes](#)
- [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](#)

## 1.9.0 Release Notes

*Release Date: August 29th, 2022*

- Users can now create a Secret Server connection via an external browser. This resolves issues with limitations in the embedded browser that prevent some SAML logins from completing successfully.
- Users can now automatically see secrets created on new templates without editing connection settings. The 3rd step of the **Edit Connection** dialog now contains two options: one to select all templates including ones created later, and one to select specific templates to view in Connection Manager. The default option for new installations is *All Templates* and can be changed by the user by editing the Secret Server connection.
- Silent installations will now set the selected templates to *All Templates*. This can be changed by the user after installation by editing the Secret Server connection.
  
- Updated FreeRDP 2.4.0 to the latest version.
  
- Updated Coverlet.Collector to the latest version.
- Updated Newtonsoft.Json to the latest version.
- Updated log4net 2.0.13 to the latest version.
  
- Fixed an issue where Connection Manager was not showing the full password.
- Fixed an issue where the 1.8 version of Connection Manager was missing the Refresh button in dark theme.
- Fixed an issue with the RDP Client title bar behavior with RDP Proxy. The title was not showing the target in full screen mode.
- Fixed an issue where the connections list attempted to connect to the wrong server.
- Fixed an issue where users were seeing the wrong font for SSH Local Connection after installing Connection Manager.
- Fixed an issue where users were getting an error message when clicking the **Show** button to show the password.
- Fixed an issue where Connection Manager was not honoring the *Hide Password* setting when adjustments were made at the Secret Template level

### iOS Specific

- Fixed an issue where the cursor position would change when the window was resized on a Mac.



## Changelog

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

Your Connection Manager version is compatible with any Secret Server version released within the 12 months preceding the Connection Manager release.

Example: For Connection Manager Version 1.6.1 - Released August 2021, the oldest Secret Server Version compatible would be 10.9.000000, released in August 2020.

- 1.9.0 release, refer to [Release Notes](#)
  
- 1.8.0 release, refer to [Release Notes](#) for details.
- Updated Connection Manager to reflect Delinea Inc. rebranding along with our new company colors and icons.
  
- 1.7.1 hotfix release, refer to [Release Notes](#) for details.
- 1.7.0 release, refer to [Release Notes](#) for details.
- Added section, [Using SSH Session Groups](#)
- Added more command line arguments to the [documentation](#) and we clarified related content such as which arguments should be used for installation and which should be used for startup.
- Added information to the [documentation](#) identifying default folders for macOS.
- Updated and clarified content in the [documentation](#) on Global Configuration options and their related behaviors.
  
- 1.6.2 release updates, refer to [Release Notes](#) for details.
- 1.6.1 Hotfix release updates, refer to [Release Notes](#) for details.
  
- 1.6.0 Feature release updates, refer to [Release Notes](#) for details.
  
- 1.5.0 Feature release updates, refer to [Release Notes](#) for details.
  
- 1.5.0 Feature release notes, refer to [Release Notes](#) for details.
  
- 1.4.1 Feature release updates, refer to [Release Notes](#) for details.

- 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](#)