Connection Manager

Administrator Guide

Version: 2.3.x

Publication Date: 1/26/2024

Connection Manager Administrator Guide

Version: 2.3.x, Publication Date: 1/26/2024

© Delinea, 2024

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Introduction to Connection Manager

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

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

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

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](#)

Permissions Required to Install/Uninstall Connection Manager

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

Product Versioning

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

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

Connection Manager Hashes

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

Version 2.3.1

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

- SHA1 fbefd08eb6230455938d73fad36bffdeae587bf1
- SHA256 0b1eb3925bdb4b4707a2285bd2629012c5b526013e7ad37bd3c23fd387e10bad

Version 2.3.0

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

- SHA1 aedde832f7c34d79b31e88421d63e9496da4933a
- SHA256 63630fad8f528325cd2f0b5192164109a922432f4c30c937ea8b9ecc58098b82

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

- SHA1 f5f17217f4d209c6b7d3557ba8409da3affca6ec
- SHA256 e1dced949523e37491cd00e125d85b3da8609e3bb056b7616f448029e66b5468

Version 2.2.0

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

- SHA1 2ec4505043d7335802dc367fbc7d0a65f7637775
- SHA256 1bc9ebcf525d3a0c9714114915259b0d30b249e456eb286f85f4cff8f37091a8

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

- SHA1 f093d6be323c2e37b978819e2861137d012df713
- SHA256 9bc8cc637c768fcf97095edd982a28b8a2d83bb10f3fc8635b67dca10762a27c

Version 2.1.0

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

- SHA1 91c7a23bced911a1c3adda58d37a6b44a3630213
- SHA256 3494ab7f2c655371e83632142d423cdd4460abadd6938b75a39cae304d27898d

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

- SHA1 ebbaf553311f10406d5b90312256a2d464736615
- SHA256 b3a80893ddd8edcf7c6b297e186836d6fdc4712c9230f91948192fd96393cd69

Version 2.0.1

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

- SHA1 fb2b89d80ed4dc5d0be6b7b50aec27d1c921d25d
- SHA256 f6c354bc4c809665b7149d6f64d1c73fc882773b31a916d39ba53be750416c64

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

- SHA1 02b364f3e3732ea9e0ff135427b8c9c0806bb952
- SHA256 666f677c4ff3f4178af2b60c5681ecd7232c2f44b1900ea01753f73474ab5a73

Version 2.0.0

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

- SHA1 e82ee65d82f5285772fc8ba99d88da3f78e4da23
- SHA256 dd466d665a5b07426783a1cb65b3a116c4369a71434bf109021f6db099f433d8

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

- SHA1 6dd1554632cf9169b3037e3faa453d52c62095b4
- SHA256 b78f4fceb367f92a74345088ae2fda8512f55fcda77edbb4acc6d2c464be07a3

Version 1.9.6

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

- SHA1 1eafddb64e3adb59b0064c011b84415b42c13852
- SHA256 2c700193690249a4f19fea0a32e68125e5167437016a3d8eb0738a6fd9fa50c4

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

- SHA1 939bd5397823c257e37c76e203451bb35b4b5bf4
- SHA256 20898cc7e1cb8789cc8311e06d7c3d946962e4ea7ad445e3cd78f838a27efe96

Version 1.9.5

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

- SHA1 ef4877367d6b7f85747a2f0f54b2830de5221aad
- SHA256 66fa4fa4e8818f405cbd6b36be2a89dc0965e112810e9db42b575b4722f02274

Version 1.9.2

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

- SHA1 91a5c9648d59bedbf13b0afe857eb9741dba335c
- SHA256 6a6925b848637292cf576d242db5af35259269d8abb87d89ecb576d46721ae2b

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

- SHA1 e5a2dd007aaa764e568d5f4e9af603eb026b8c74
- SHA256 fcd0c3e03607e8ee75a8e4127d74c6f68b29d42f83dfefd095367ec4356887e0

Version 1.8.0

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

- SHA1 e4989e93fc2d1a3f5d0bc92a298b99be2cd0ce1e
- SHA256 d5352367df30e254678026c6724a80bb2761b96c726b78b11ef61a556c59e44b

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

- SHA1 da39a3ee5e6b4b0d3255bfef95601890afd80709
- SHA256 e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Version 1.7.1 Hashes

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

- SHA1 c0e269a41fc8ac974f445d6769ae28b9bd2008ff
- SHA256 22387c20a1620938a642906f2c103b43ea5c608975722d8a1f1a0db4d30d9cc5

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

- SHA1 4ede9f06111d11fc77900427e416b8f7a0cf0c25
- SHA256 088aa3c6ec903e04ced12871198a40d0dfc1a2028c7f8bcc21dc916786986ef2

Version 1.7.0 Hashes

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

- SHA1 343c82d10b79abcff9302b7b1772f4caa8637047
- SHA256 3cf0ed060bc2b9d2639b779dd6e9c90c48adcd268646b9c3408726eac5bb1d05

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

- SHA1 9ae109074bffade9e2e3e0bca241db23457e0c50
- SHA256 b04fa74e41f522c3f13913b05194026b17ef329ba470e0200318cabf84b4962b

System Requirements

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

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

- Microsoft Windows: Windows 10 or later, Windows Server version 2016 or later; 8GB RAM.
- Apple macOS: 12 (Monterey), 13 (Ventura), 14 (Sonoma); 8GB RAM. Both Intel and Apple based systems are supported.

  Minimum requirements for connectivity to Secret Server vaults:

- Secret Server Version: 10.7 or later

Windows Installation

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

Installation of Connection Manager
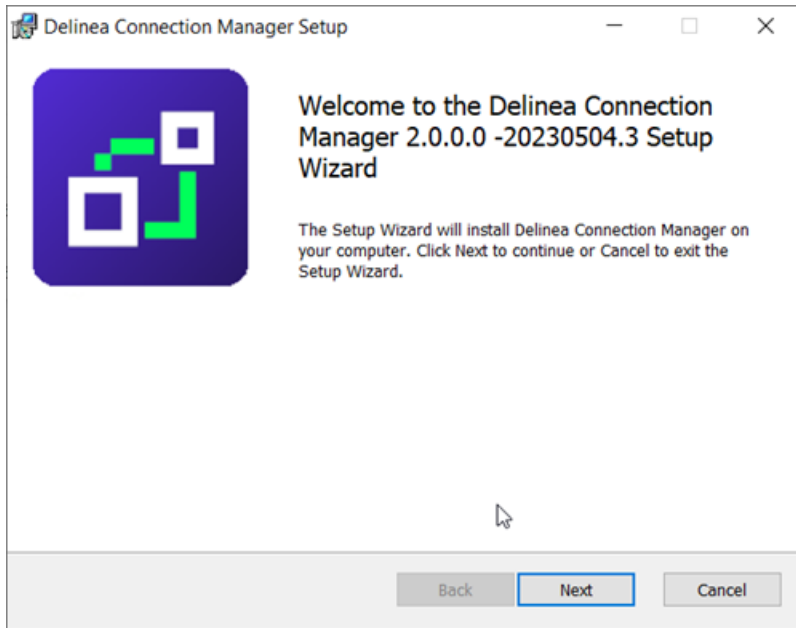
3. Click **Next** to continue.
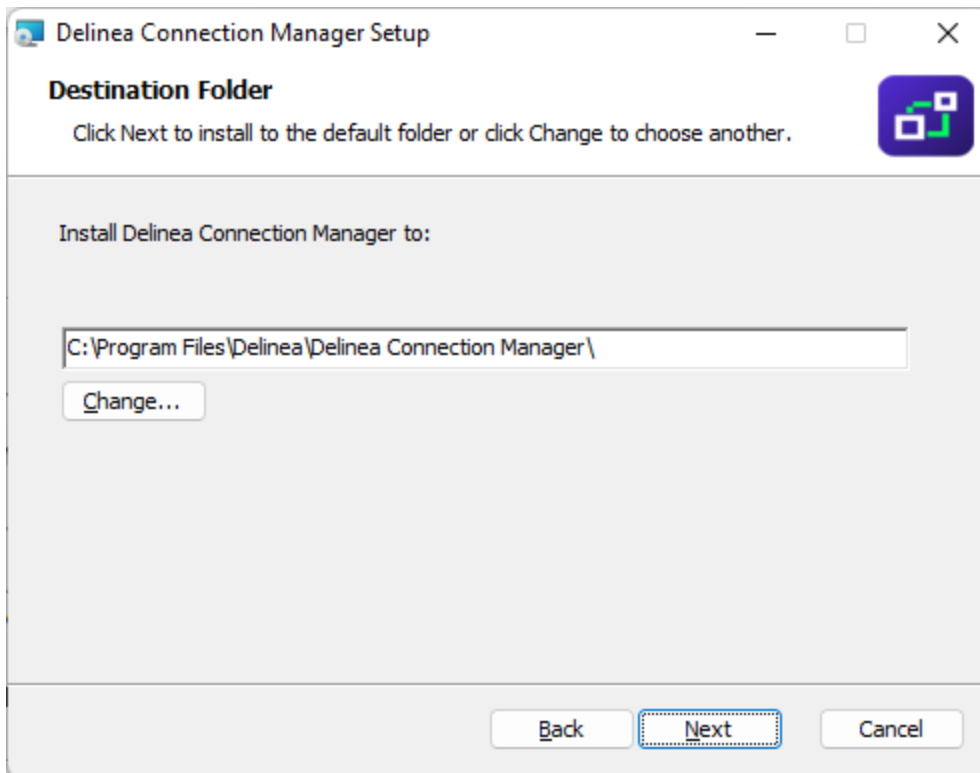
4. Select the **location to install Connection Manager** or leave the default location.
5. Click **Next** to confirm the location and accessibility for the install.
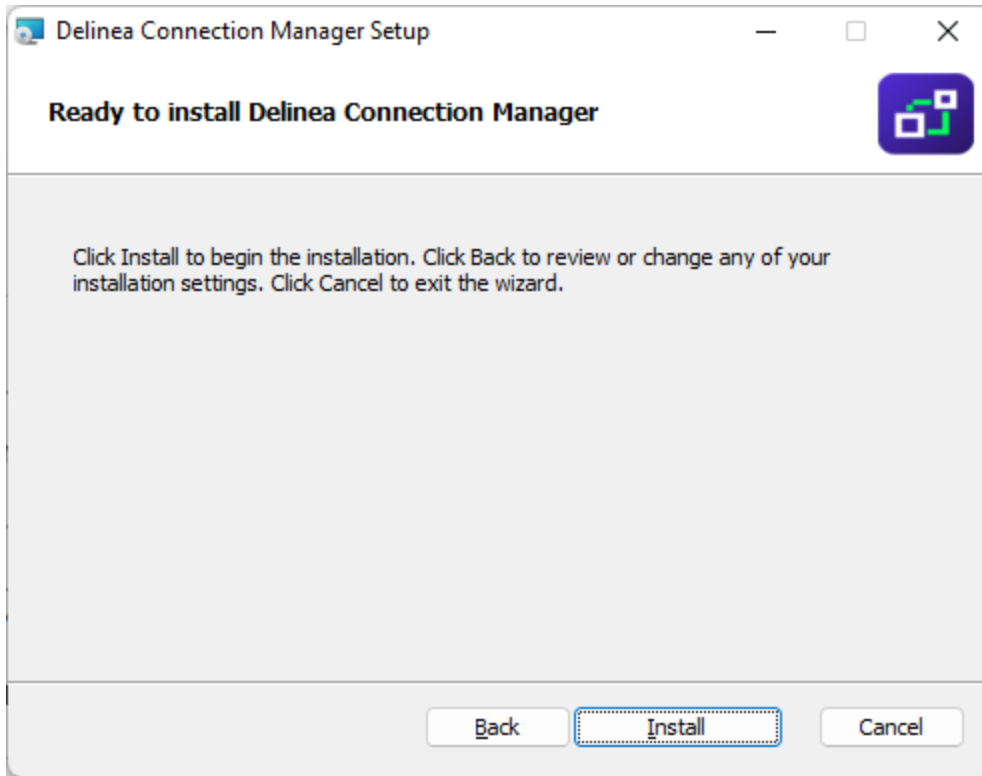
6. Click **Next** again to start the installation. A progress bar will be displayed while the installation is in progress.
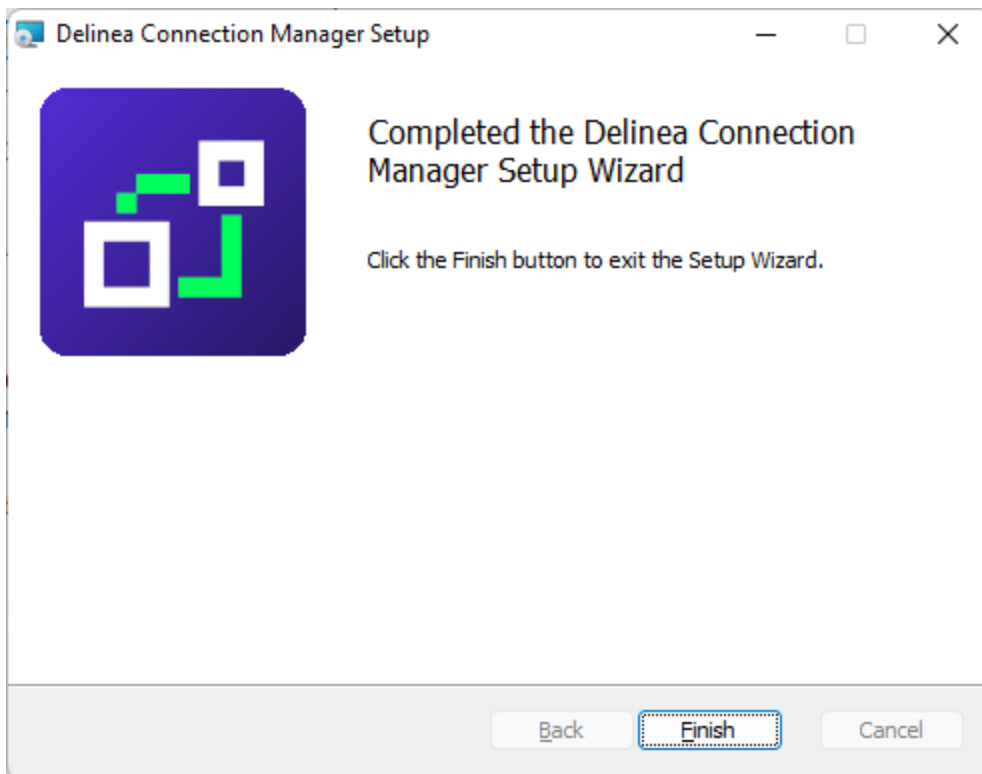
7. Once the install has finished, click **Finish**.

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

Updates

When the Connection Manager application is launched, users are prompted with an update message if a new release is available. If you would like to update, click **Download** or choose **Skip**.

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

Skip   Download

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 DelineaConnection Manager logo to the Applications folder. The installation begins.
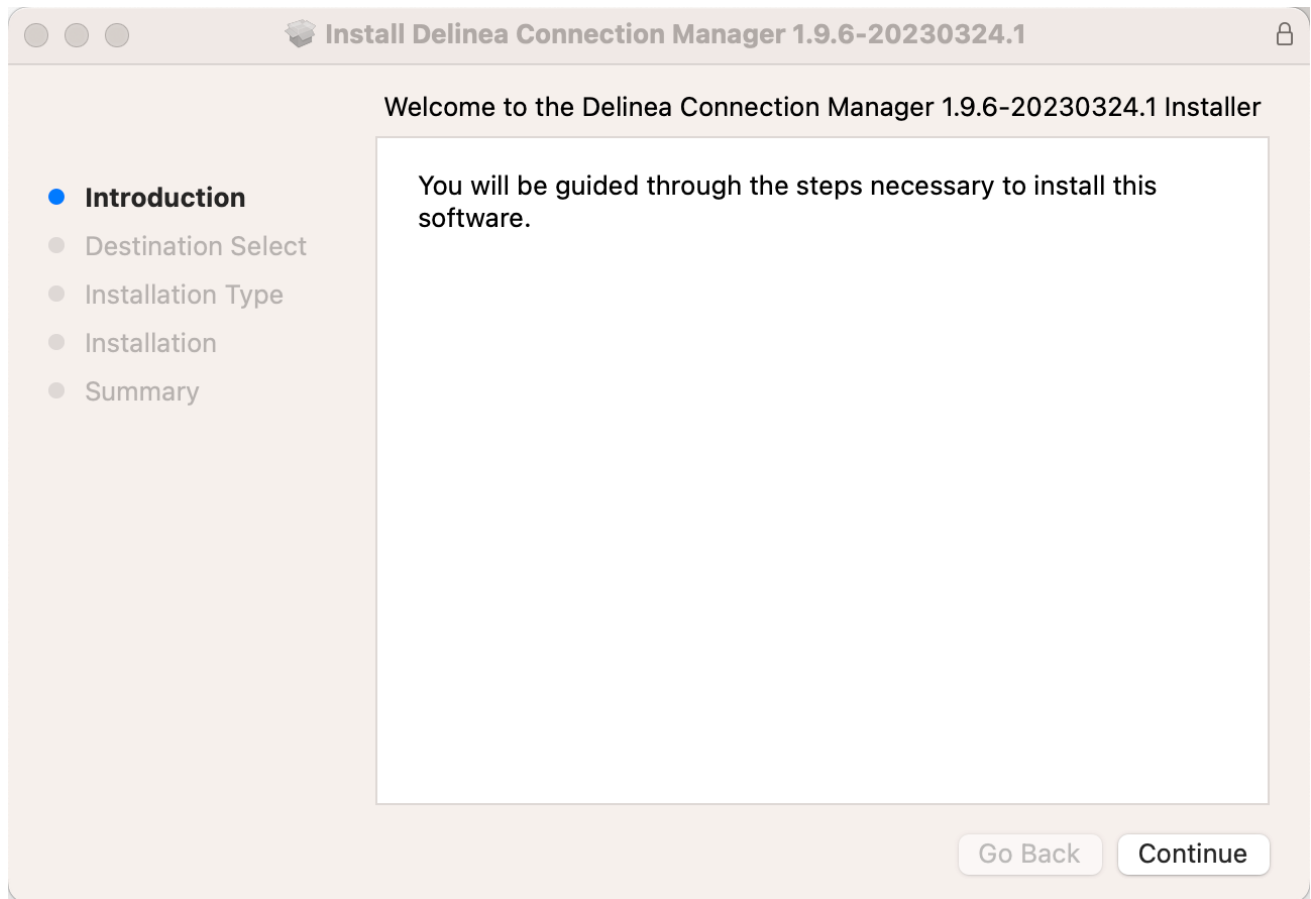
5. Once Connection Manager has been added, close the installer window.

> 📝 **Note:** If you receive the following message on your install, click **Open**.
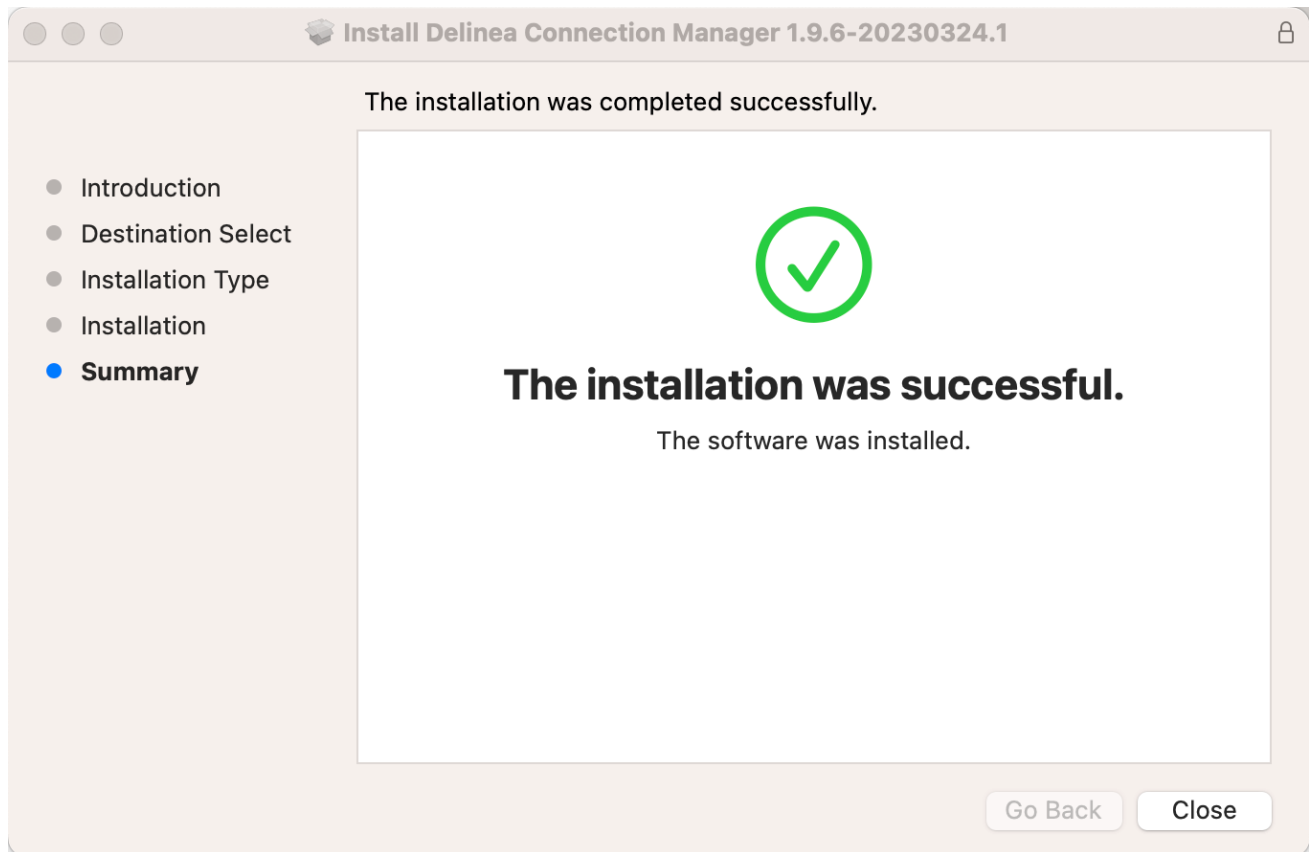
Enabling Screen Recording and Input Monitoring

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. If you would like to install the latest version of Connection Manager via quiet mode installation, you must first remove the previous version before installing the new one.

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

1. Prior to their initial log in, new users need to run Connection Manager via command line with *args -ssurl "your ss url" -ssname "your ss name" -ssauth "your auth type"*

2. Prior to their initial login, each user admin should create a file in path *C:\ProgramData\Delinea\Connection Manager\repository.dat* with the following content:

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

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

Disable Local Vault on Installation

Use this argument to disable the local vault on installation:

`-disablelocalvault`

Example

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

Specify Custom Logo Images to Copy to the Proper Location

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

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

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

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

`-logo, -logocollapsed`

Example

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

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

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

Two files are necessary to use custom logos:

1. Logo.png - 50 x 250 pixels

2. Logo_collapsed.png - 50 x 100 pixels

Delinea Platform Connection

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

Pre-create Secret Server Connection

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

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

External Browser Connection

Example

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

Example Powershell Command Line

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

Local Connection

Example

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

Example Powershell Command Line

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

Web Connection

Example

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

Example Powershell Command Line

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

Disable Local Vault

Example Powershell Command Line

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

Custom Logo

Example Powershell Command Line

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

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* C:\Users\ilyus\AppData\Roaming\Delinea\Connection Manag

Browse

Password*

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

Confirm Password*

Exit   Create

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.

1. Enter the password you previously created.

2. Click **Start**.

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

User Interface Components

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

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

Main Screen

The main screen consists of two components:

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

The two sections work in concert with each other.
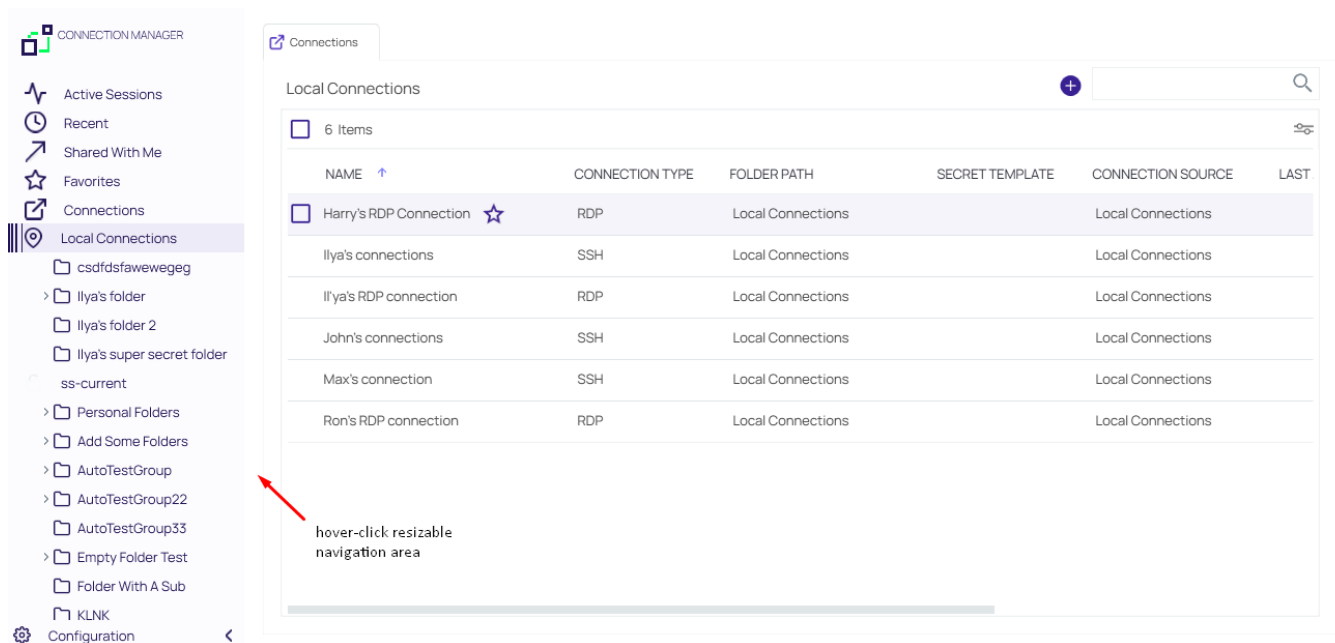
The navigation area is hover-click resizable.

Menus

There are several menu types available within the user interface:

Stack Menu

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

File

Under File you can do the following:

- Create new connections (RDP or SSH)

- Create new folders

- Delete folders/connections

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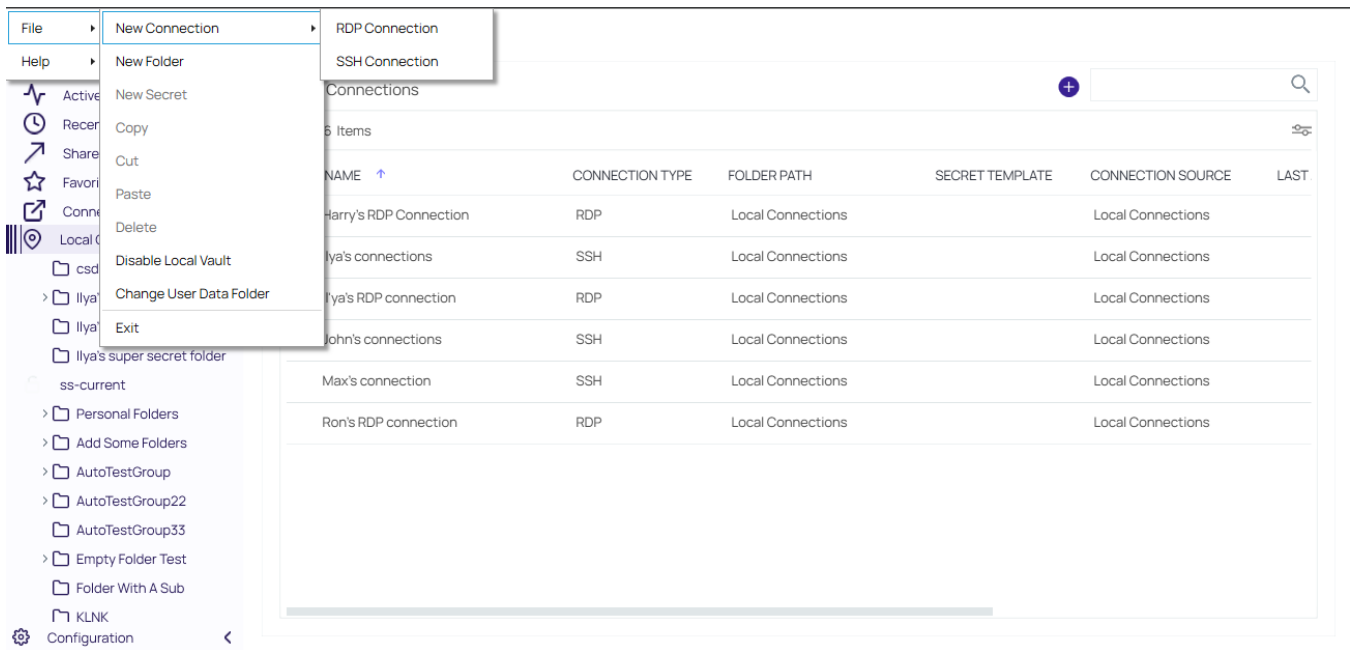
Note: The Stack menu is context sensitive so the available, displayed options depend on what is currently selected in the navigation tree or the main work area.

Help

Under Help you can select User Guide and About:
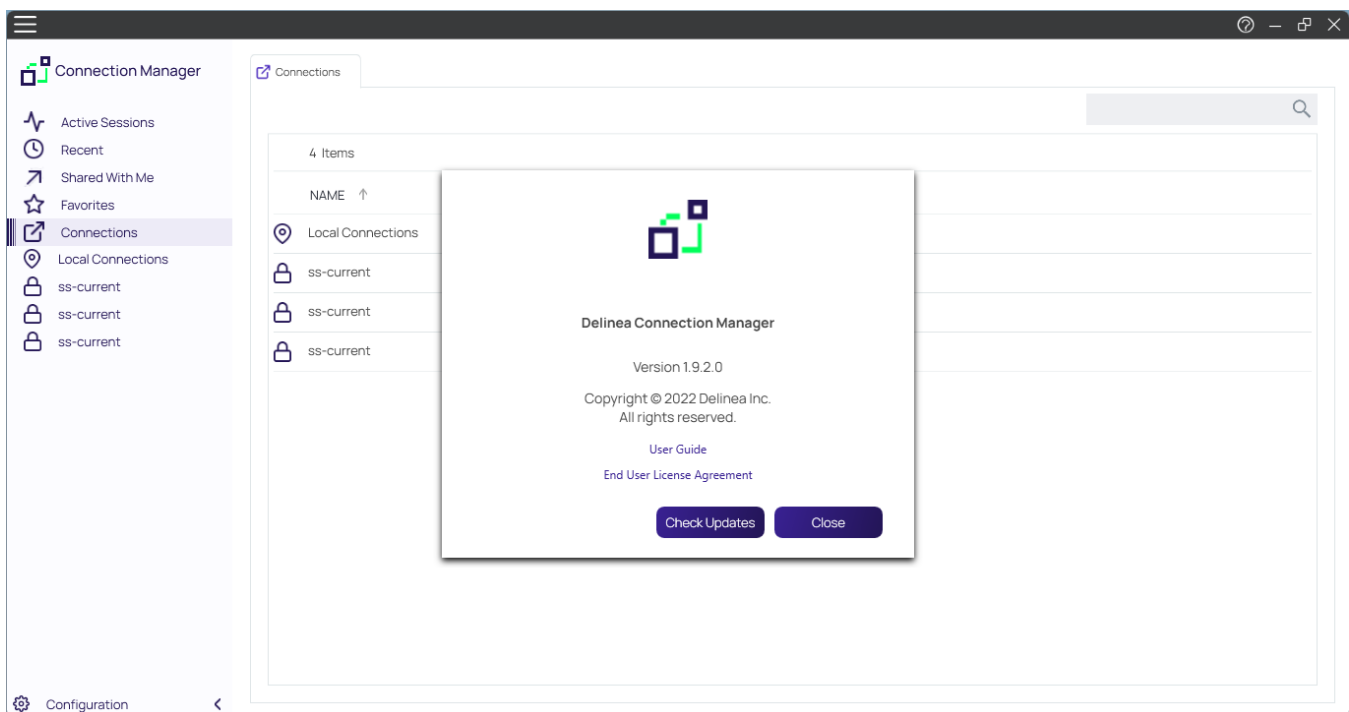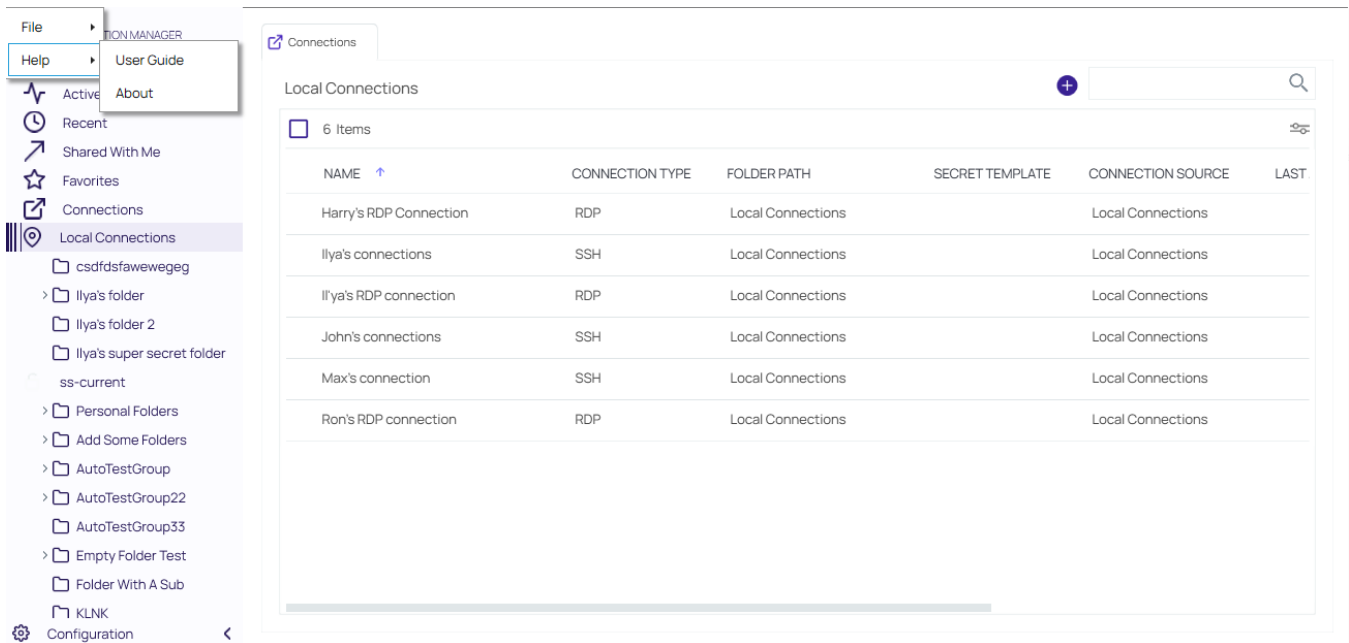
Right Click Navigation Menu

Right clicking a folder allows you to:

- Create new folders
- Create new connections
- Delete folders

- Export and Import connections
- Collapse and Expand Secret Server connections and Local connections

Work Area Menu

Right clicking the work area allows you to:

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

Search

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

Global Search

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

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

Configuration

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

Navigation Tree

Active Sessions

Select to view all active sessions.
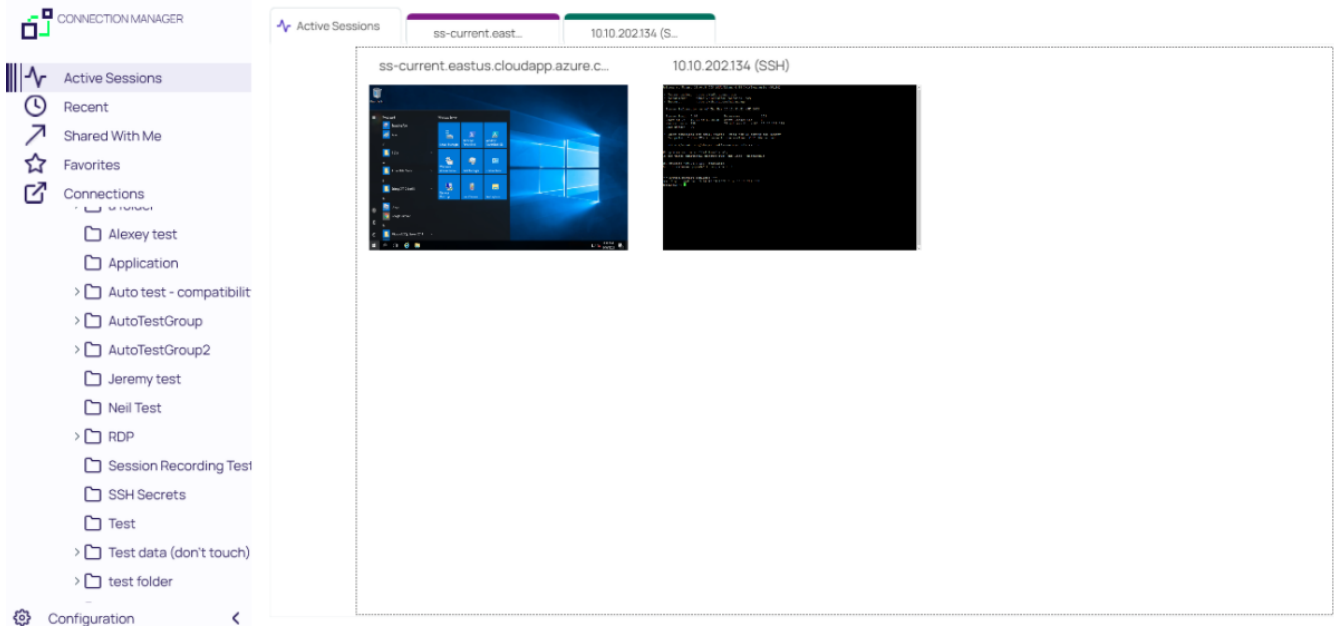
Favorites

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

Favorites page showing only local connection favorites:
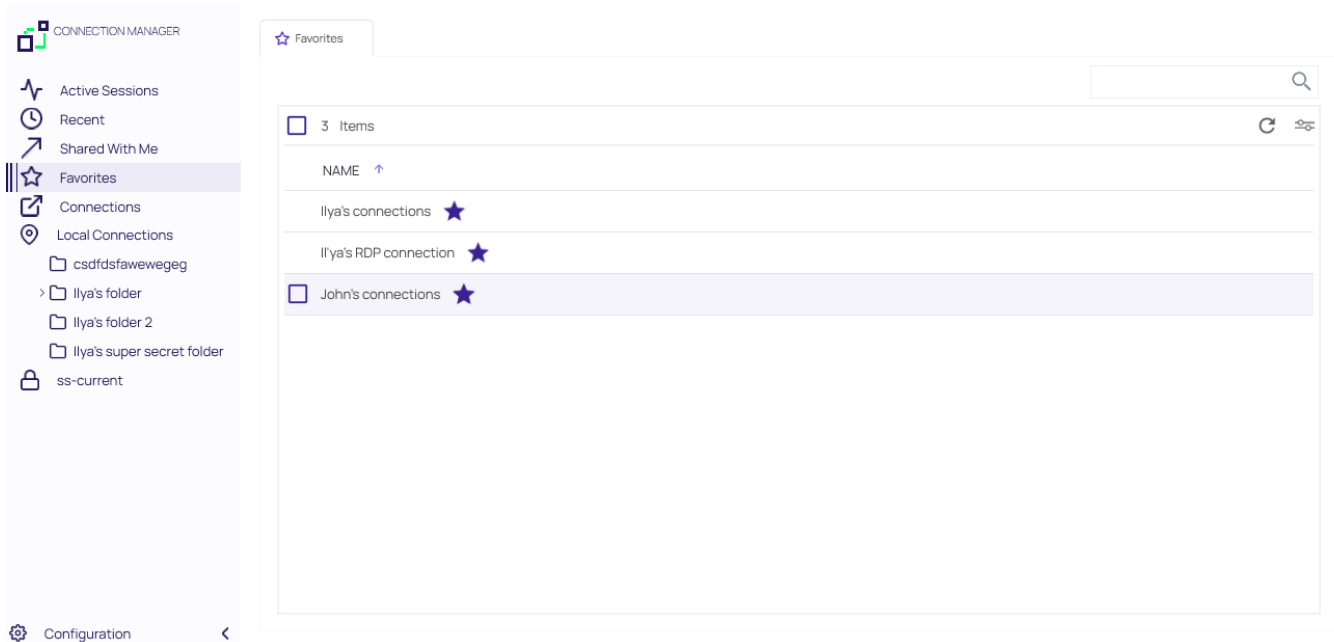
Favorites page showing local and Secret Server connection favorites:

Shared With Me

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

Double clicking on these Secrets will launch sessions.

Recent

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

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

Connections

Select to display the folder tree for Local and Secret Server connections.
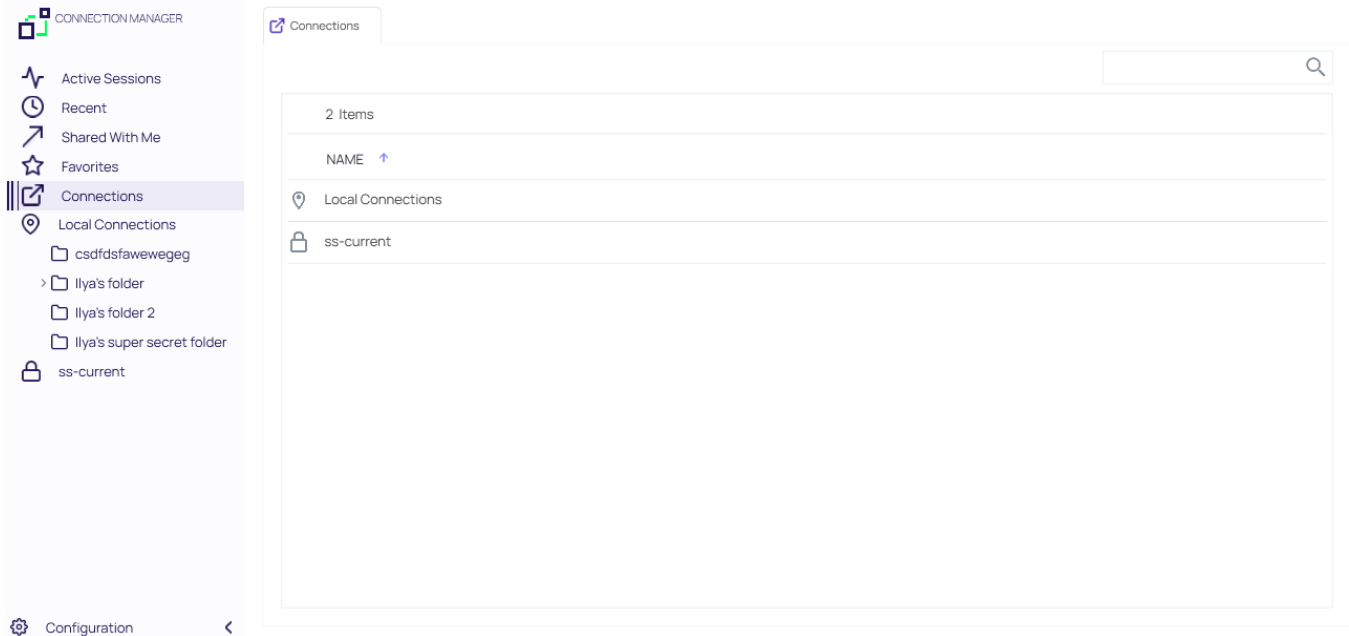
Navigate using the tree, or drill-down through folders to display in the work area window. Existing connections can be viewed via tab.
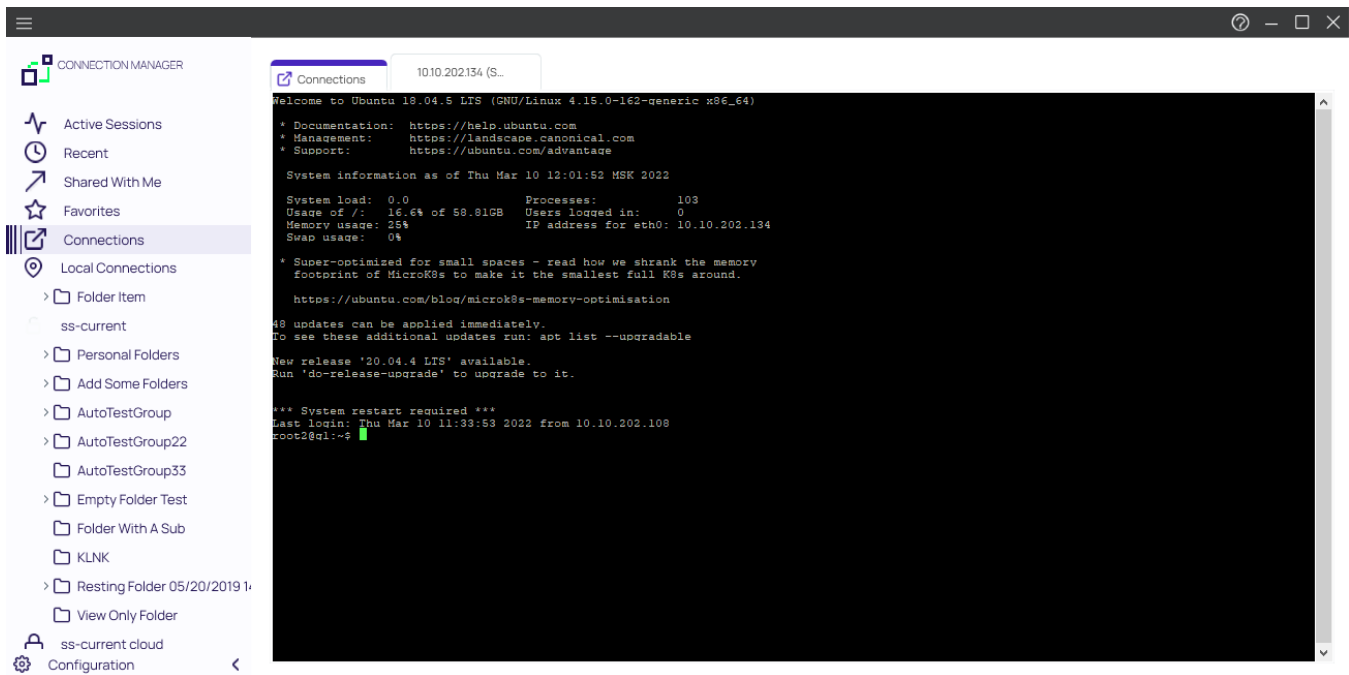
Local Connections

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

Shared with me

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

Configuration

Clicking within this area brings up a sub-menu with options such as
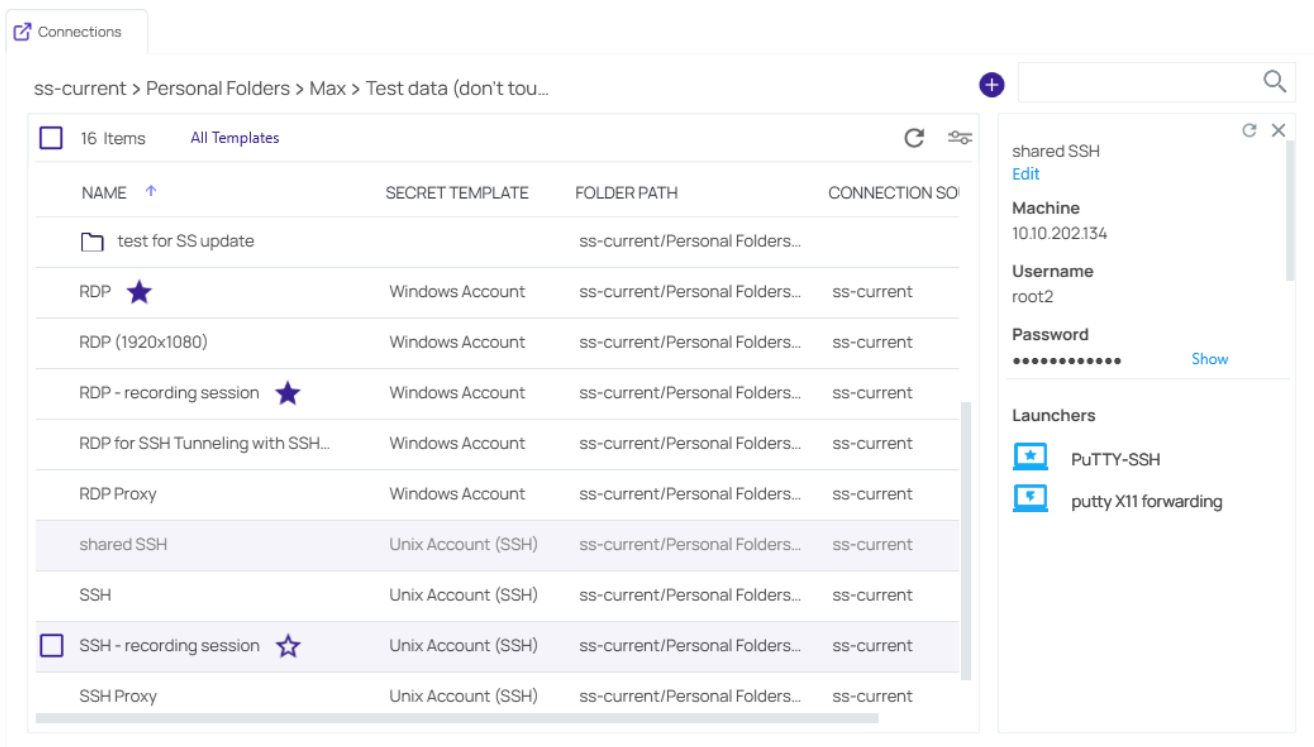
- Secret Server Connections and
- Global Configurations.
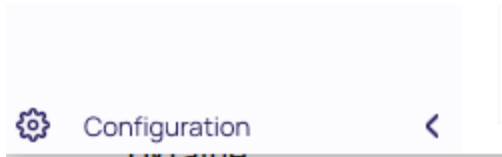
The **<** can be used to collapse and **>** expand the Navigation menu.

Properties Area

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

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

Work Area

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

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

Secret Server Requirements

What are the quick, hard requirements for connecting to Secret Server?

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

Connect to a Delinea Vault

Connect to the Delinea Platform

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

Connect to a Delinea Vault
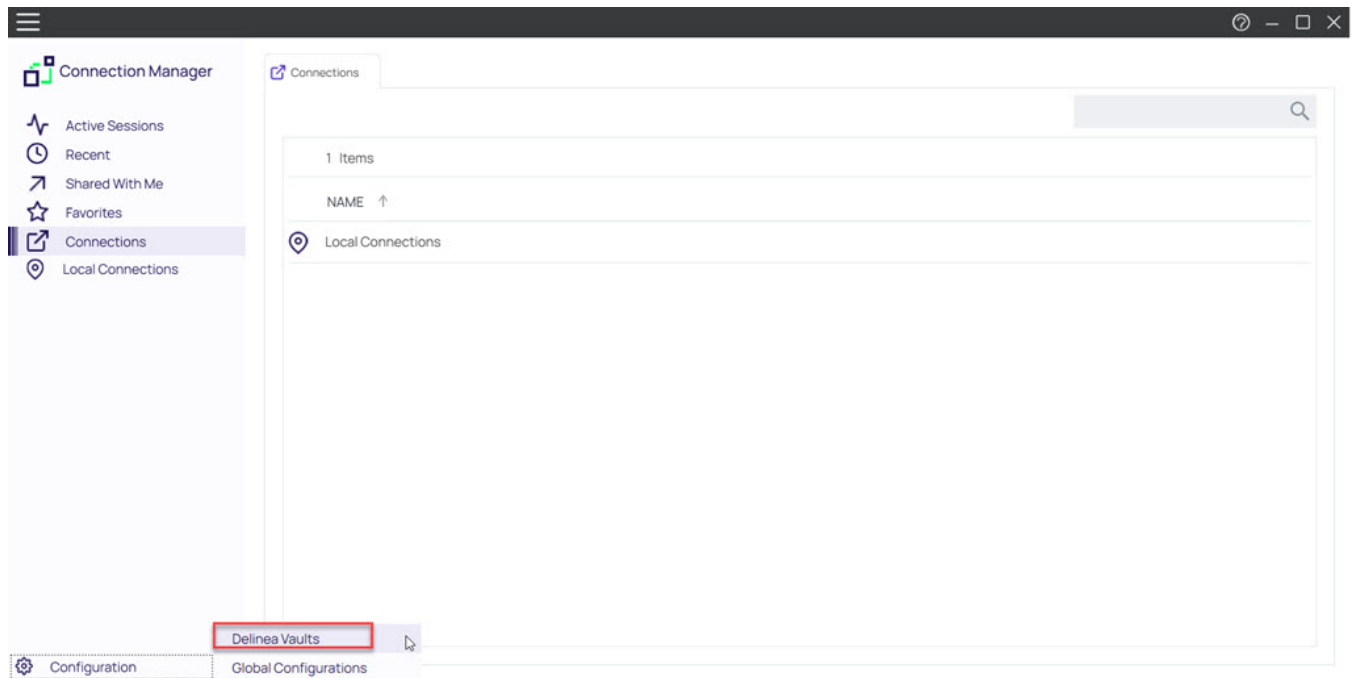
2. Enter your *Connection Name* and *Connection URL* and click **Next**

Add External Connection
Enter vault connection details

Connection Name*   art decco

Connection URL*   https://mycompany.delinea.app|
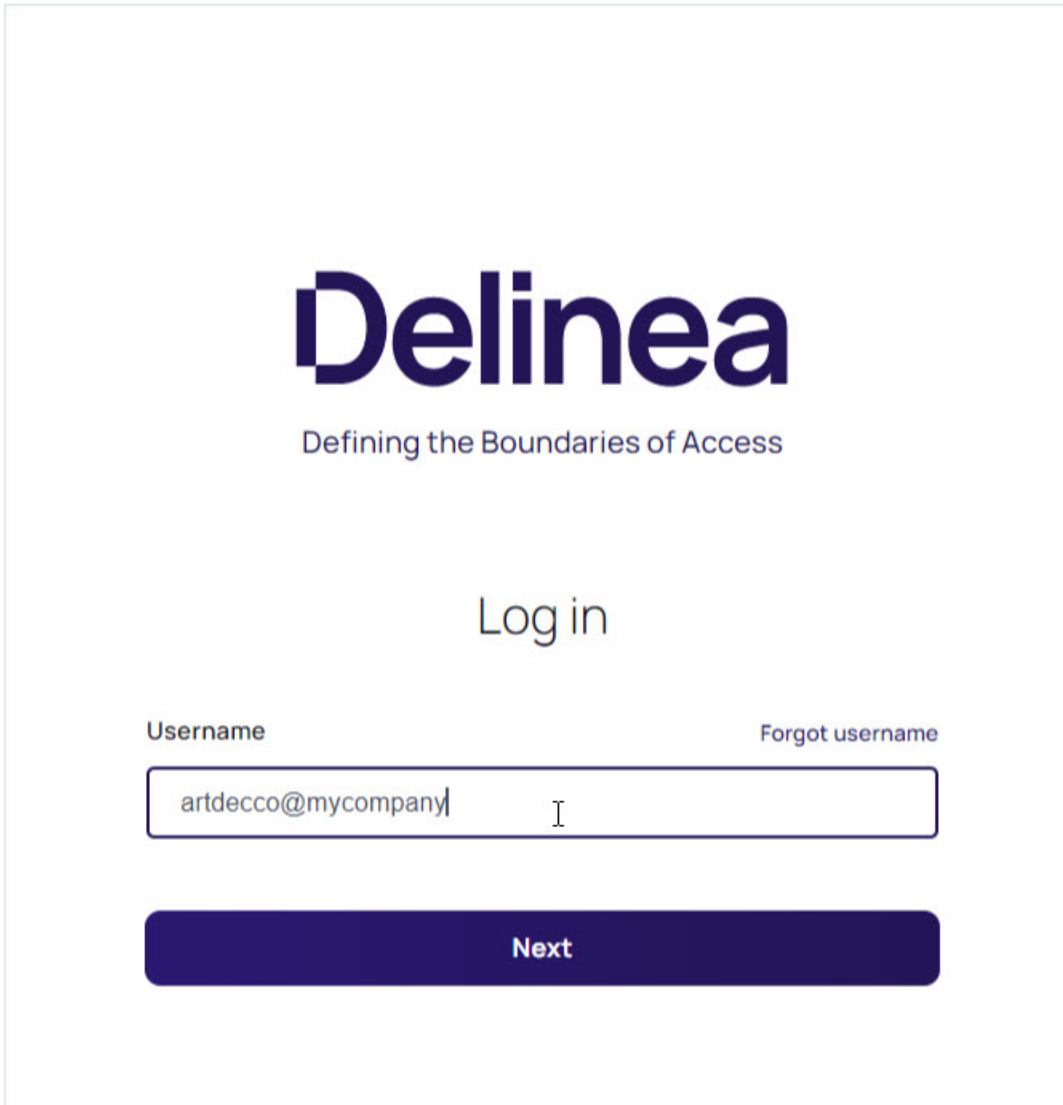
Cancel   Next

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

Add External Connection
Please, enter your credentials

Delinea

Defining the Boundaries of Access

Log in

Username   Forgot username

artdecco@mycompany
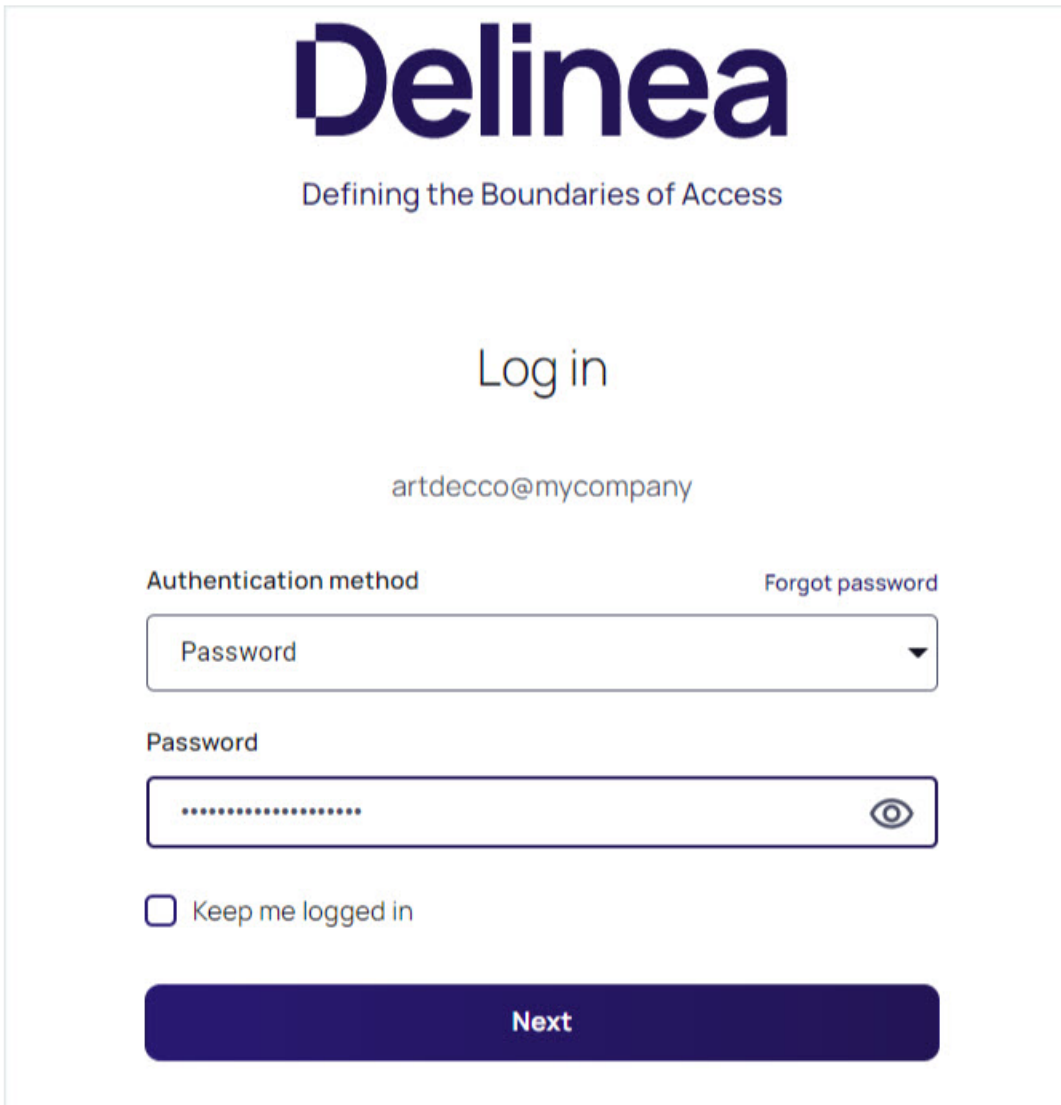
Next

Back   Cancel   Reload

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

Add External Connection
Please, enter your credentials

Delinea

Defining the Boundaries of Access

Log in

artdecco@mycompany

Authentication method   Forgot password

Password ▼

Password

•••••••••••••••••• 👁

☐ Keep me logged in

Next

Back   Cancel   Reload

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

Add External Connection
Select secret server templates to use in this application

- ● Everything (detect newly added templates)
- ○ Custom Selection (new templates must be manually added)

Back   Cancel   Finish

Add External Connection
Select secret server templates to use in this application

○ Everything (detect newly added templates)

◉ Custom Selection (new templates must be manually added)

Search for Template Name

▬	6	Selected
☐		17Jan
☑		Active Directory Account
☐		Active Directory Account Bug
☐		ADWEB
☐		Amazon IAM Console Password
☐		Amazon IAM Key
☐		AnOddWebPasswordTemplate
☐		Azure AD Account
☐		Azure Service Principal
☐		Bank Account
☐		BugTest
☐		Check

Back   Cancel   Finish

6. Your external vault has been created

External Vaults

Learn more about Adding Vaults

art decco   Edit   https://mycompany.delinea.app   Remove

Close   Add Vault

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.

External Browser

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

2. Click **Add Vault**

External Vaults

Learn more about Adding Vaults

art decco   Edit   https://mycompany.delinea.app   Remove

Close   Add Vault

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

Add External Connection
Enter vault connection details

Connection Name*   art decco's secret server

Connection URL*   https://mycompany.secretservercloud.com

Cancel   Next

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

Add External Connection
Choose login method and complete login.

Connection Name*	art decco's connection
Connection URL*	https://mycompany.secretservercloud.com
Authentication Type:	External Browser ▼

Local Login
Internal Browser
External Browser

ⓘ Clicking 'Next' will open Secret Server in browser.
Click Connection Manager Launcher to complete login process.
Click the Launcher to complete login process.

Back   Cancel   Next

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

Add External Connection
Please, enter your credentials

ⓘ **Must be on Secret Server Version 11.2**
If you are on a lower version, please change login option in the previous step.

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

Back   Cancel   Reload

6. Login with your Delinea Platform or Local Login credentials
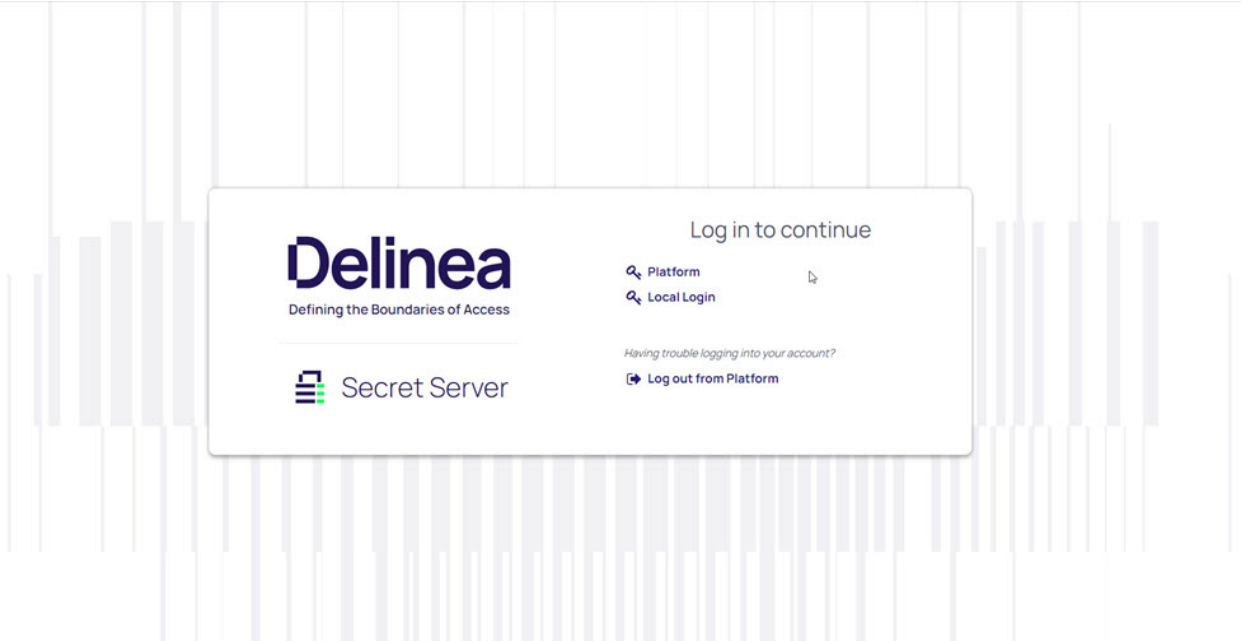
7. Under *Launchers,* click **Connection Manager**
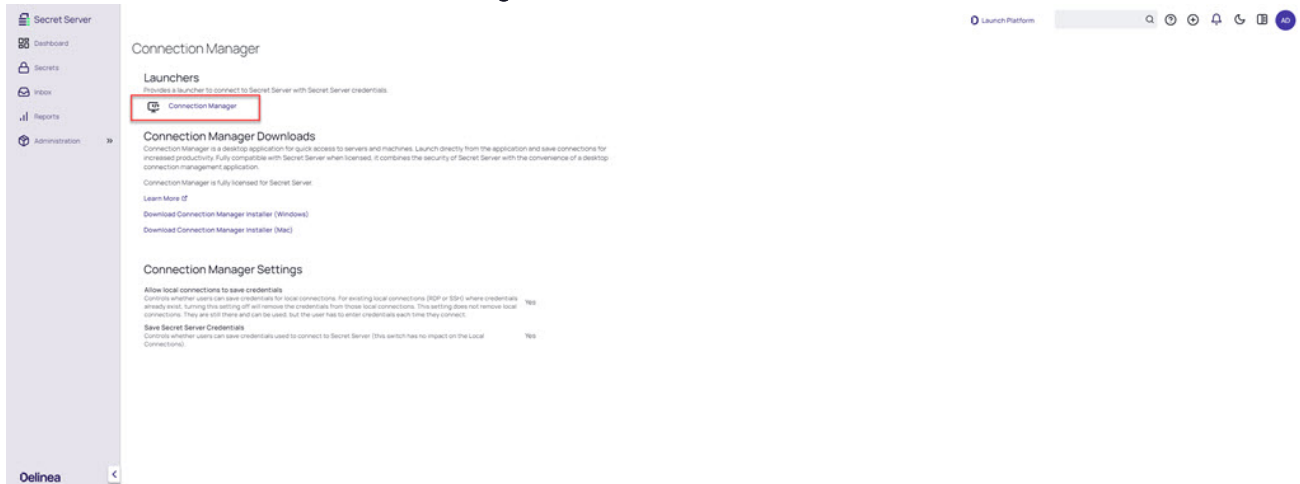
Internal Browser

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

2. Click **Add Vault**

External Vaults

Learn more about Adding Vaults

🔒 art decco   Edit   https://mycompany.delinea.app   Remove

Close   Add Vault

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

Add External Connection
Enter vault connection details

Connection Name*   art decco's secret server

Connection URL*   https://mycompany.secretservercloud.com

Cancel   Next

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

Add External Connection
Choose login method and complete login.

Connection Name*	art decco's secret server vault
Connection URL*	https://mycompany.secretservercloud.com
Authentication Type:	Internal Browser ▼

Local Login
Internal Browser
External Browser
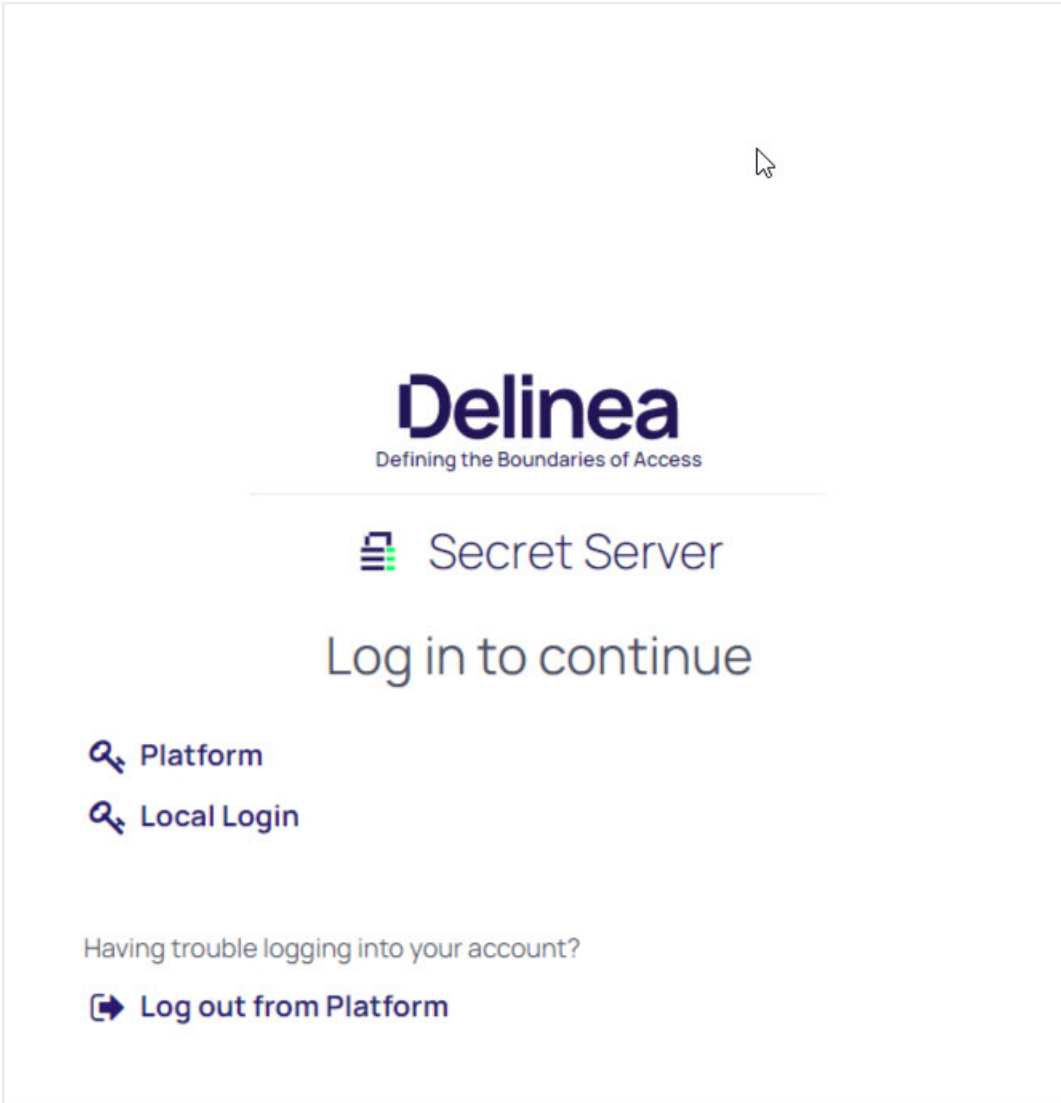
Back		Cancel	Next

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

Add External Connection
Please, enter your credentials

Delinea
Defining the Boundaries of Access

⊟ Secret Server

Log in to continue

🔑 **Platform**

🔑 **Local Login**

Having trouble logging into your account?

➡ **Log out from Platform**

Back   Cancel   Reload

Local Username/Password

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

2. Click **Add Vault**

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

Add External Connection
Enter vault connection details

Connection Name*   art decco's secret server

Connection URL*   https://mycompany.secretservercloud.com

Cancel   Next

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

Add External Connection
Choose login method and complete login.

Connection Name*   art decco's secret server

Connection URL*   https://mycompany.secretservercloud.com

Authentication Type: Local Login   ▼
                      Local Login
                      Internal Browser
                      External Browser

Back   Cancel   Next

5. Complete all of the required fields

Add External Connection
Please, enter your credentials

Username*

Password*

Domain

Two Factor: Select two factor authentication that applies:

   ◉ None

   ○ Pin Code

   ○ Duo Push

   ○ Duo Phone Call

Remember me: ☐ Store credentials locally

   ☐ Launch automatically at application start

Back   Cancel   Connect

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

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

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

Click **Connect**.

6. Select the Secret Server templates to use with this connection. You can choose to use all templates or custom selcted ones.

Add External Connection
Select secret server templates to use in this application

- ⦿ Everything (detect newly added templates)
- ◯ Custom Selection (new templates must be manually added)

Back   Cancel   Finish

Add External Connection
Select secret server templates to use in this application

○ Everything (detect newly added templates)

◉ Custom Selection (new templates must be manually added)

Search for Template Name

▬	6	Selected

☐ 17Jan

☑ Active Directory Account

☐ Active Directory Account Bug

☐ ADWEB

☐ Amazon IAM Console Password

☐ Amazon IAM Key

☐ AnOddWebPasswordTemplate

☐ Azure AD Account

☐ Azure Service Principal

☐ Bank Account

☐ BugTest

☐ Check

Back

Cancel

Finish

7. Click **Finish**

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*   ss-current

Secret Server URL*   https://connmanagerss.thycotic.net/ss-current

Authentication Type: ⦿   Local Username/Password
                        ○   Web Login

Cancel   Next

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*	max
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 ☐

[Back]   [Cancel] [Connect]

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.
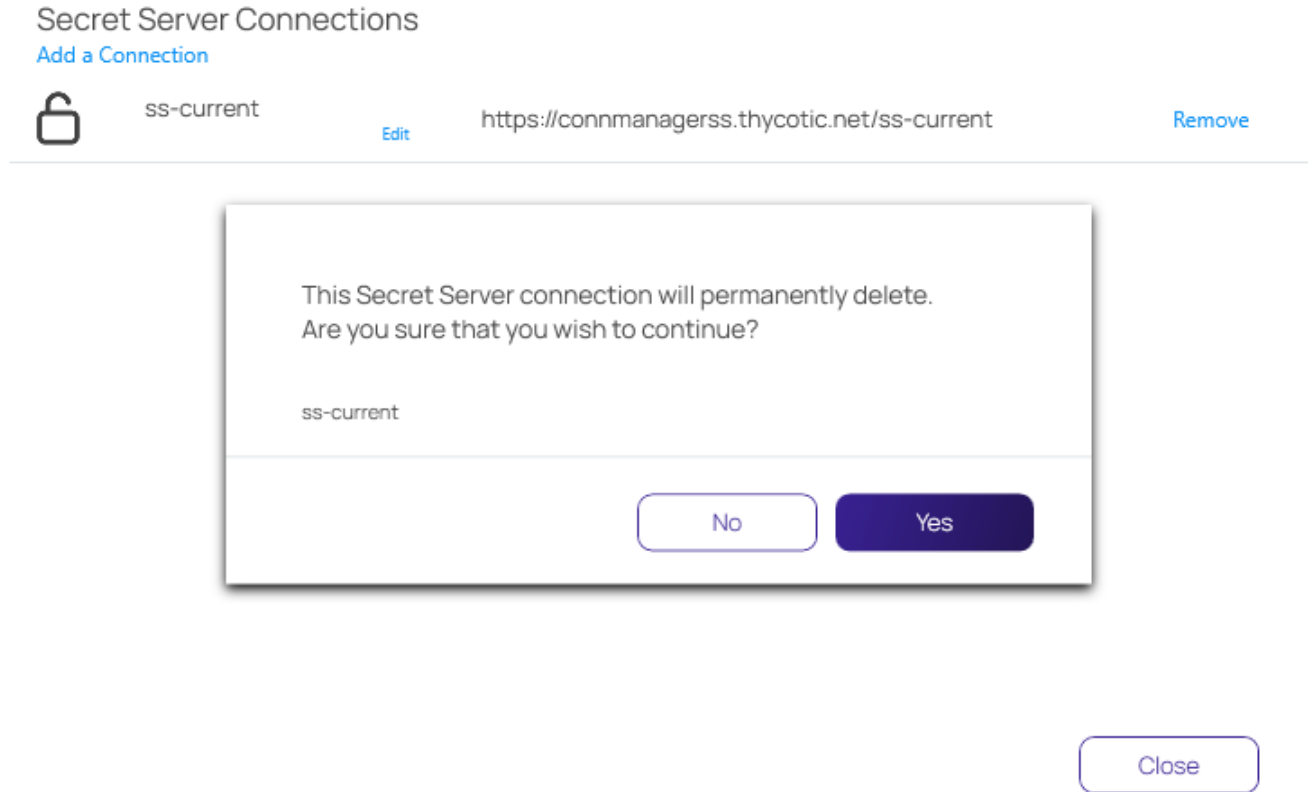
3. Click **Yes** to confirm.

Import and Export Connections

The following topics are available:

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

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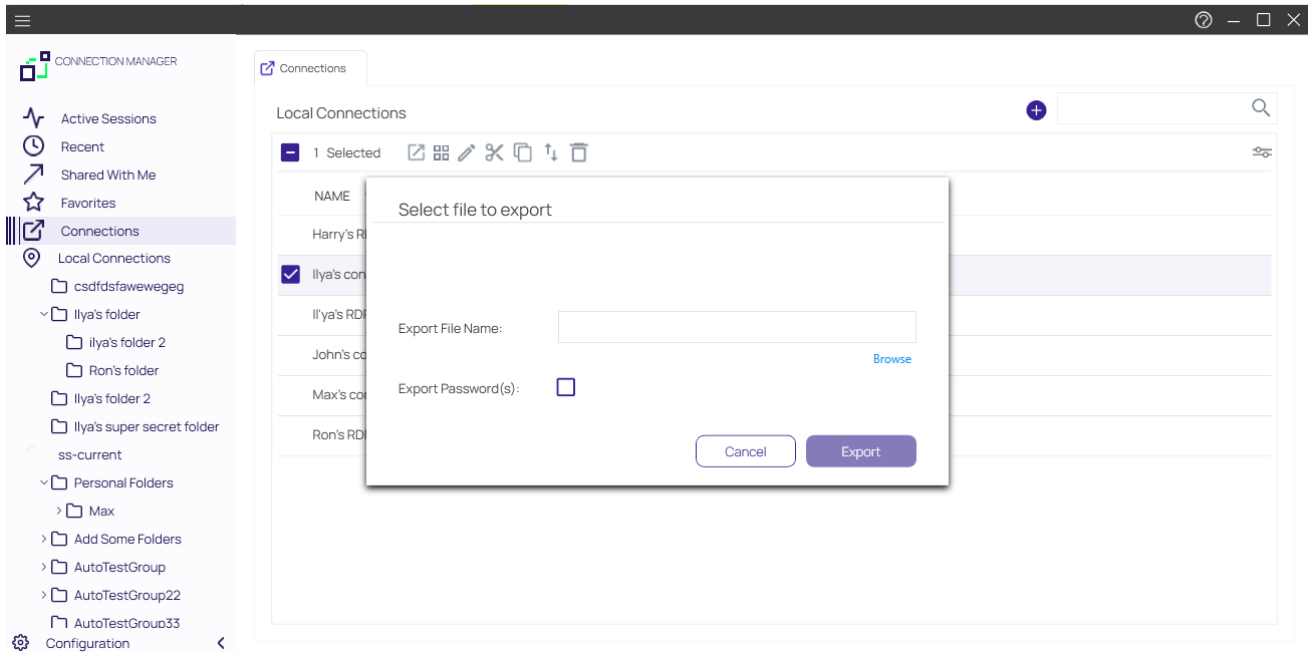
3. Click **Browse** and enter **the location and file name** for export.

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

4. Click **Export** to complete the action.

Import of JSON Files

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

To initiate an import, perform the following:

1. On the Connection Manager navigation tree, select the **Local Connection folder** to which the contents should be imported.

2. Right-click and select **Import**. A file browser window opens.

3. Navigate to the location of the .JSON file containing the content for import.

4. Select the .JSON file and click **Open**. The Connections are imported.

JSON Example

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

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

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

Import of Devolution Files

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

1. Right click on **Local Connections**

2. Hover over **Import** and select **Devolutions file**
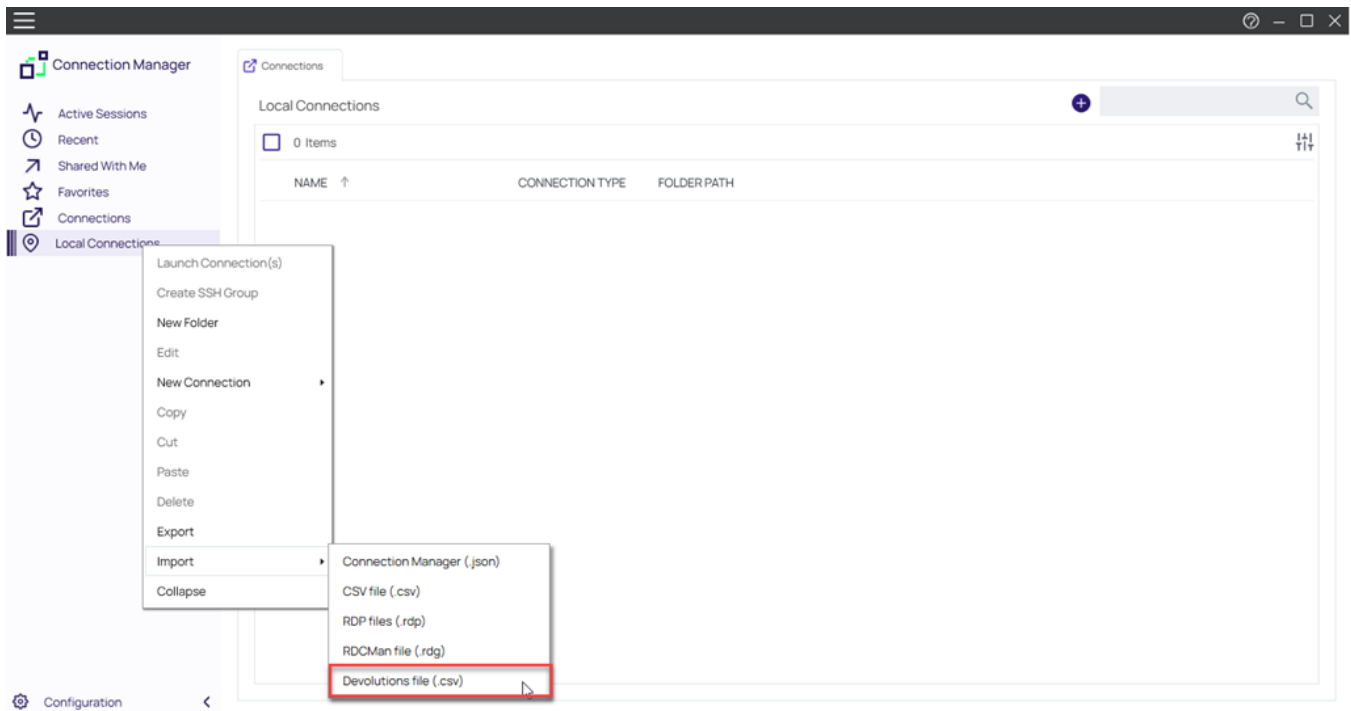
3. A dialog window will appear. Select the files you would like to import.
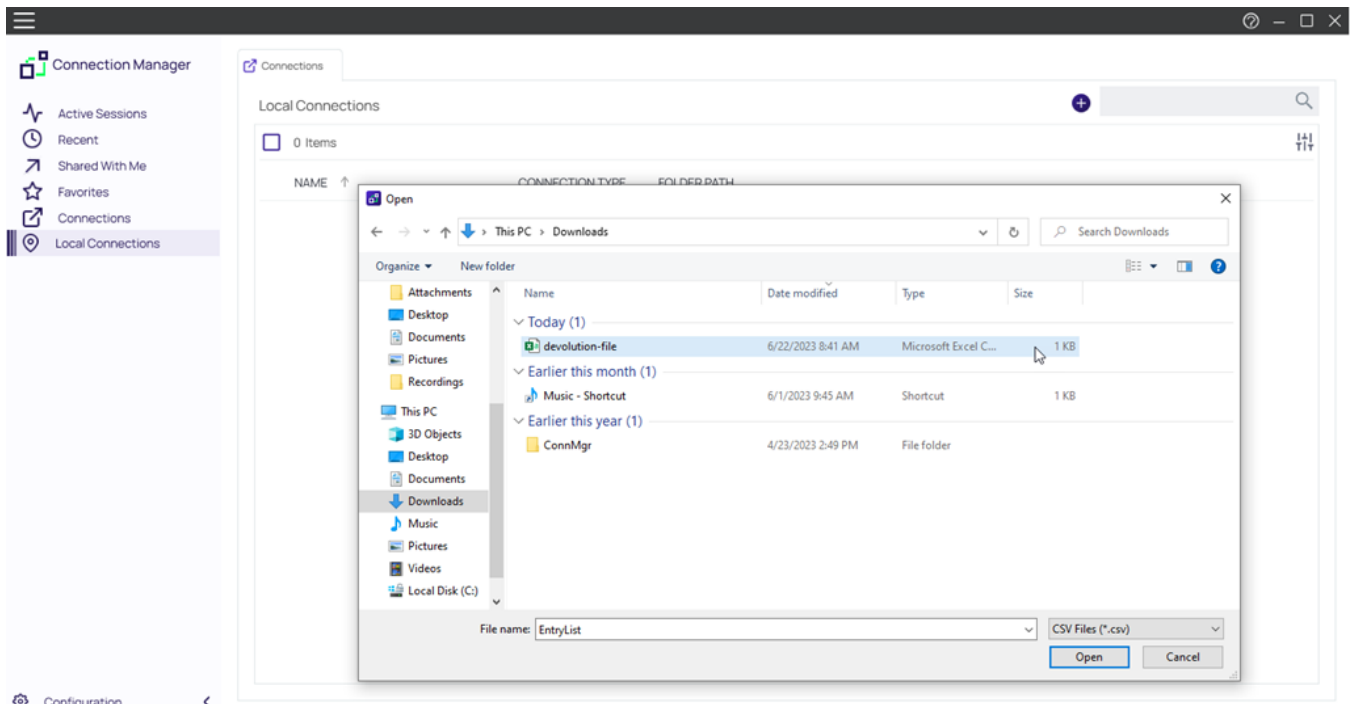
4. After the import is complete, a confirmation window will appear that the import was successful.
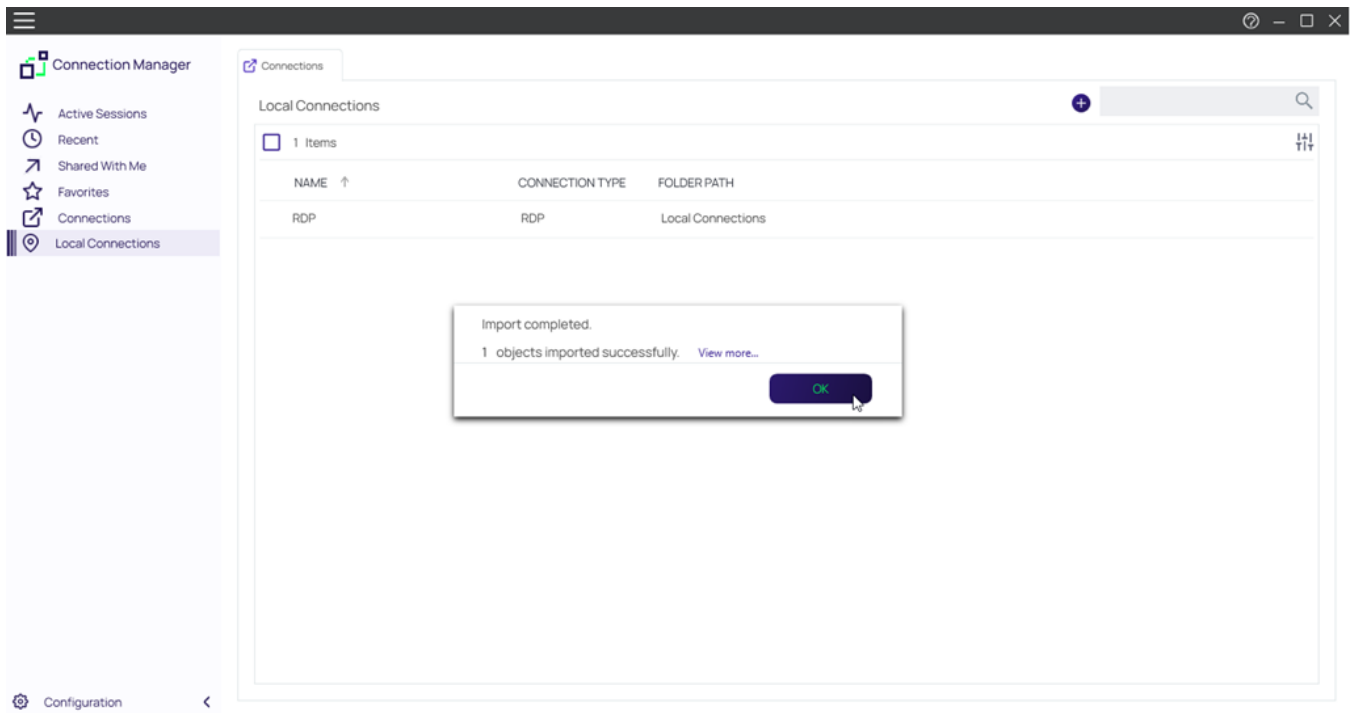
5. Click **OK** to return back to your Local Connections.

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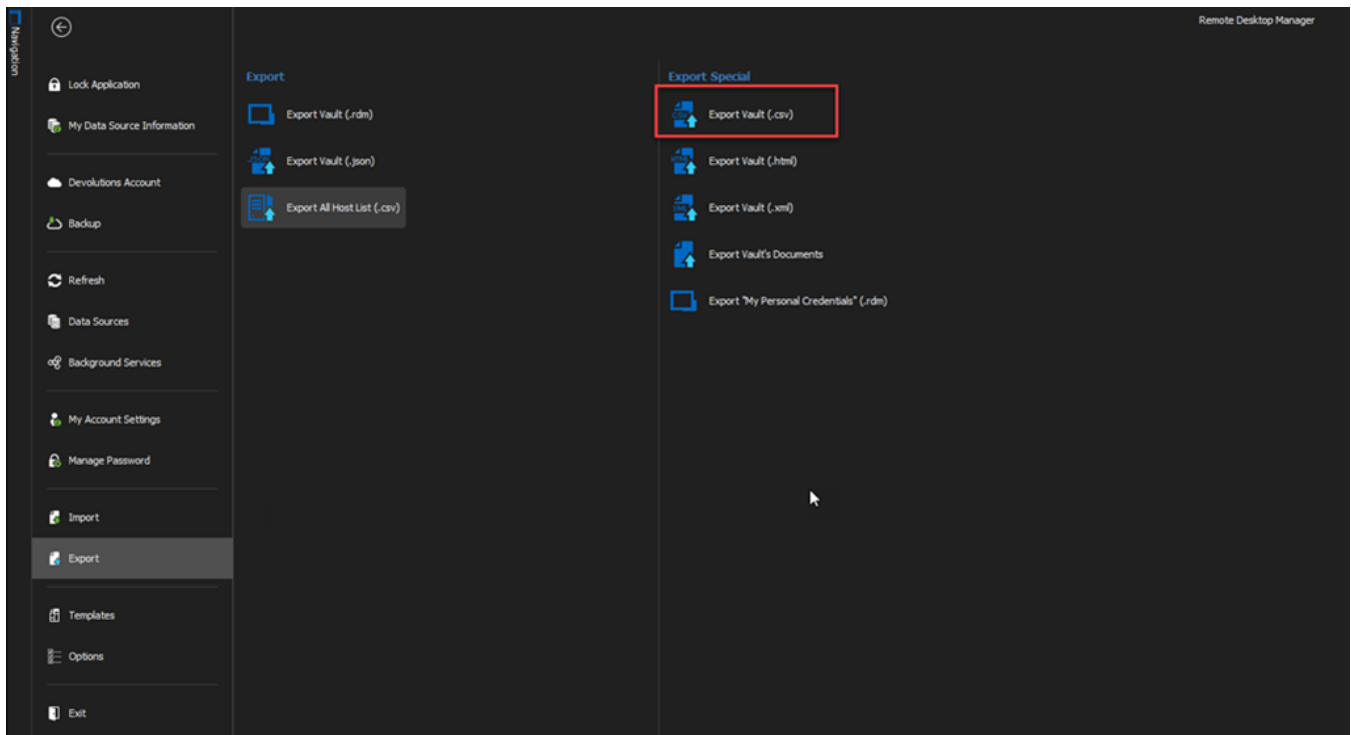
Import of RDG Files

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

1. Right click on **Local Connections**

2. Hover over **Import** and select **RDG**
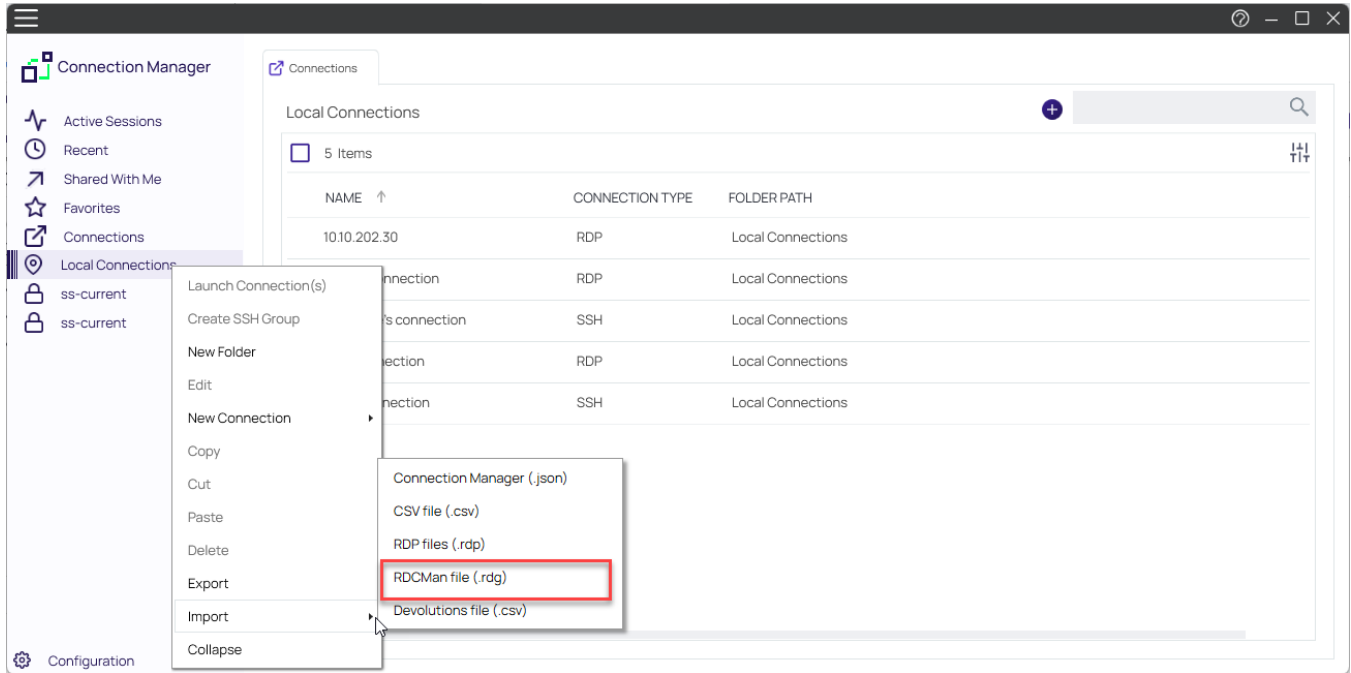
2. A dialogue window will appear. Select the files you would like to import.
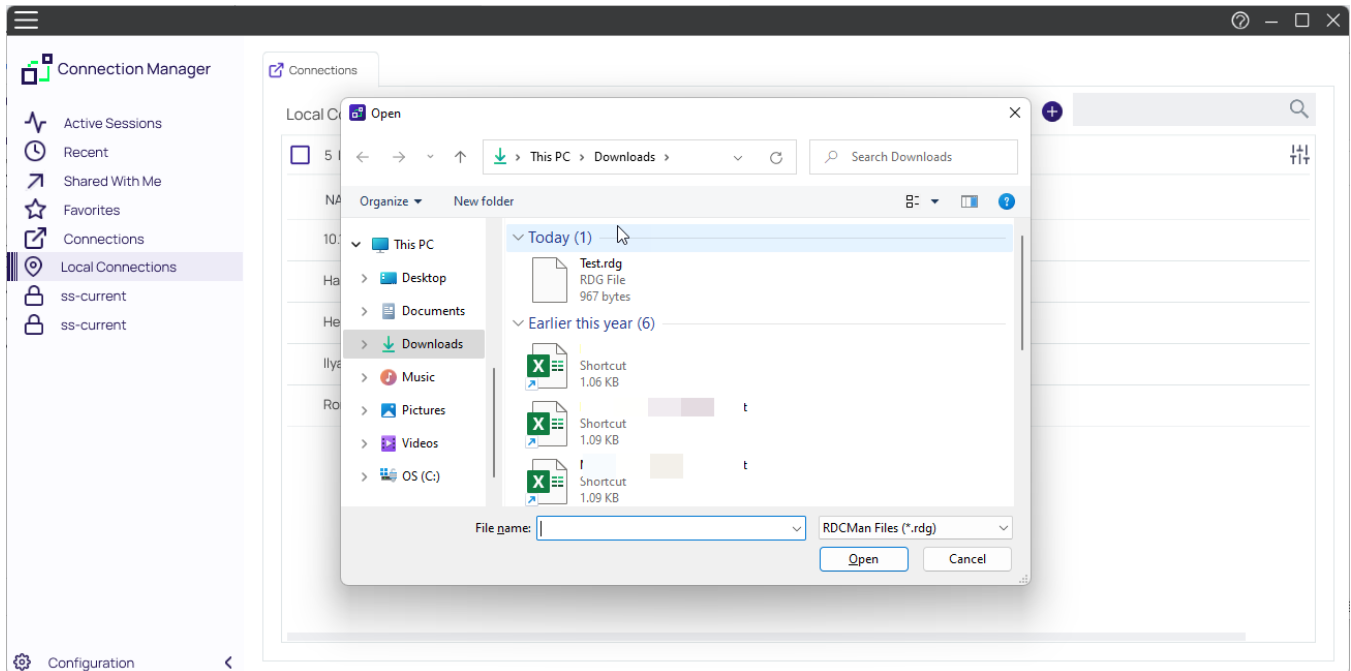
3.   After the import is complete, a confirmation window will appear that the import was successful.
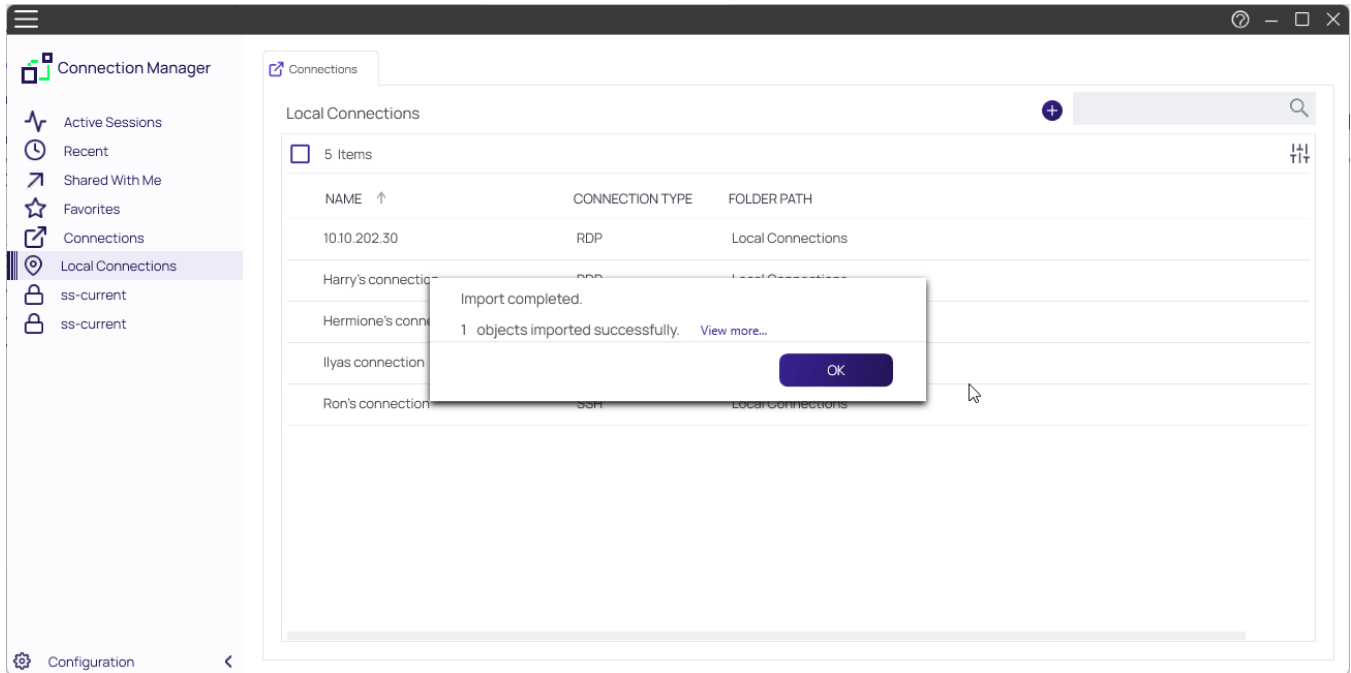
Click **OK** to return back to your Local Connections.

Import of RDP Files

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

1.   Right click on **Local Connections**

2.   Hover over **Import** and select **RDP**
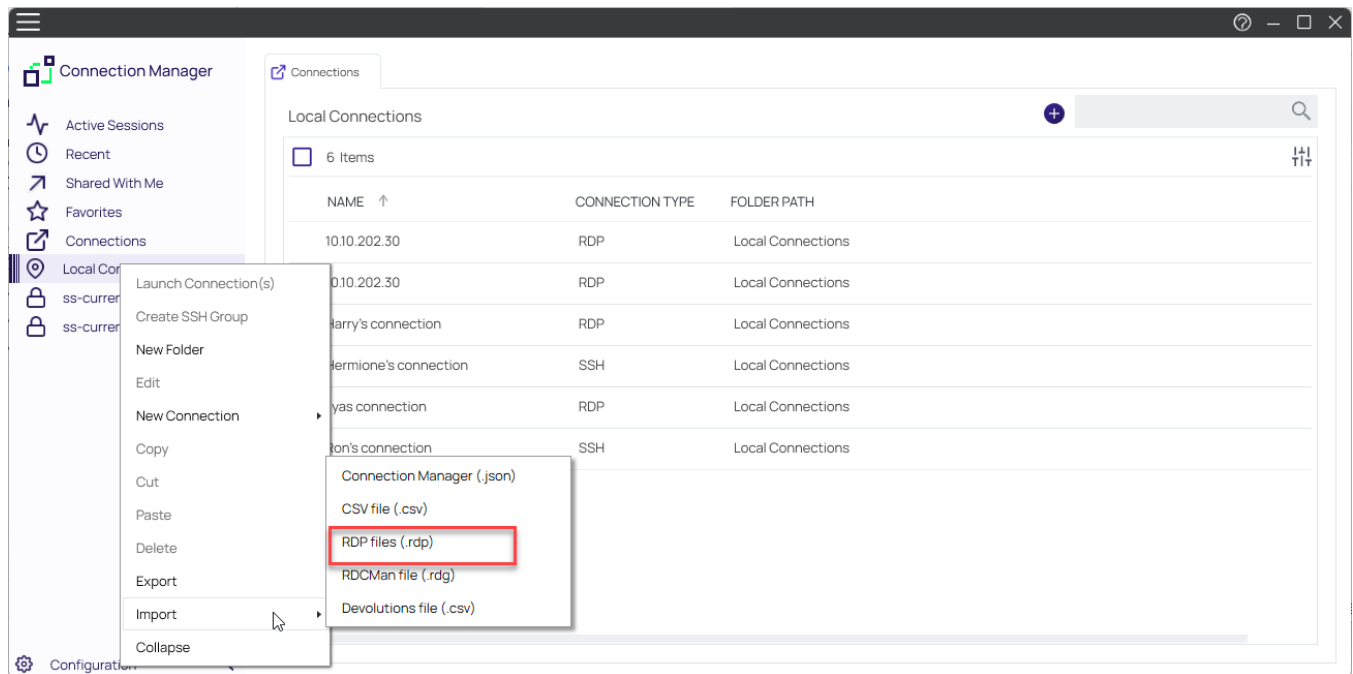
3. A new window will appear. Click **Browse** to start selecting RDP files to import.

Import RDP files (.rdp)
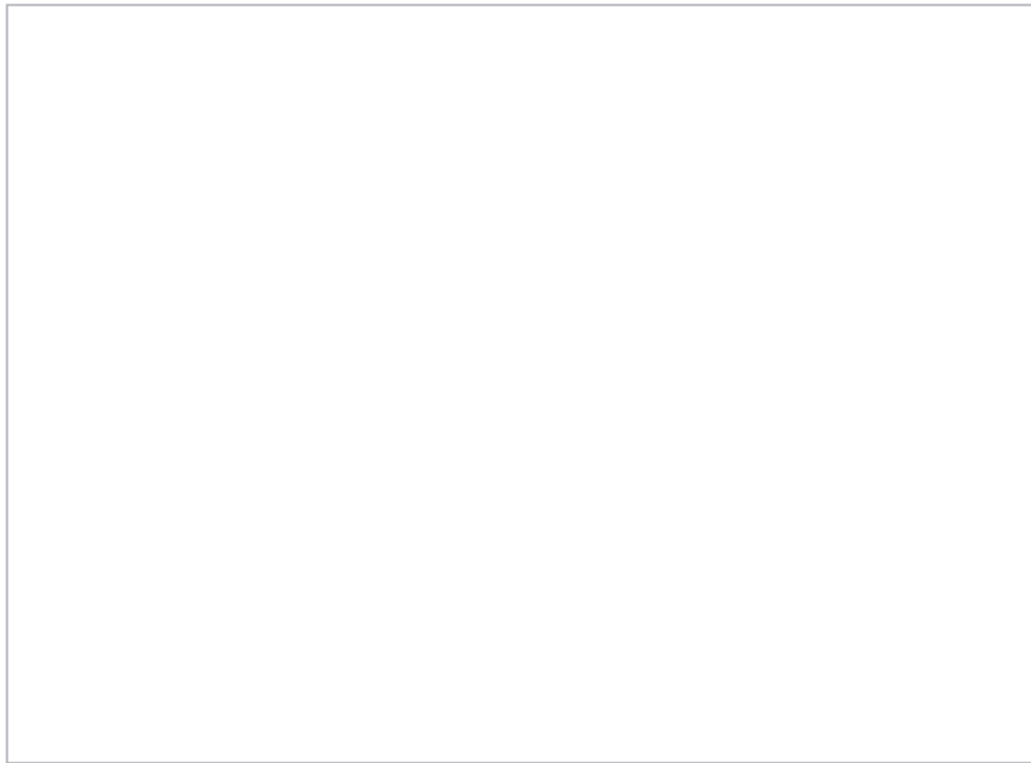
Select RDP files

Browse

Cancel   Finish

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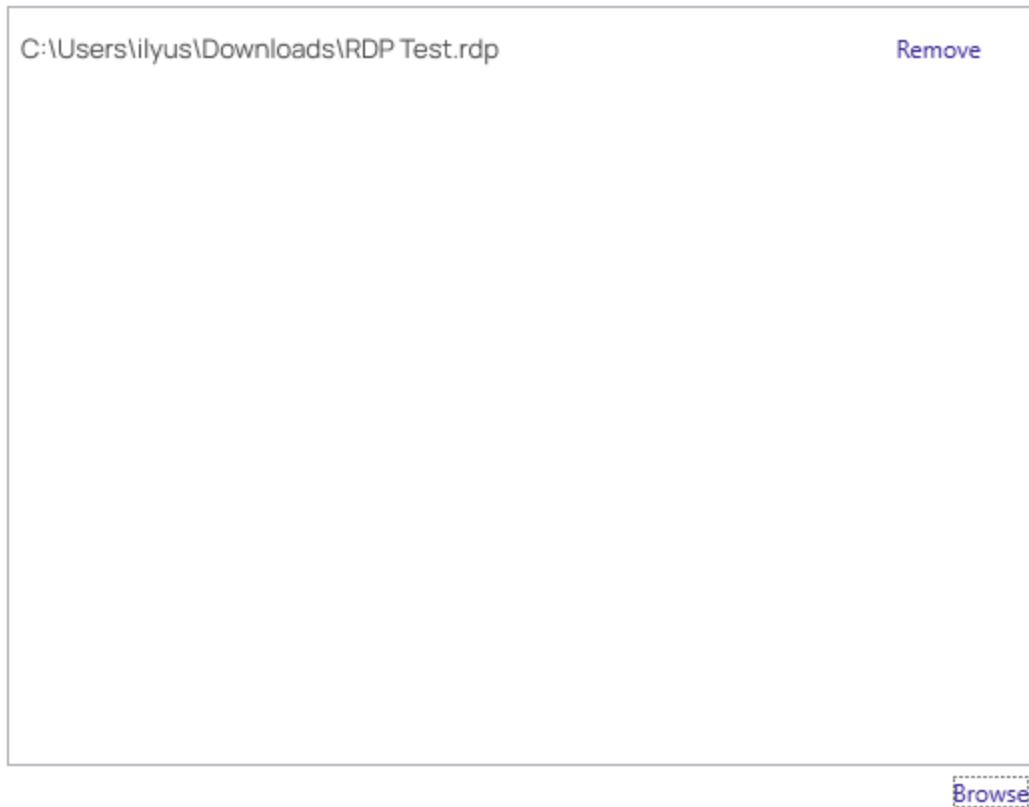
Import RDP files (.rdp)

Select RDP files

C:\Users\ilyus\Downloads\RDP Test.rdp   Remove

Browse

Cancel   Finish

5. A confirmation window will appear that the import was successful.
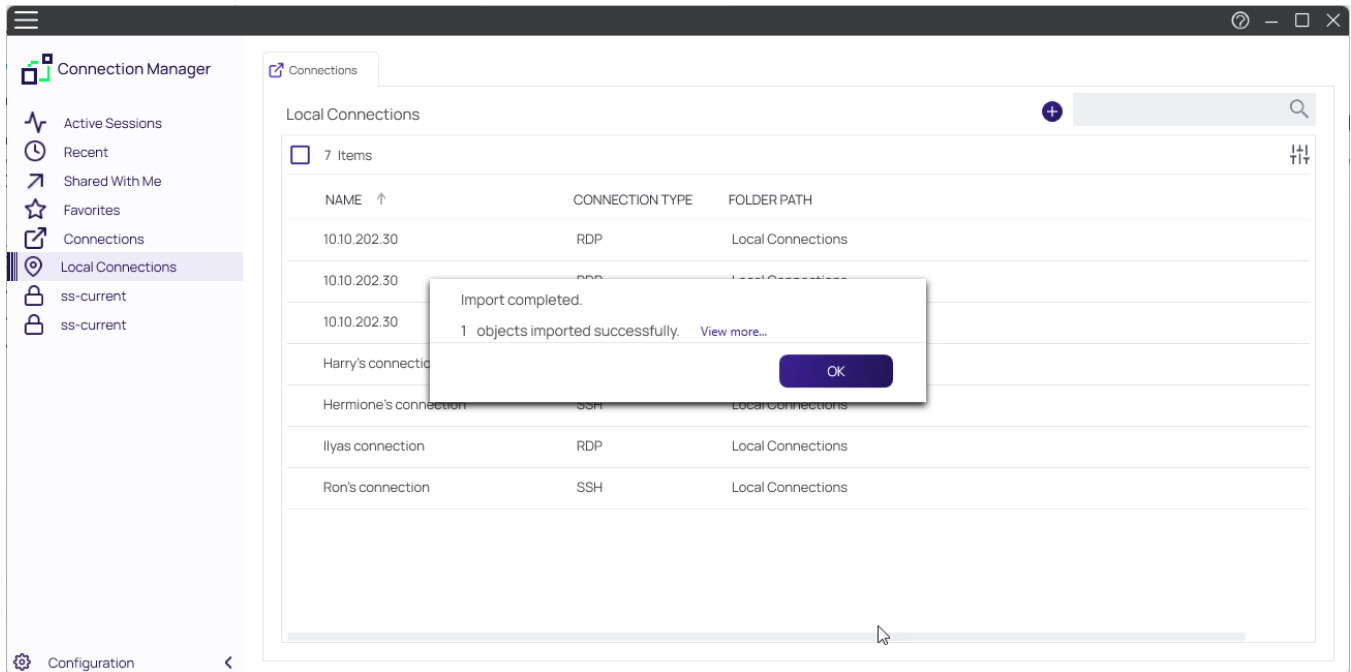
6. Click **OK** to return back to Local Connections.

Import of CSV Files

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

This example is for CSV file imports.

1. Right-click on **Local Connections**.

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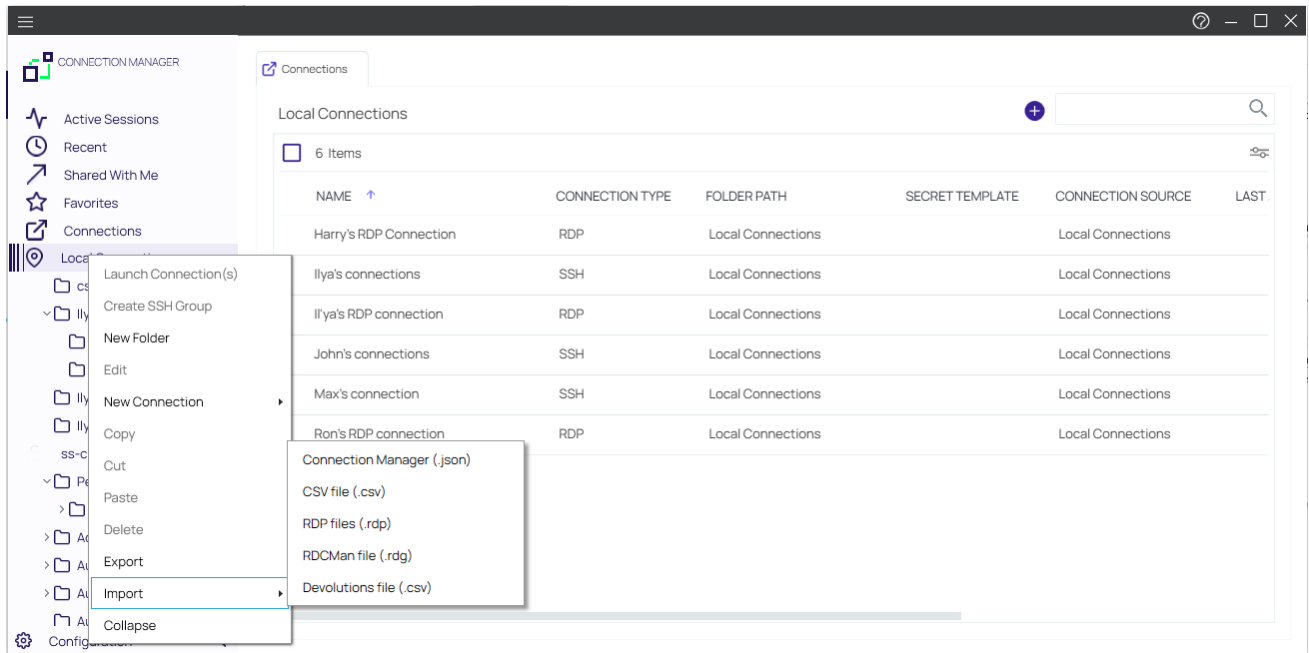
3. Select from the import options available based on your source file.

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,

   a. select the file to import,

   b. specify the connection type, and

   c. select which Delimiters are used in the import file, the default is comma separated.

Import from a CSV file
Step 1 of 2: Please, enter CSV parameters

CSV File*

Browse

Connection Type*   RDP

Delimiters   ⦿ Comma (,)

                    ◯ Tab

                    ◯ Semicolon (;)

Cancel   Next

2. Click **Next**.

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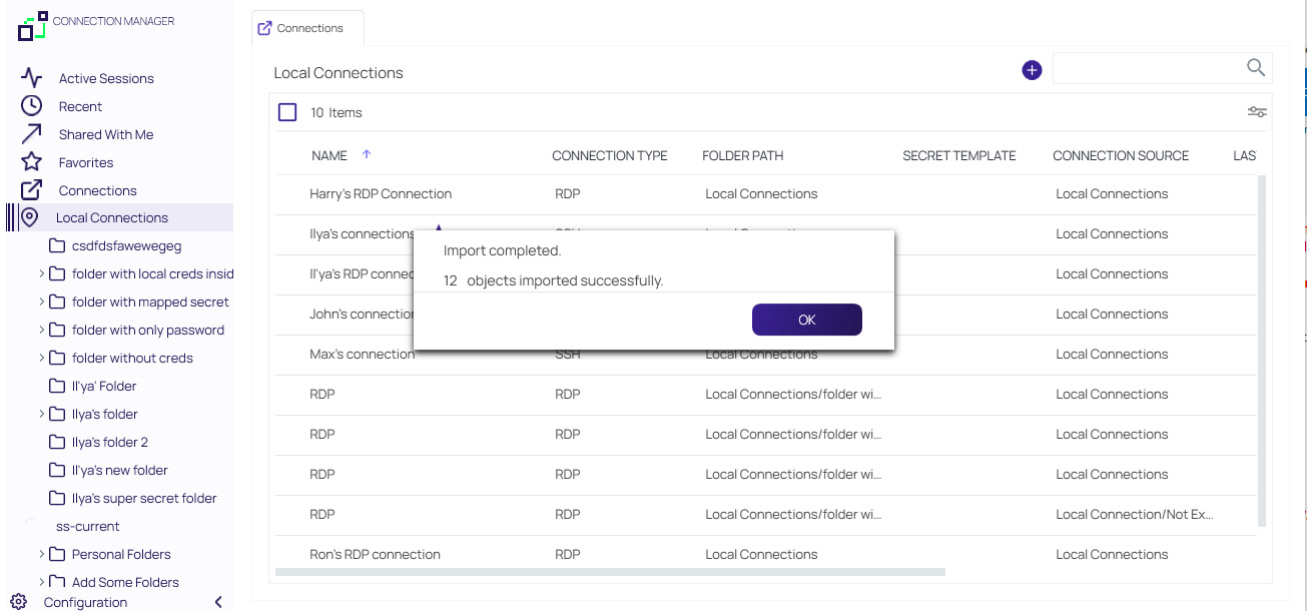
Each connection in the file is imported as a Local Connection. Links to informational or error reports will be displayed, but only if the import encountered errors or if it automatically mapped fields during the import.

4. To further examine which information failed to import, click **View more...**.
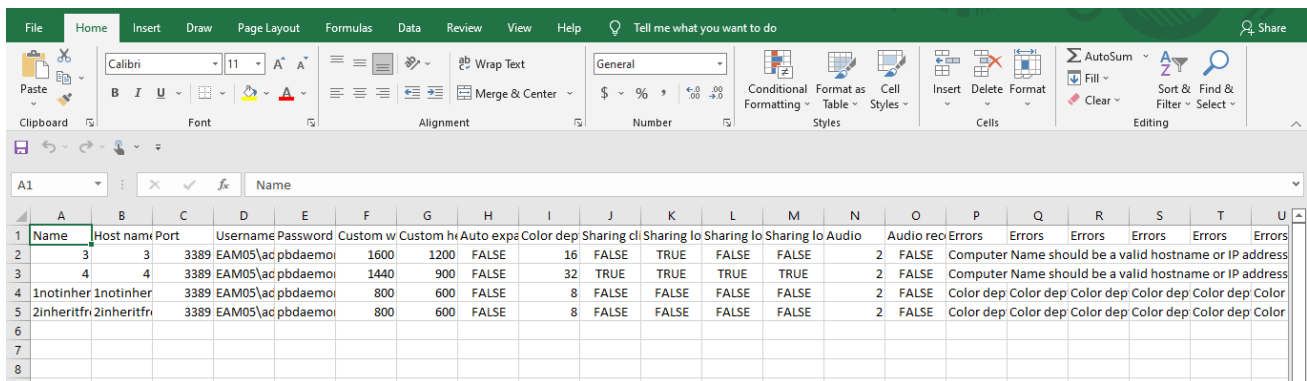
Connection Manager saved the connection data that failed to import in a separate Excel file. The data can be edited and the file can be used to retry the import for the remaining connections.

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

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

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

Desktop Size

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

//4:3 resolutions

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

//16:10 resolutions

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

//16:9 resolutions

- 1024x576

- 1152x648

- 1280x720

- 1366x768

- 1600x900

- 1920x1080

- 2560x1440

- 3840x2160

- 7680x4320

Import Completed Reports

Imports and trigger none, one, or up to two reports.
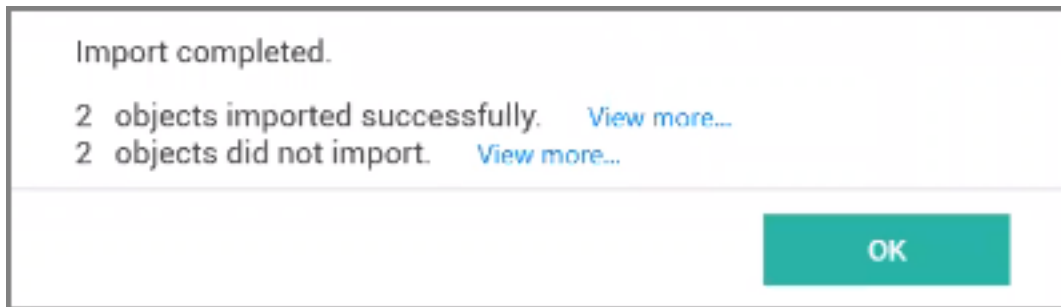
- Successful: This report lists all objects that have been successfully imported.

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

CSV Import Differences

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

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.

Local Data Vault Enabled

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.

Local Data Vault Disabled

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.

Enable or Disable Local Data Vault on Installation or Upgrade

When Connection Manager is installed on a machine for the first time, or when upgrading to version 1.6.0 or higher, the application asks, "How will you use Connection Manager?"
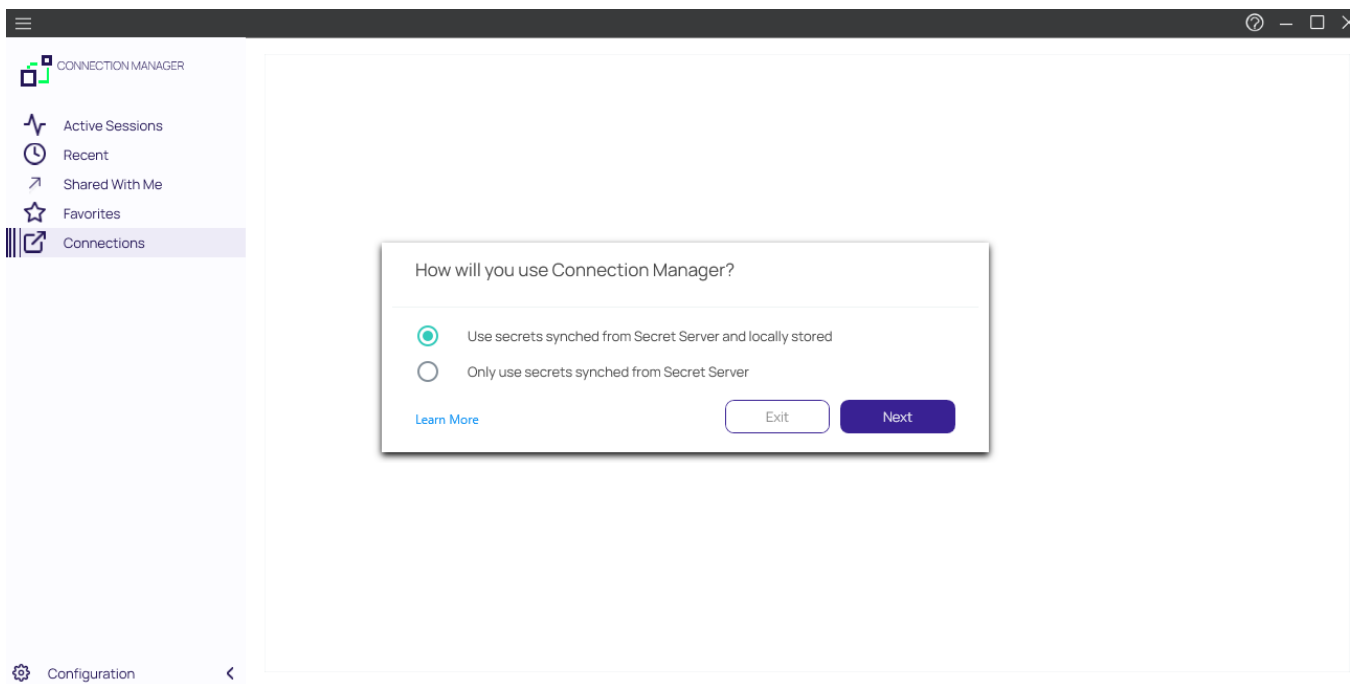
The first choice, **Use secrets synched from Secret Server and locally stored**, enables use of the local data vault.

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

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

Mac

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

Enable or Disable Local Data Vault when Connecting to Secret Server

In the workflow for connecting to Secret Server, the user can check the box next to **Remember me** to store their credentials to a local 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   ☐

Cancel   Connect

Enable or Disable Local Data Vault at Any Time

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

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

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

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

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.

Global Configurations

RDP Global Settings   SSH Global Settings   Preferences   Launcher Settings

Initial Size

Auto   ▼
Auto
Size 640x480
Size 800x600
Size 1024x768
Size 1280x720
Size 1280x800
Size 1280x960
Size 1366x768
Size 1600x900
Size 1680x1050
Size 1920x1080

Auto Resize

Color Depth

Run As Admin

Local Devices

☑ Clipboard   ☐ Smart Cards

Windows Shortcuts | Only when using the full screen   ▼ |

Audio Playback | This Computer   ▼ |

Audio Recording   ☐

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   Unicode (UTF-8) ▾

Font   Courier New ▾

Font Size   8 ▾

Color Presets   Default ▾

Background Color   [black]   Bold Color   [white]

Standard	Advanced

Standard Colors

Foreground Color   Color   [light gray]
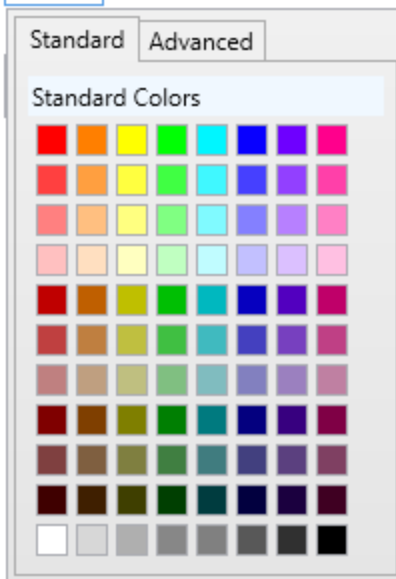
Cancel   Save

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   Connection Manager ▾

Connection Manager

Secret Server Launcher

Cancel   Save

Globally Enforced Secret Server Settings

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

To access this in Secret Server:

1. Navigate to **Admin | See All**.

2. Select **Tools & Integrations**.
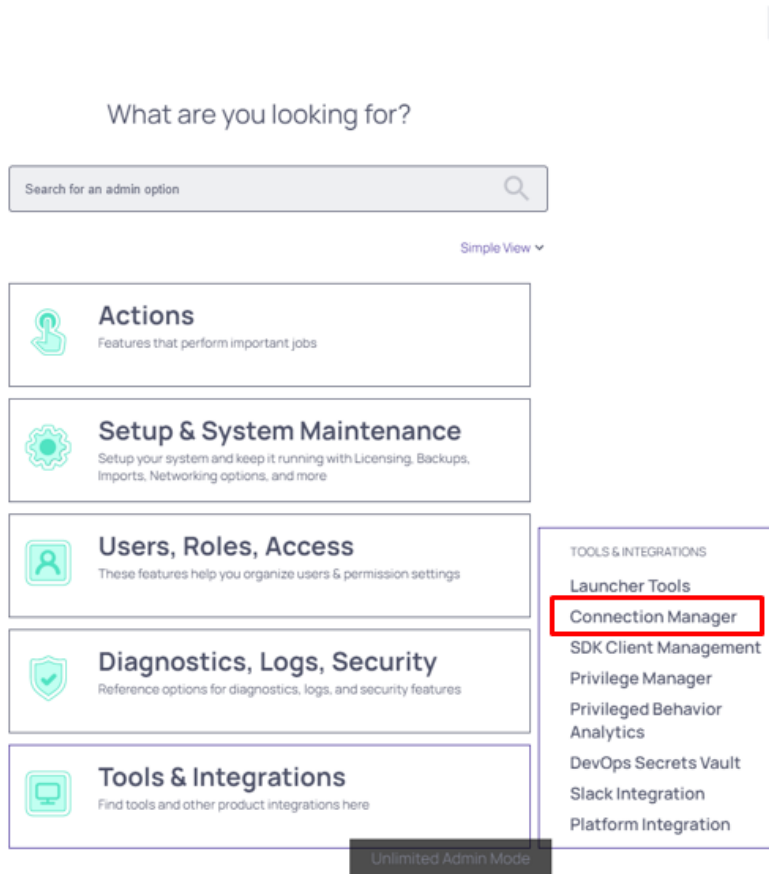
These options are by default enabled:

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

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

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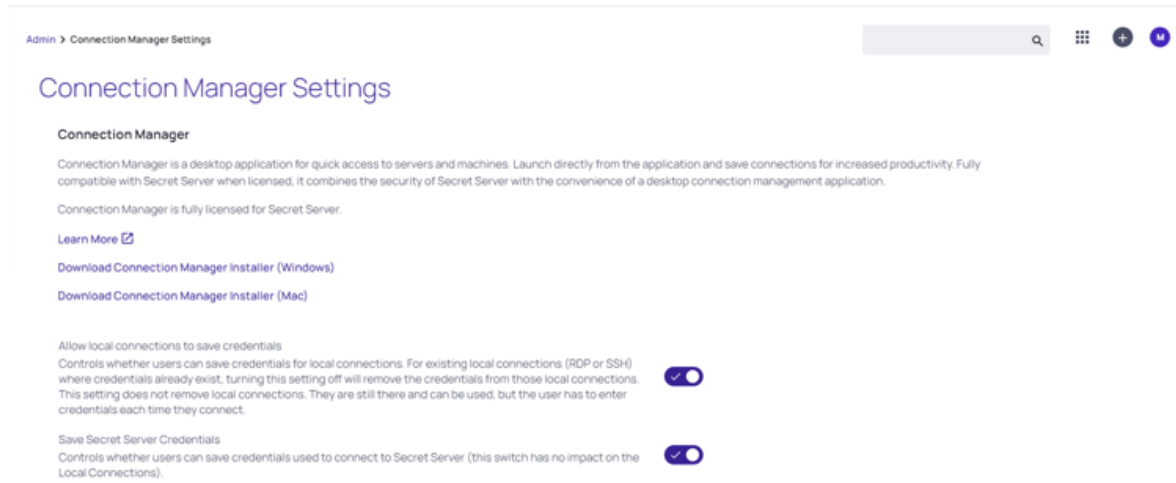
If Connection Manager is connected to multiple Secret Server Instances, and those instances have different values for these new settings, then Connection Manager will always use the more secure option set for security purposes. For example, if Connection1 allows Local Connections, and Connection2 does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

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

Create a Remote Desktop Connection

General   Windows Mode   Local Resources

GENERAL CONNECTION INFORMATION

Connection Name*

Computer Name*

Enter a computer name or IP address

Port*   3389

Credentials*   None

Cancel   Create

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.
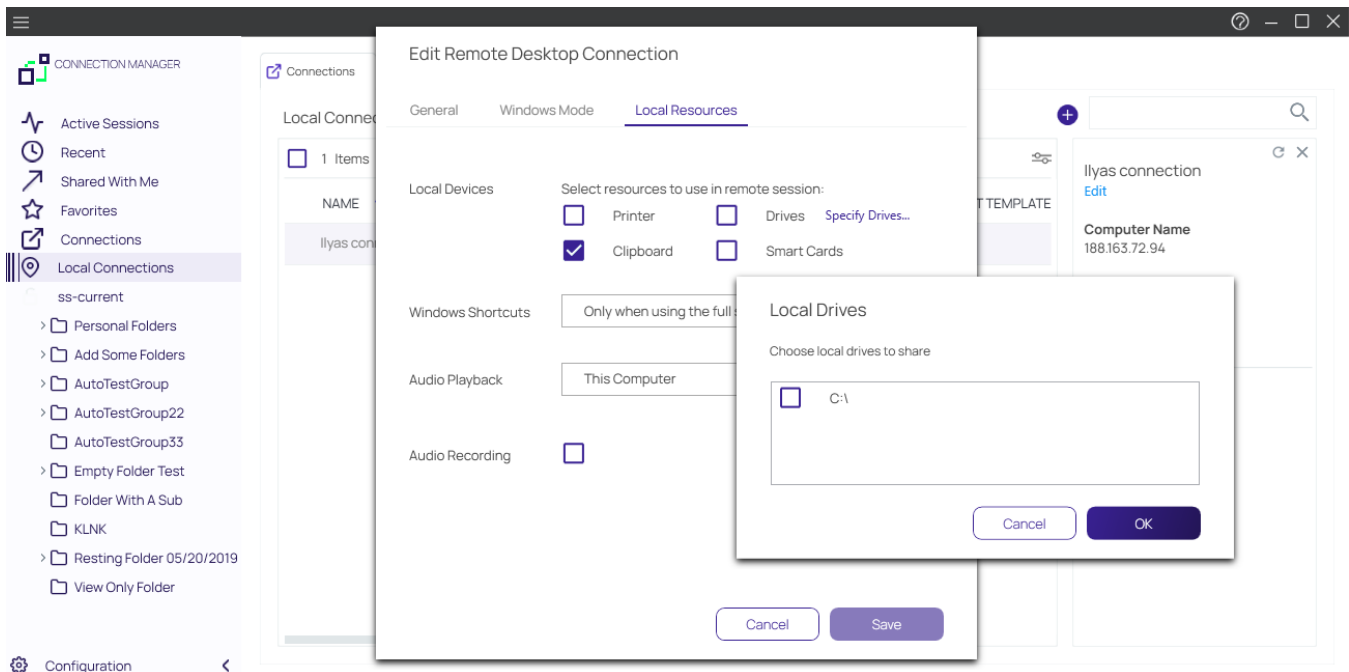
Use a Custom Logo in the Connection Manager Interface

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

Manual Procedure

1. Create two versions of your logo image file in PNG format, with names exactly as specified below:

   - One sized to 250 x 50 pixels, named `logo.png`. This version is the full-sized logo that will appear in the main interface.

   - One sized to 100 x 50 pixels named `logo_collapsed.png`. This version is the collapsed logo that appear when the left navigation panel is collapsed

2. Store both image files in the following location (if you don't have this folder structure already, you'll need to create it): `C:\ProgramData\Delinea\Connection Manager\Resources\`

3. Assign all users permissions to read, execute, and list folder content from this location.

4. Restart Connection Manager

Command Line Procedure

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

```
Delinea.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 of deny approval URL and the system will automatically remember this selection for future use.
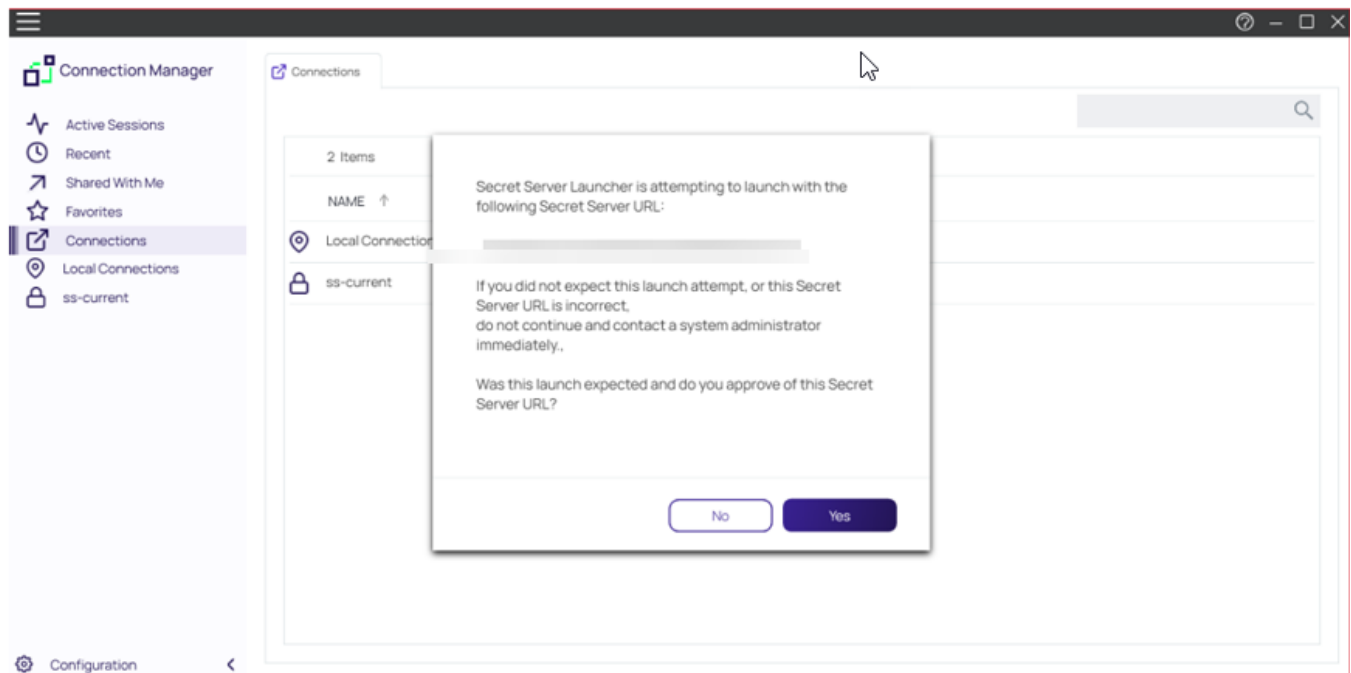
Connection Managerwill not run secret from denied SS URLs. If the user denied the SS url by mistake, and wants to fix this issue, they should delete the ApprovedSsUrlStorage.dat file located in the application's data folder (reload application).

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

Initial Size

Auto ▼

Auto

Auto Resize   Size 640x480

Size 800x600

Color Depth   Size 1024x768

Size 1280x720

Size 1280x800

Run As Admin   Size 1280x960

Size 1366x768

Local Devices   Size 1600x900

Size 1680x1050

Size 1920x1080

☑ Clipboard ☐ Smart Cards

Windows Shortcuts

Only when using the full screen ▼

Audio Playback

This Computer ▼

Audio Recording ☐

Cancel Save

Global Configurations

RDP Global Settings   SSH Global Settings   Preferences   Launcher Settings

Initial Size   Auto

Auto Resize   ☑

Color Depth   True Color (24 bit)

Run As Admin   ☐

Local Devices   Select resources to use in remote session:
                        ☐   Printer   ☐   Drives   Specify Drives...
                        ☑   Clipboard   ☐   Smart Cards

Windows Shortcuts   Only when using the full screen

Audio Playback   This Computer

Audio Recording   ☐

Cancel   Save

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

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

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

Launchers

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

Note: ActiveX components will not be recorded.

Launchers
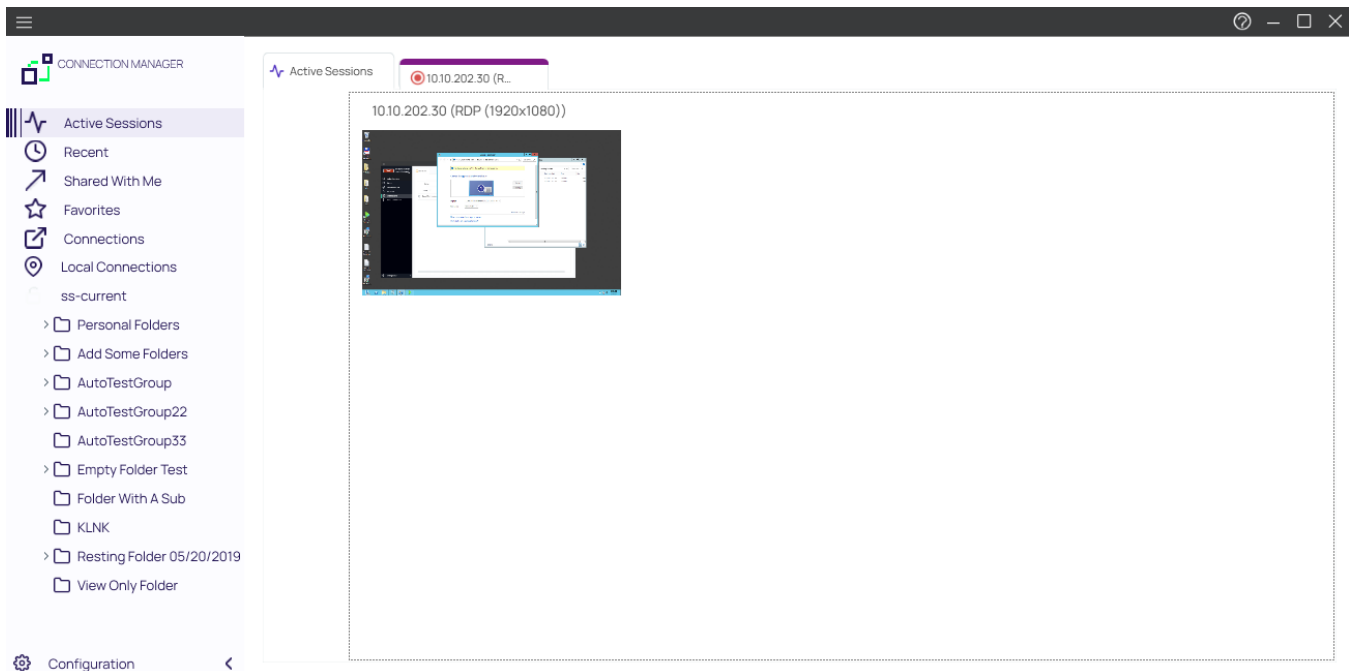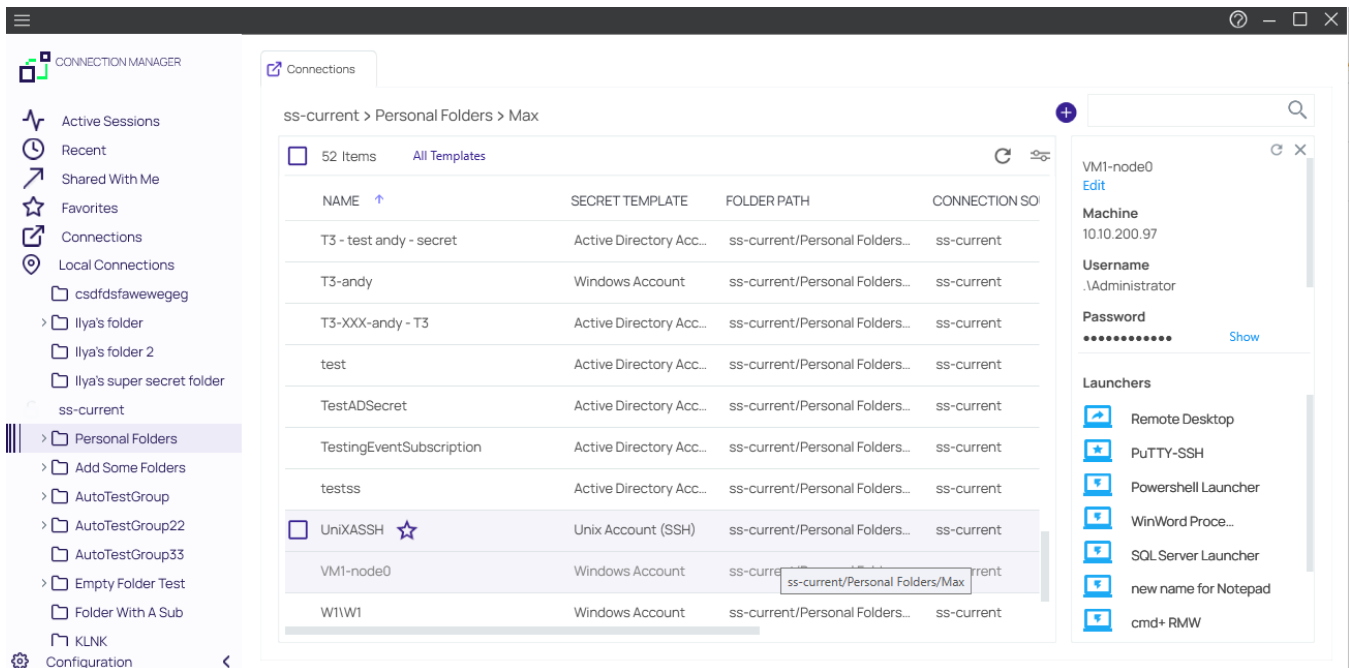
The Secrets with launcher can be launched in the Secret Server UI and have the protocol handler open and run the launcher in Connection Manager. The Secret needs to be configured to use the protocol handler, and when launched it uses Connection Manager if available. When Connection Manager opens, it 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.

Proxy Tabs Show Remote Host Name

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

Screen Resolution for New Session Window Views

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

Moving and Reorganizing Session Tabs and Windows

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

To redock a session window, click and drag it toward the row of docked tabs in the main Connection Manager window. As you drag the window close to the tab dock, a blue line appears around the dock:
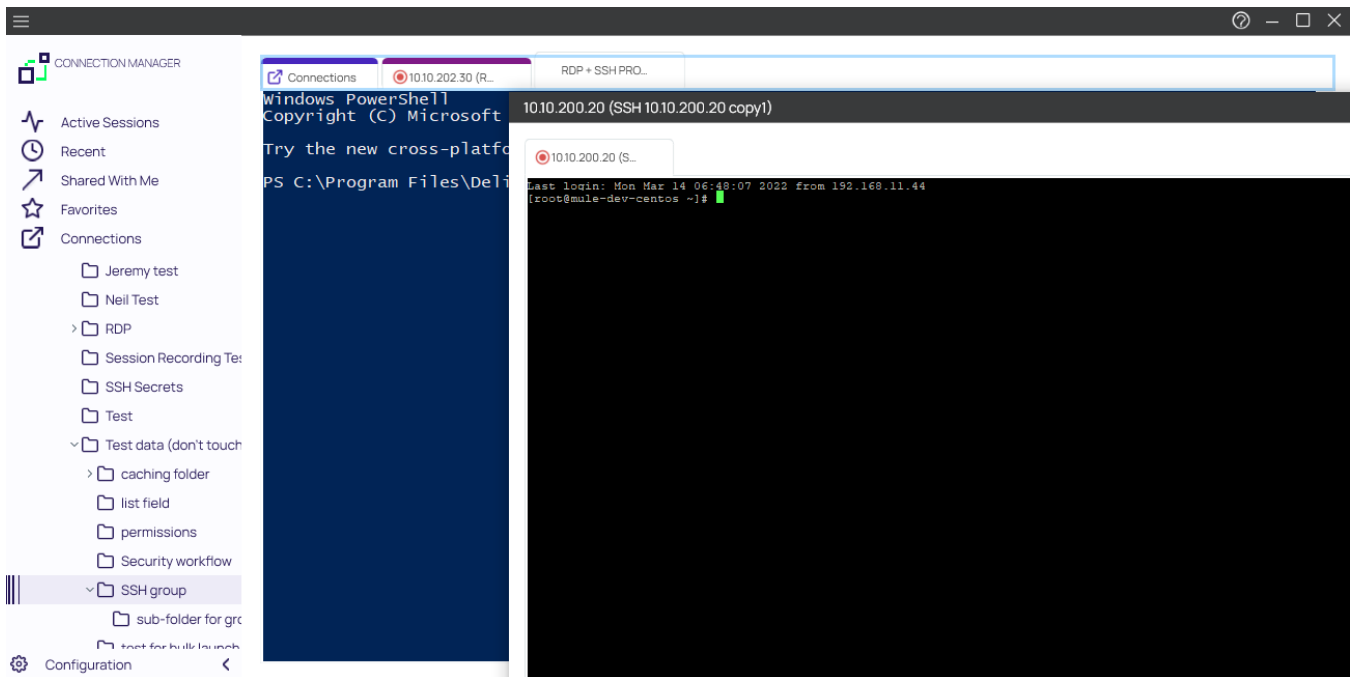
When you drag the window onto the tab dock, the dock turns light blue to indicate that you can drop the window:
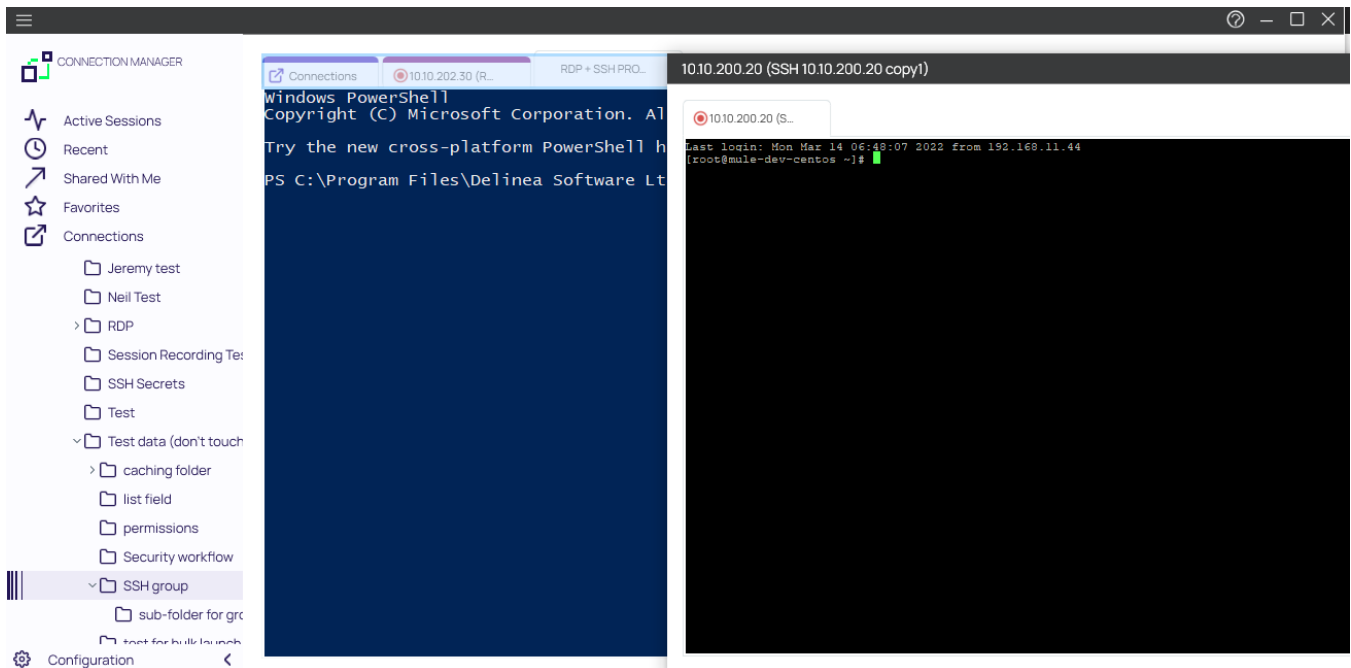
Session Recording

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

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.

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

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

Launching from Secret Server without Connection Manager Open

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

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

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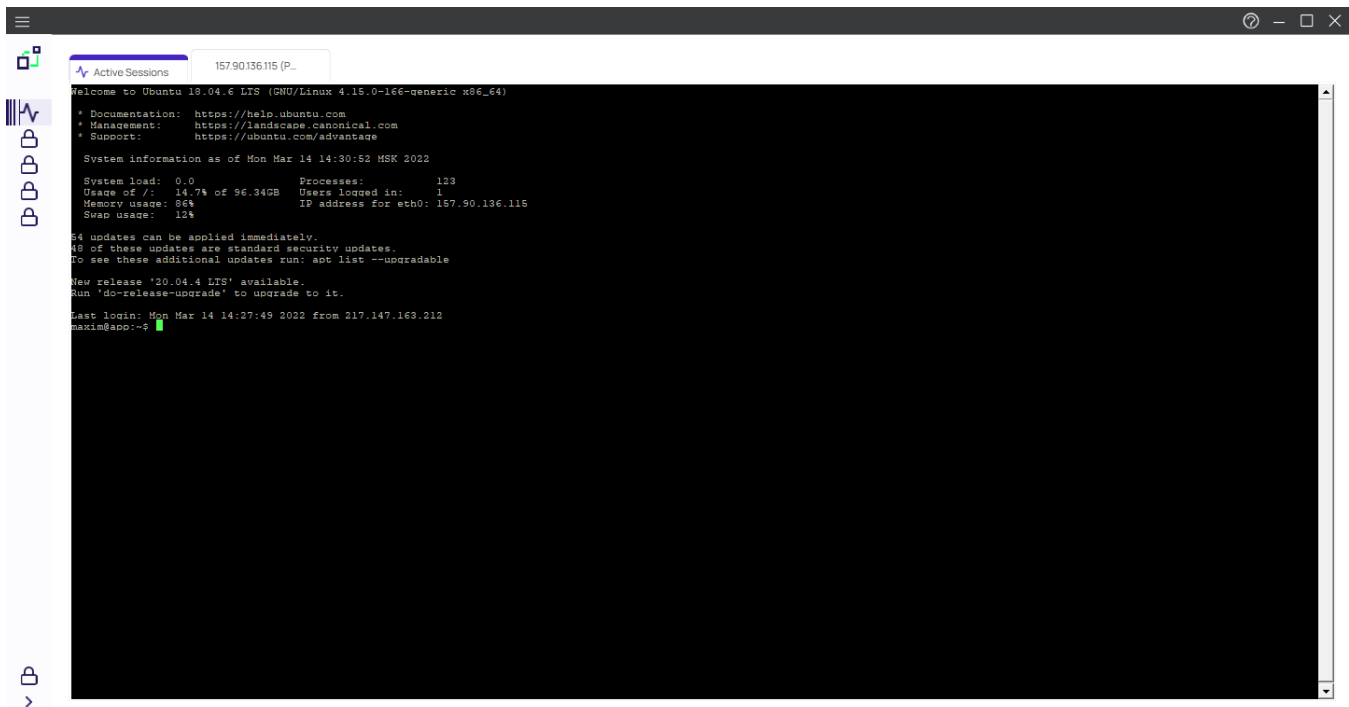
In this example the application was opened and placed inside the new tab. Certain applications won't fit in the tab and will be opened in an independent window outside the tab. Other windows opened by the user won't be placed inside the tab either, but everything that originated from the originally launched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

For applications launched from within a Secret Server, the other configured local and existing Secret Server connections remain locked in Connection Manager.
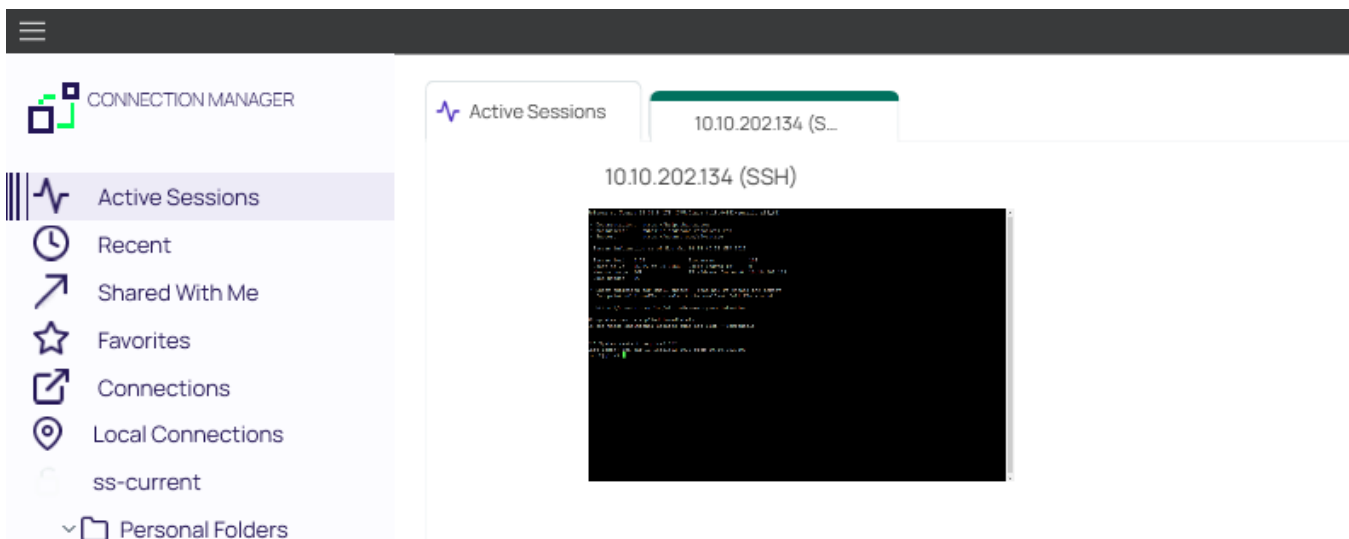
Only navigation between different Active Session tabs initiated from Secret Server is possible.

Signing In After the Launch

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

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

Sign In

Enter your password to access the local storage file.

Password

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

Cancel   Sign In
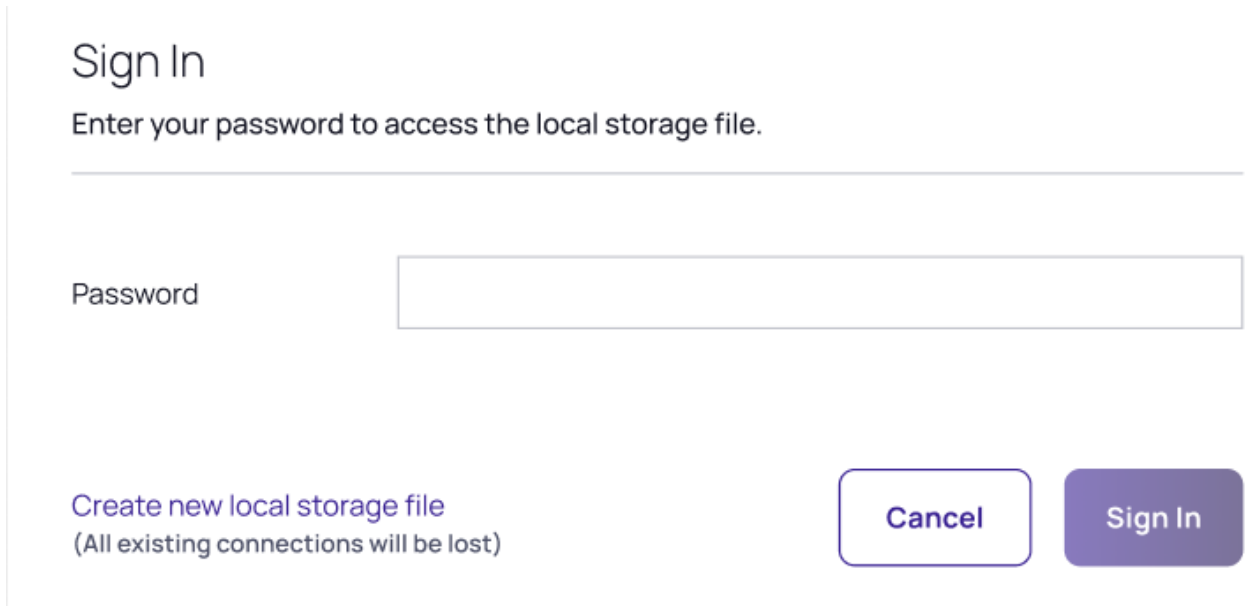
2. Enter your password.

3. Click **Sign In**.

Once signed in, the user has access to all connections and all Connection Manager functionality is unlocked.
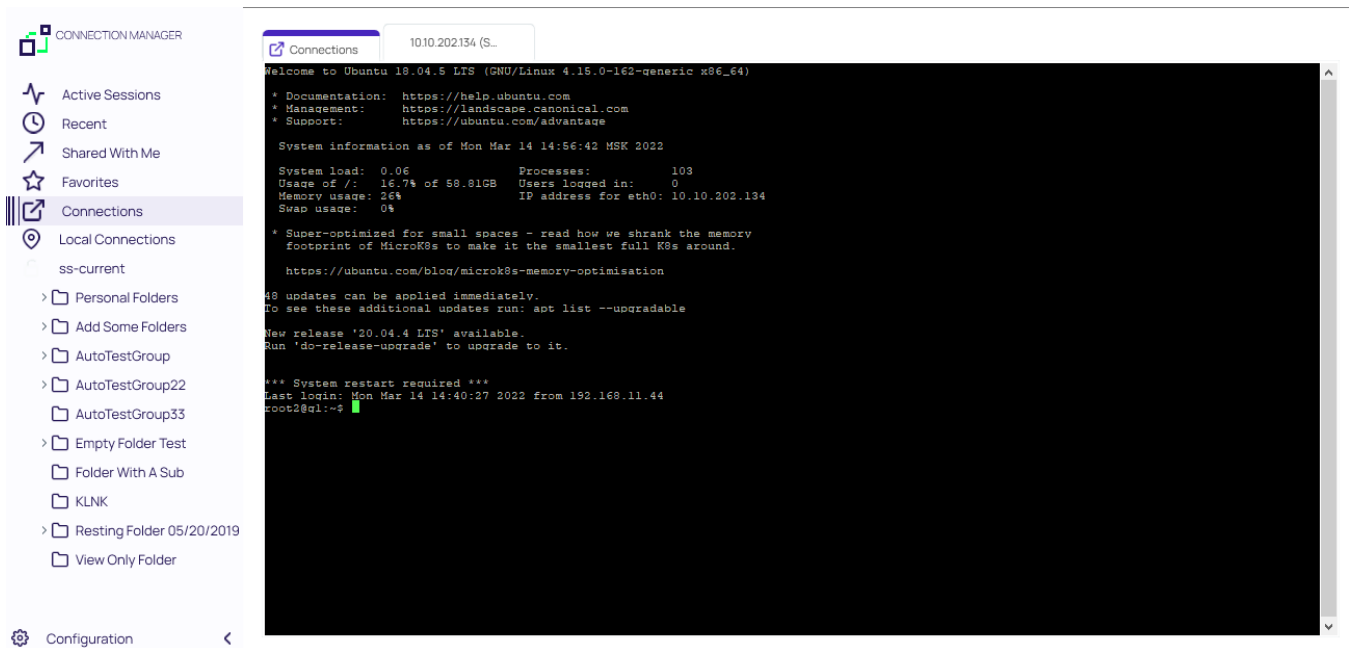
Create a New Local Storage File

During the sign in, users can select to create a new local storage file by clicking the link in the sign in modal:
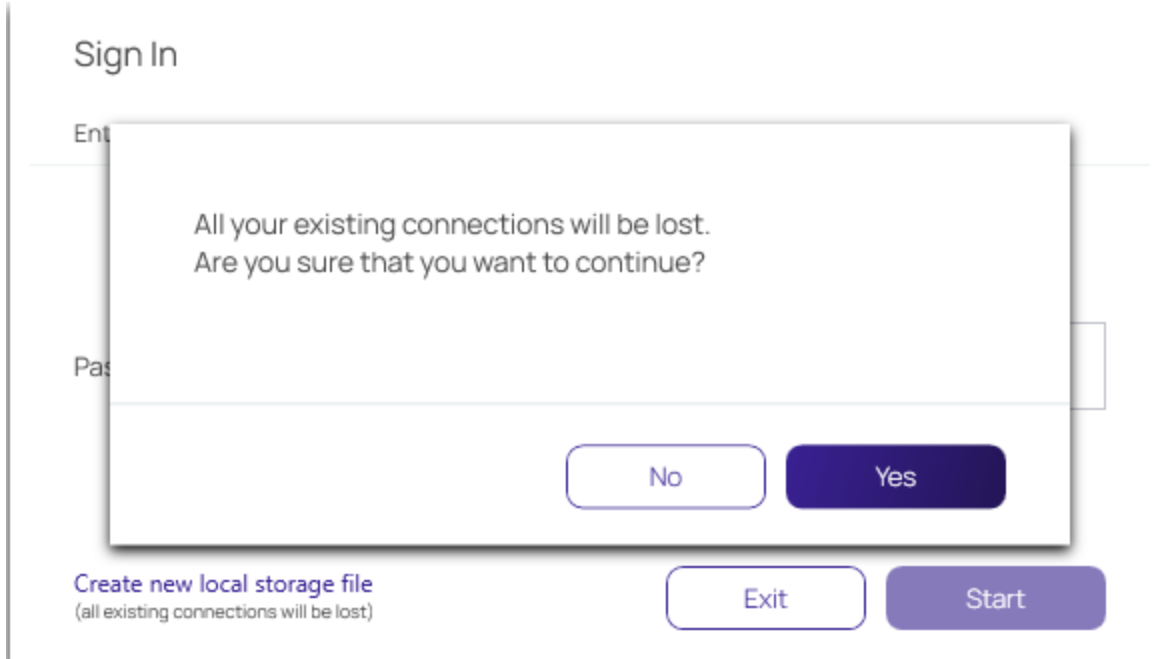
Note: If this option is used, existing connections will be lost.

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

Connections

The following Connections related topics are available:

- Re-authenticate
- Remote connections
- Integrated connections

Re-authenticate

> **Note:** When 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**.
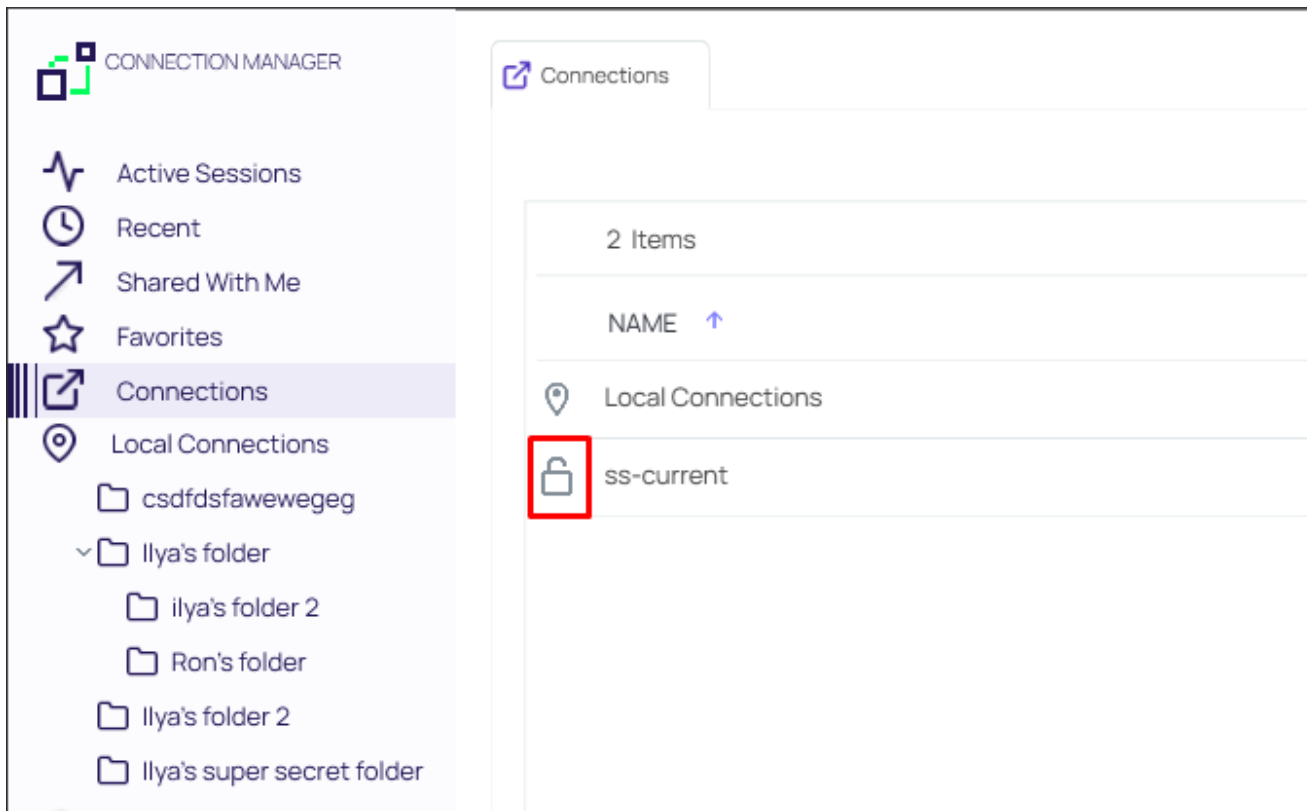
If you lose your internet connection to Secret Server, Connection Manager makes multiple attempts to automatically reconnect and re-authenticate to Secret Server in the background. After 30 seconds, Connection Manager displays the dialog, **Attempting to Auto-reconnect to [Secret Server name]** for three 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.
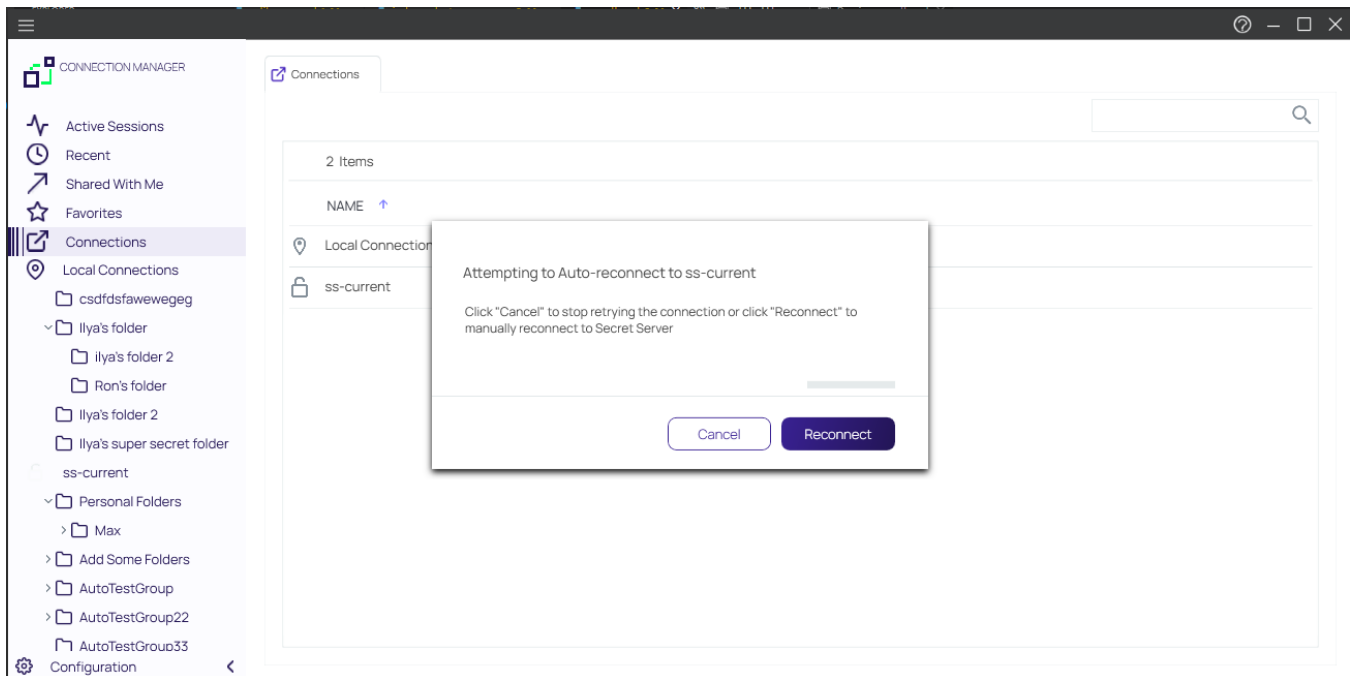
Create a New Connection to Remote Systems

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.

Common User Activities
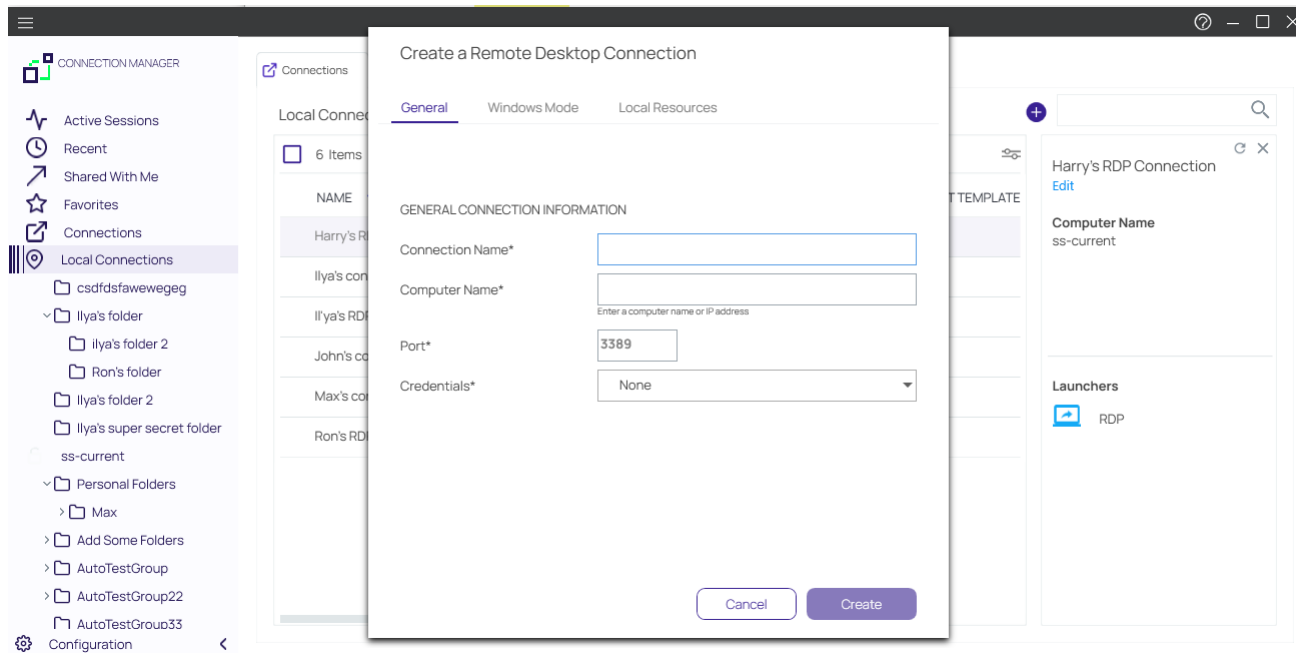
SSH Connection

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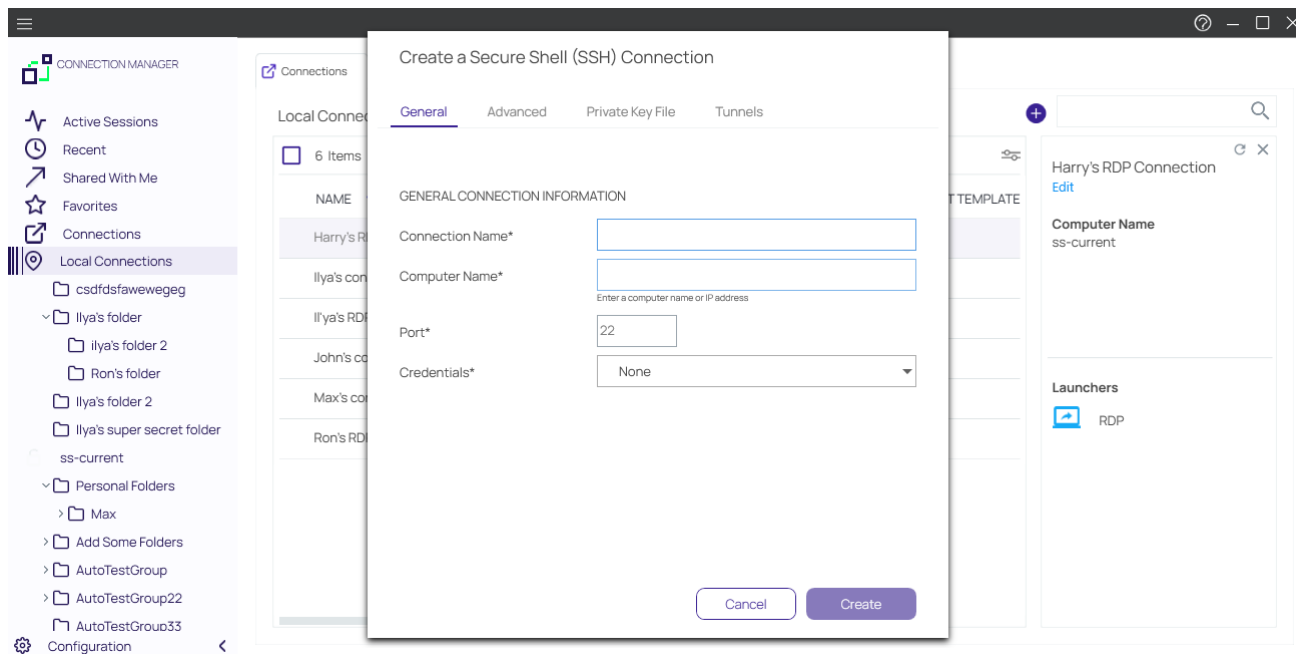
> **Note:** The default value settings may be modified under the Configuration option.

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

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

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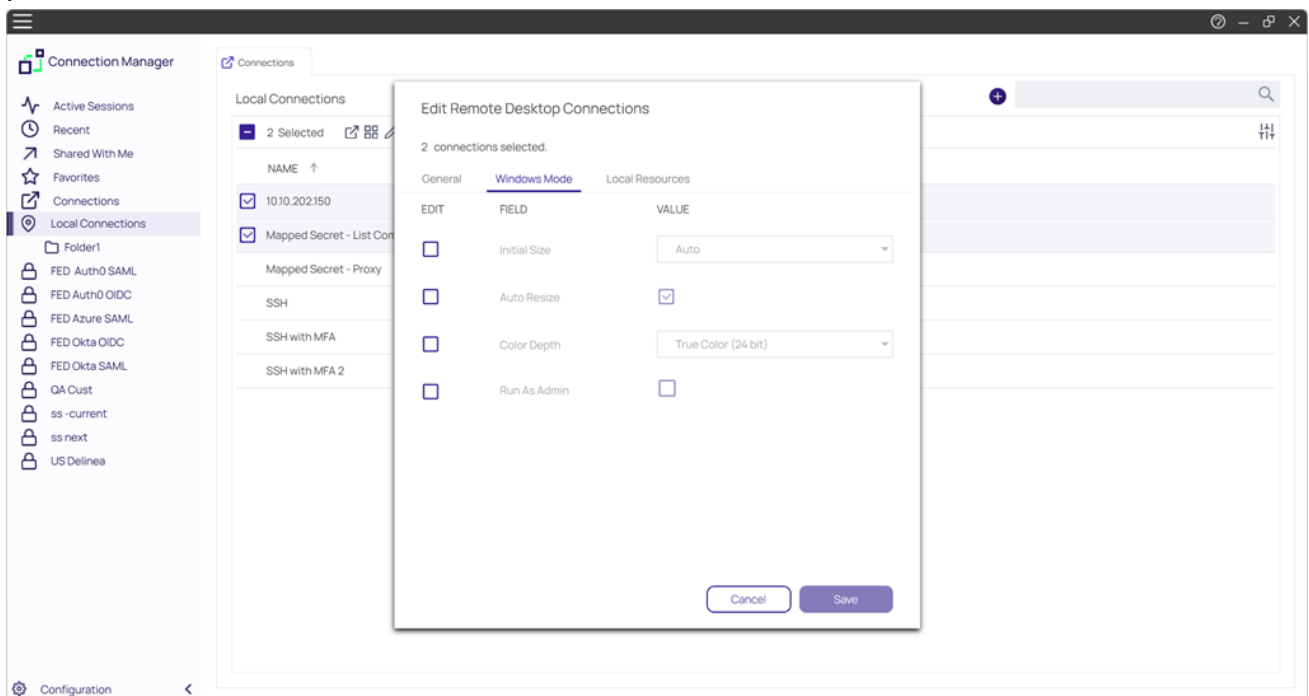
2. In the toolbar click the **Edit** icon.
3. Edit the settings you wish to apply to all of your selected connections and click **Save**.

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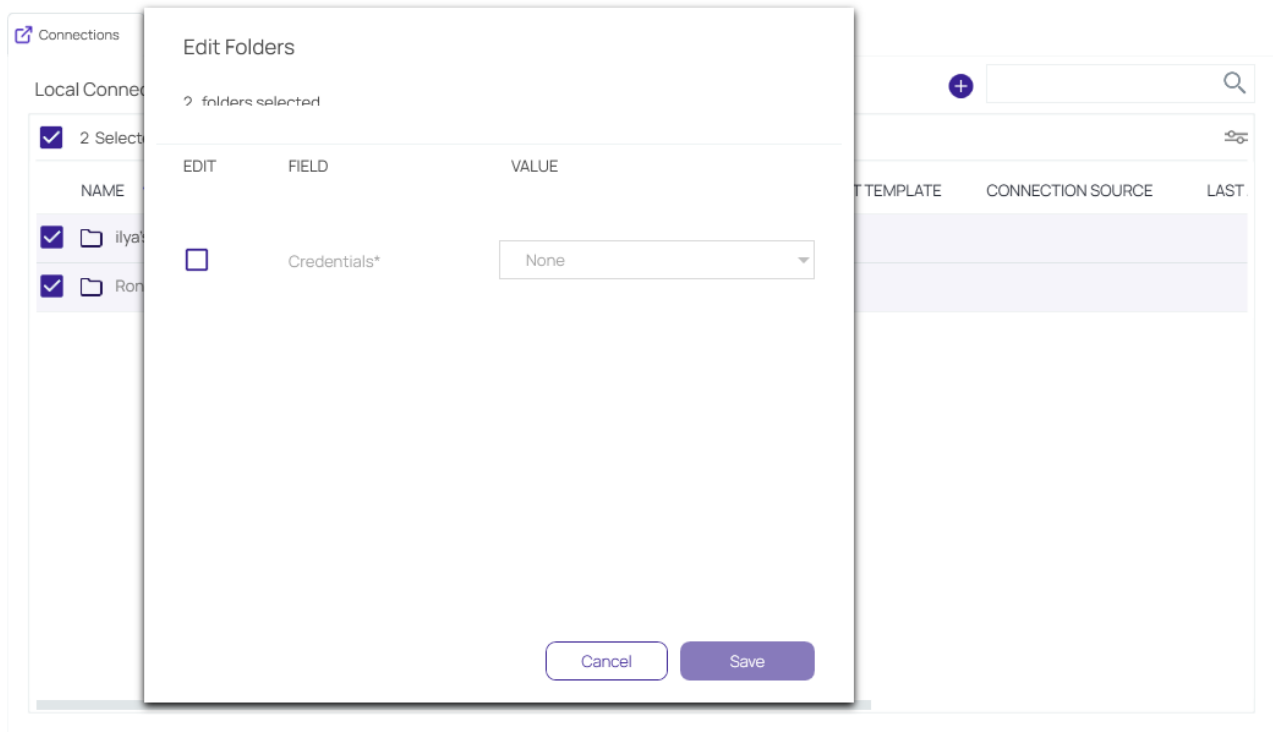
2. In the toolbar click the **Edit** icon.
3. Edit the Credentials you wish to apply to all connections in your selected folder or folders and click **Save**.

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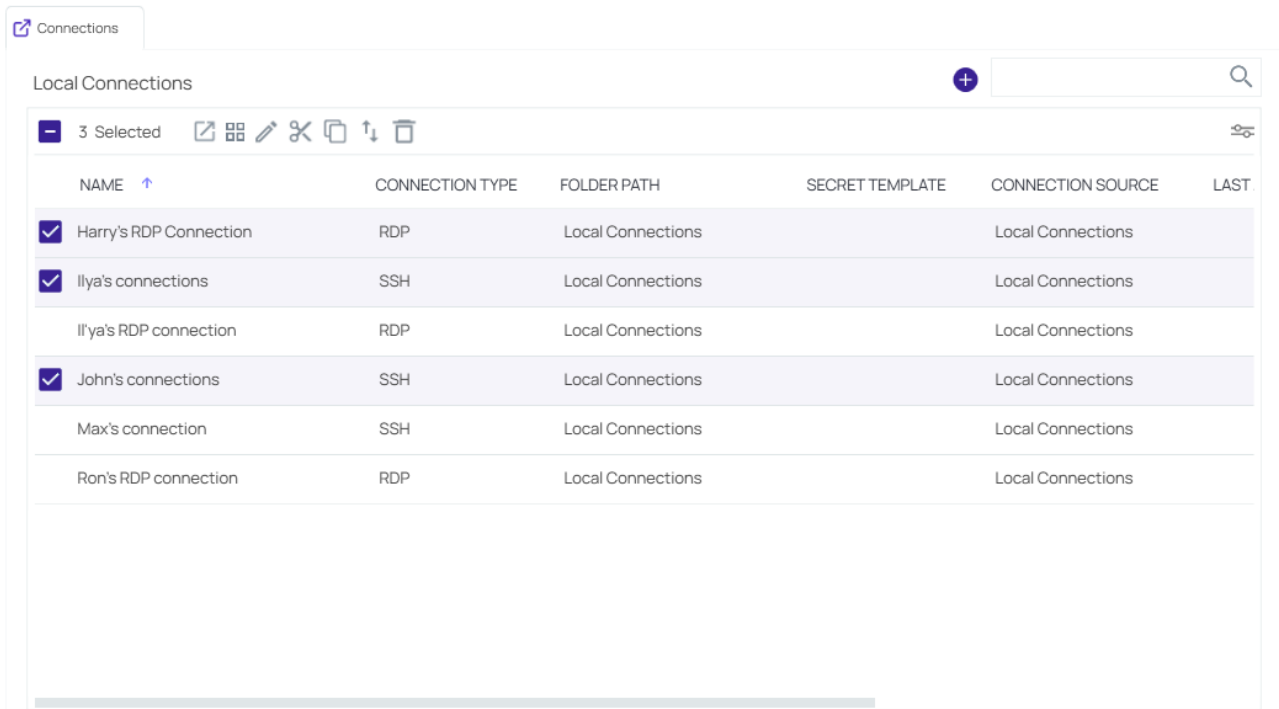
2. In the toolbar click the **Connect** icon.

Batch Open All Connections in a Folder

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

Common User Activities

1. Click to check the box before the folder whose connections you wish to batch open.
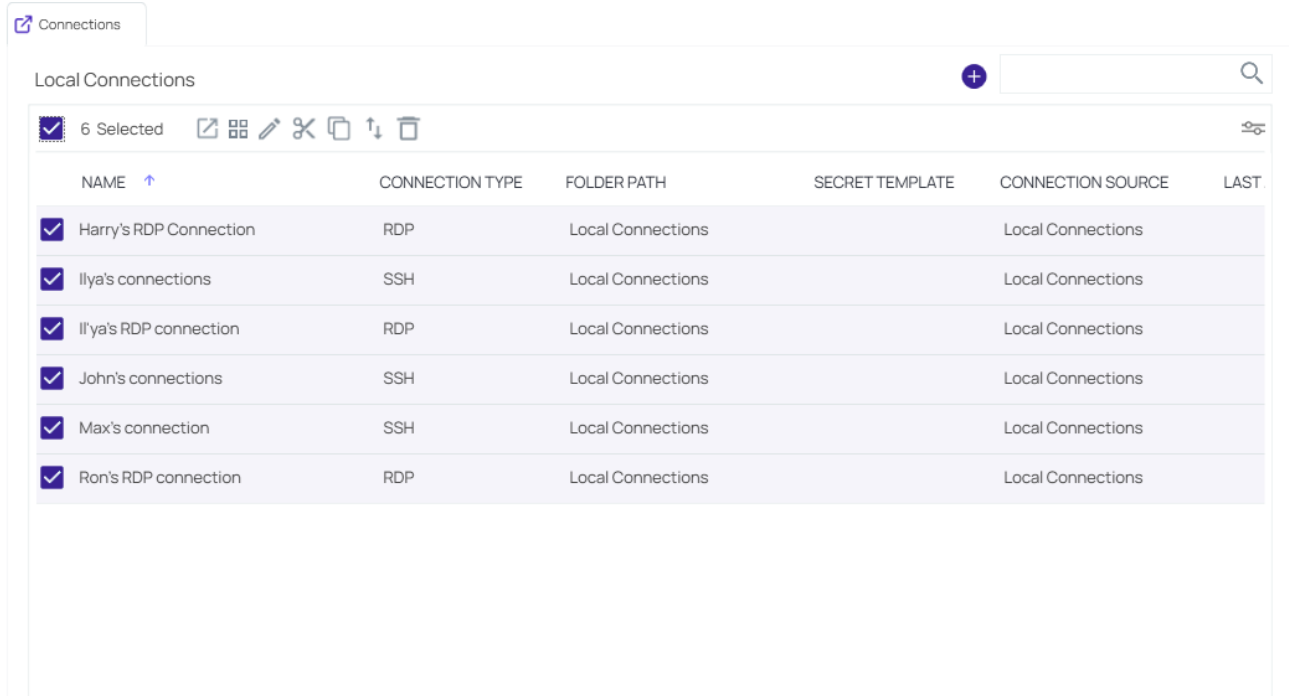
2. In the toolbar click the **Connect** icon.

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.
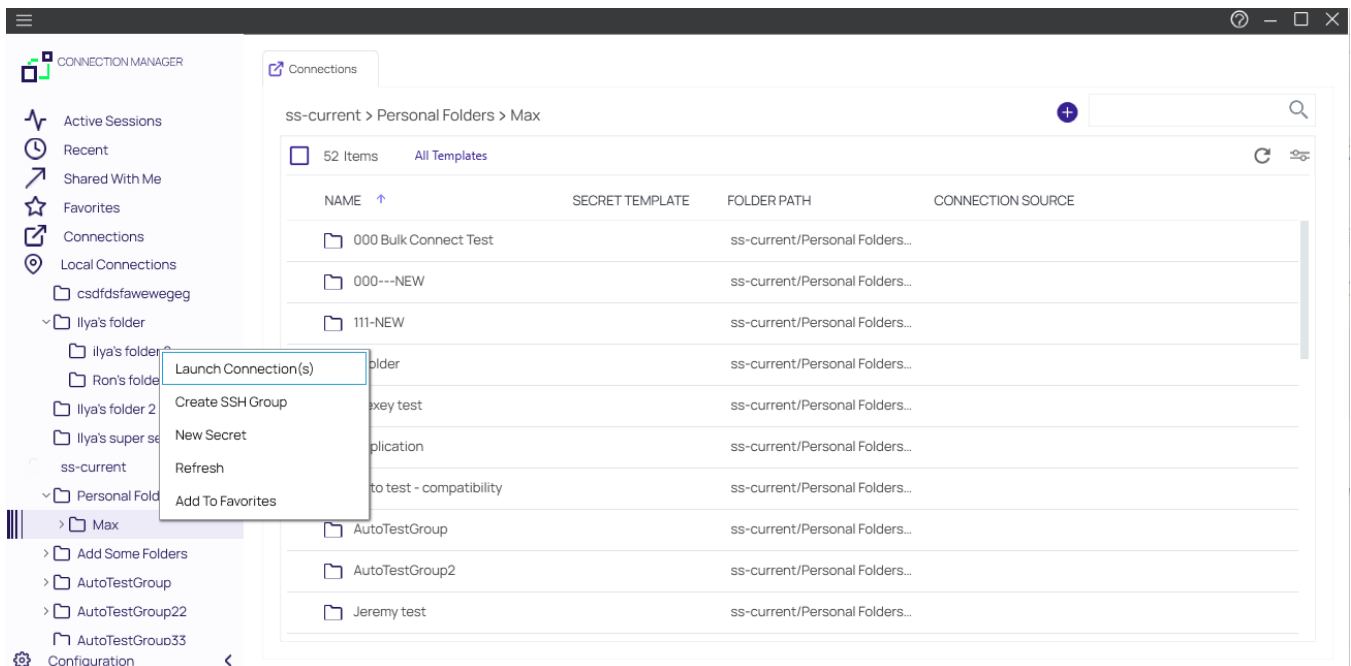
Delete Connections from Remote Systems

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.
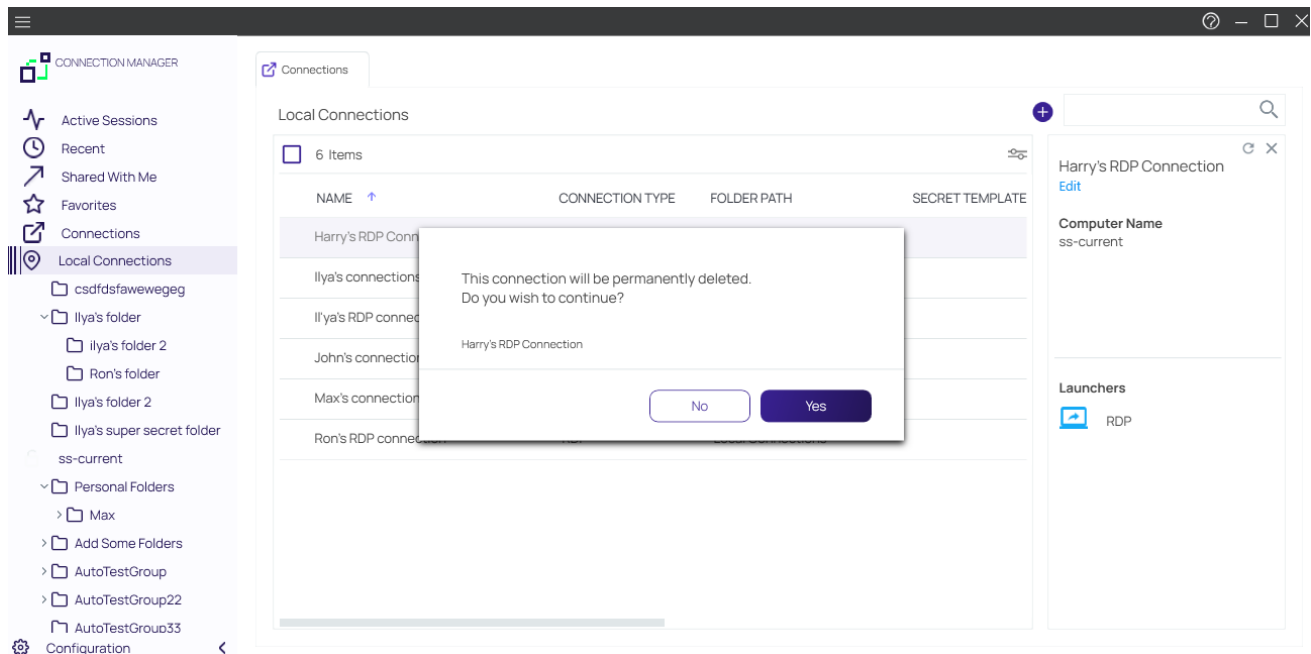
"Confirm connection delete")

3. Click **Yes** to confirm.

Map a Secret to a Connection

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

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

1. From within Connection Manager, "Create a New Connection to Remote Systems" on page 95or "Edit Connections to Remote Systems" on page 103. 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
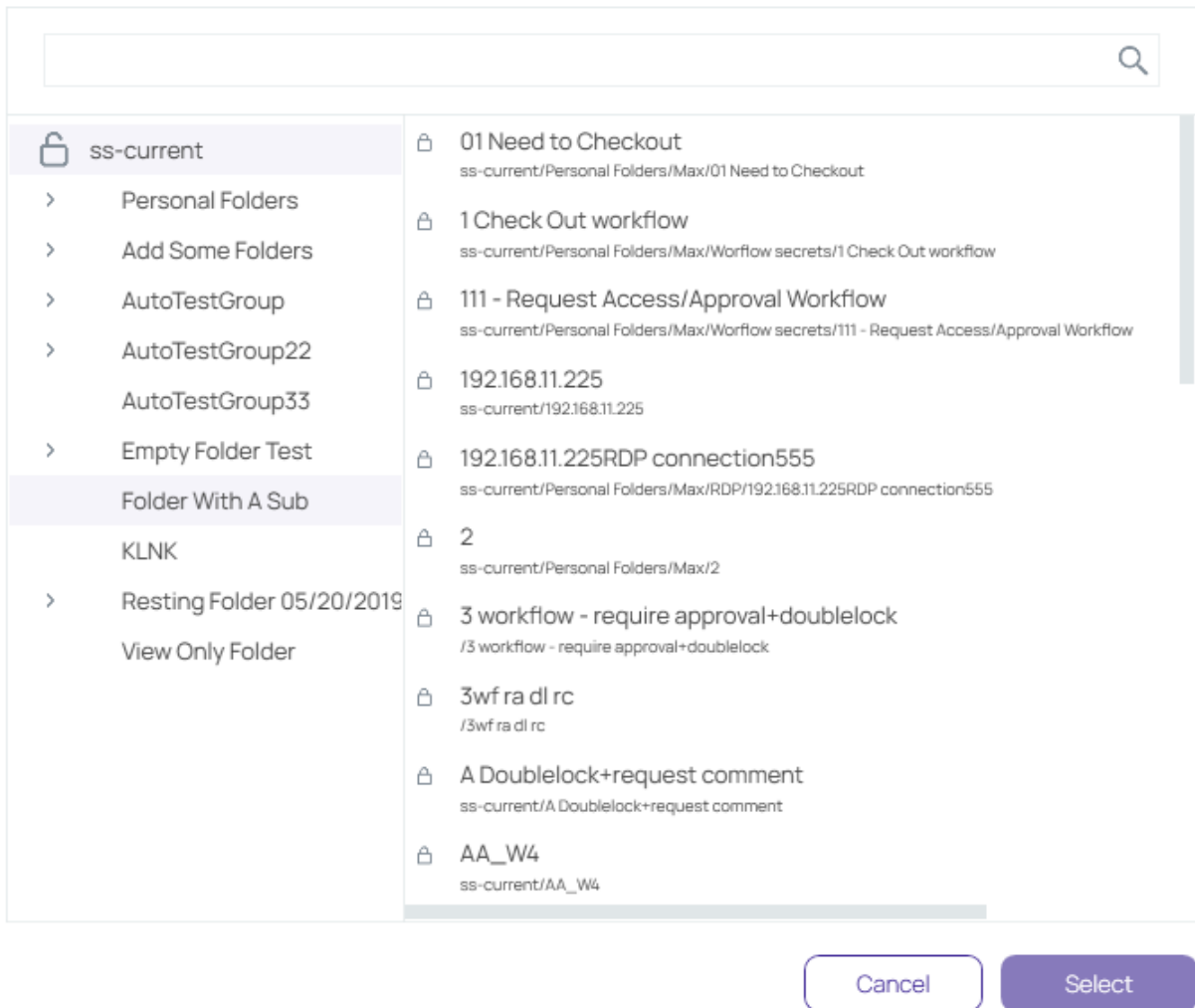
The Select Secret dialog box shows the currently existing connections. Those that are authenticated and accessible, are shown with an open lock next to the name. A closed lock indicated authentication is required, generally a username and password. Users can drill-down the navigation tree to access more 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.

3. Click the **Secret** to which you would like to map and click **Select**.

4. Click **Save.**

5. Your secret is now mapped to a connection.

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.

Edit Connections to Remote Systems

1. Navigate to the connection to be edited and click the connection name.
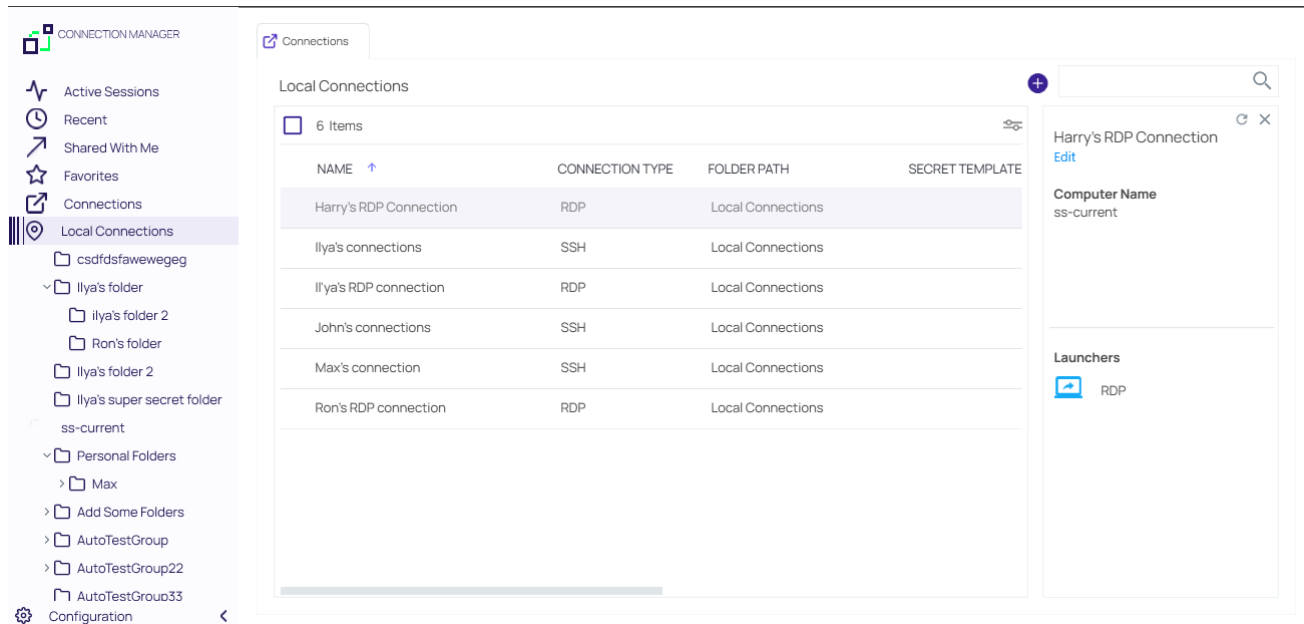
2. In the Connection properties area under the connection name, click **Edit**. An Edit dialog will open depending on the connection type.

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

4. Click **Save** when finished.

Open a Remote Connection

The process of connecting to a Local connection or to a Secret from Secret Server is essentially the same.
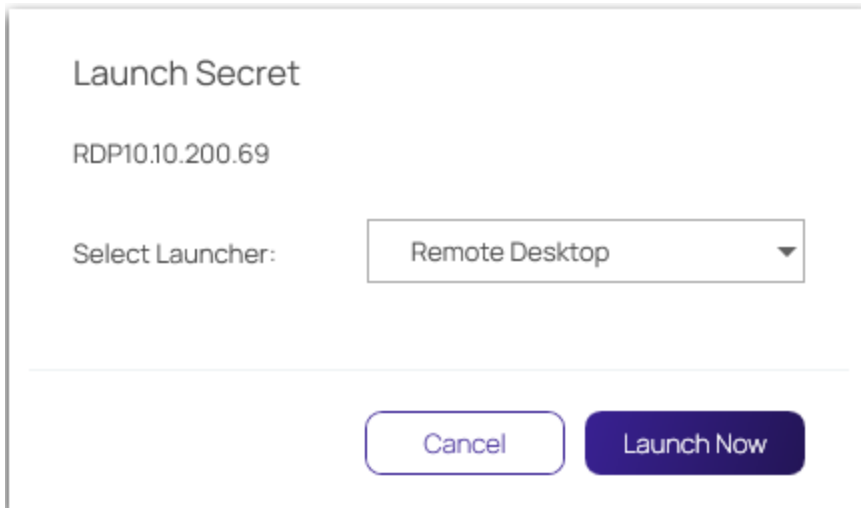
1. Navigate to the remote connection. The remote session can be opened two ways:

   ▪ 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 .

Launch Secret

Host: *

Cancel   Connect

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**.

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/Il'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.

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

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

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

CONNECTION CREDENTIALS

User Name

Password

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

Configuration File

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

Windows Configuration File Location

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

macOS Configuration File Location

/Users/<yourusername>/Library/Preferences/com.Delinea.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>
    <Delinea.ConnectionManager.Wpf.Properties.Settings>
      <setting name="UpdateOnStartup" serializeAs="String" >
        <value>false</value>
      </setting>
    </Delinea.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.Delinea.ConnectionManager Env.CheckUpdateOnStartup -bool false
```

Folder: Create, Edit, Move, Delete

Create a New Folder

Connection Manager uses folders to help organize local connections.

1. Navigate to the location where a new folder should be created.

2. Right-click and select **New Folder**.

3. Enter the **Folder Name** and click **Create**.

4. Choose the appropriate **credential option** from the list:

   - **None**: No credential values will be set or required for the new folder.

   - **Local Credentials**: Allows a user to create the credentials for the new folder.

   - **Inherit from Folder**: Allows a user to set credentials for a sub-folder to imitate the folder in which it will reside.

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

View Integrated Connections for additional information on credentials.

Edit a Folder

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*   Ilya's folder

                       Parent Folder: Local Connections

Credentials*   None   ▼

                                         Cancel   Save

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

View the Integrated Connections section for additional information on credentials.

Move a Folder

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

Delete a Folder

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

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

1. Navigate to the folder to be deleted.

2. Right-click the **folder name** and select **Delete**. A confirmation modal opens.

> This folder and its contents will permanently delete.
> Are you sure that you wish to continue?
>
> Local Connections/Ilya's folder
>
> [No]   [Yes]
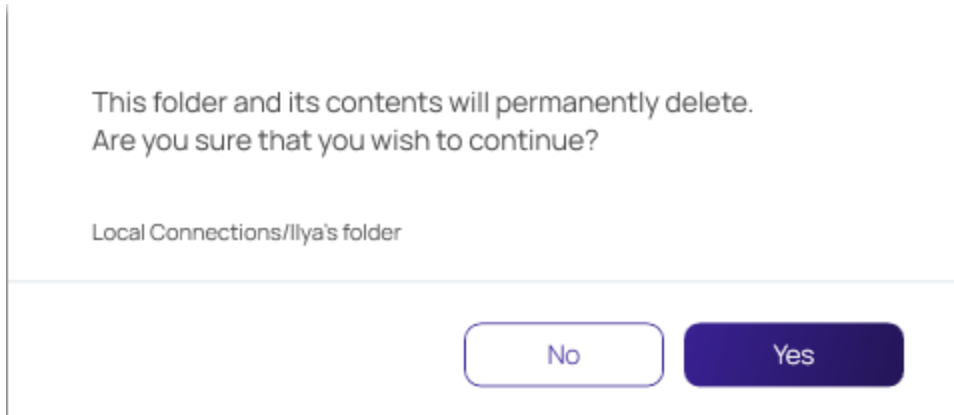
3. Select **Yes** to confirm.

Log Files

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

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>
```

Windows Log File Location

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

MacOS Log File Location

`~/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.

Creating and Naming an SSH Group

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

1. Select the sessions you want to include in the group

2. Click the **Create a Group** toolbar icon.
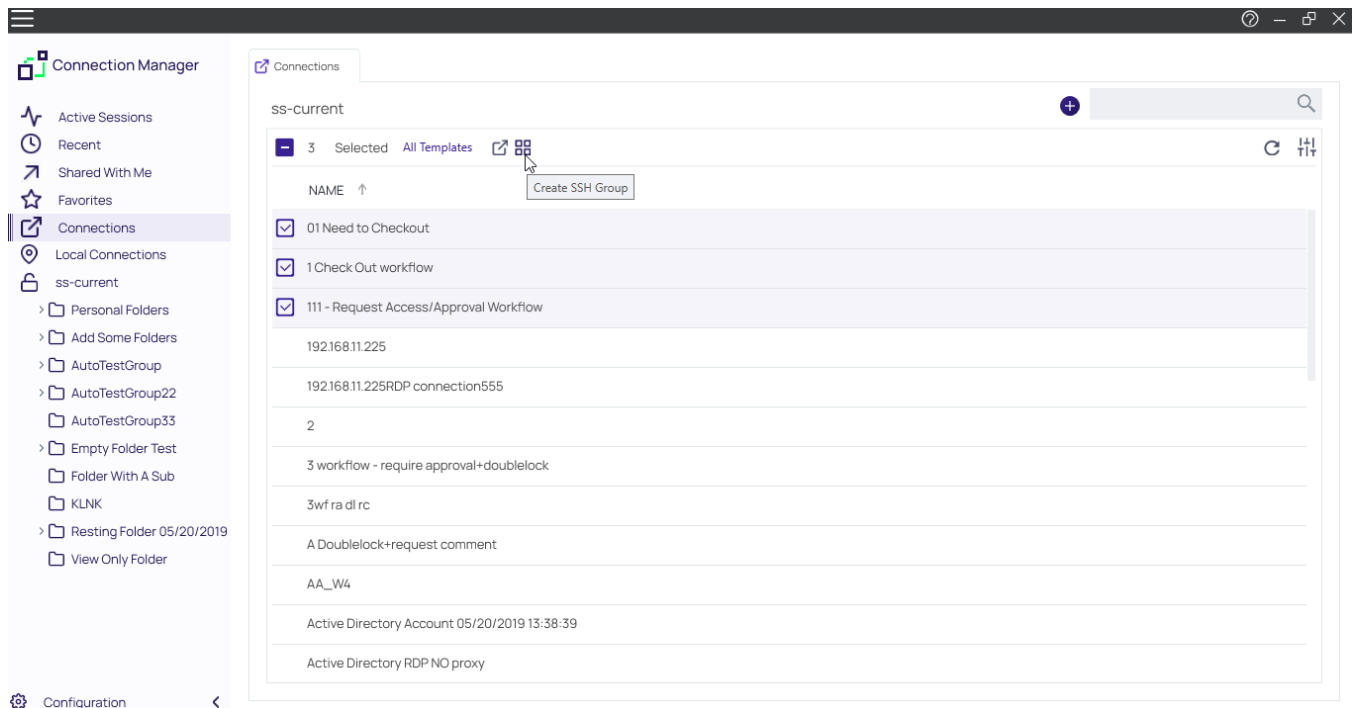
The second is to use the **Create SSH Group** option in right-click context menus.

Common User Activities
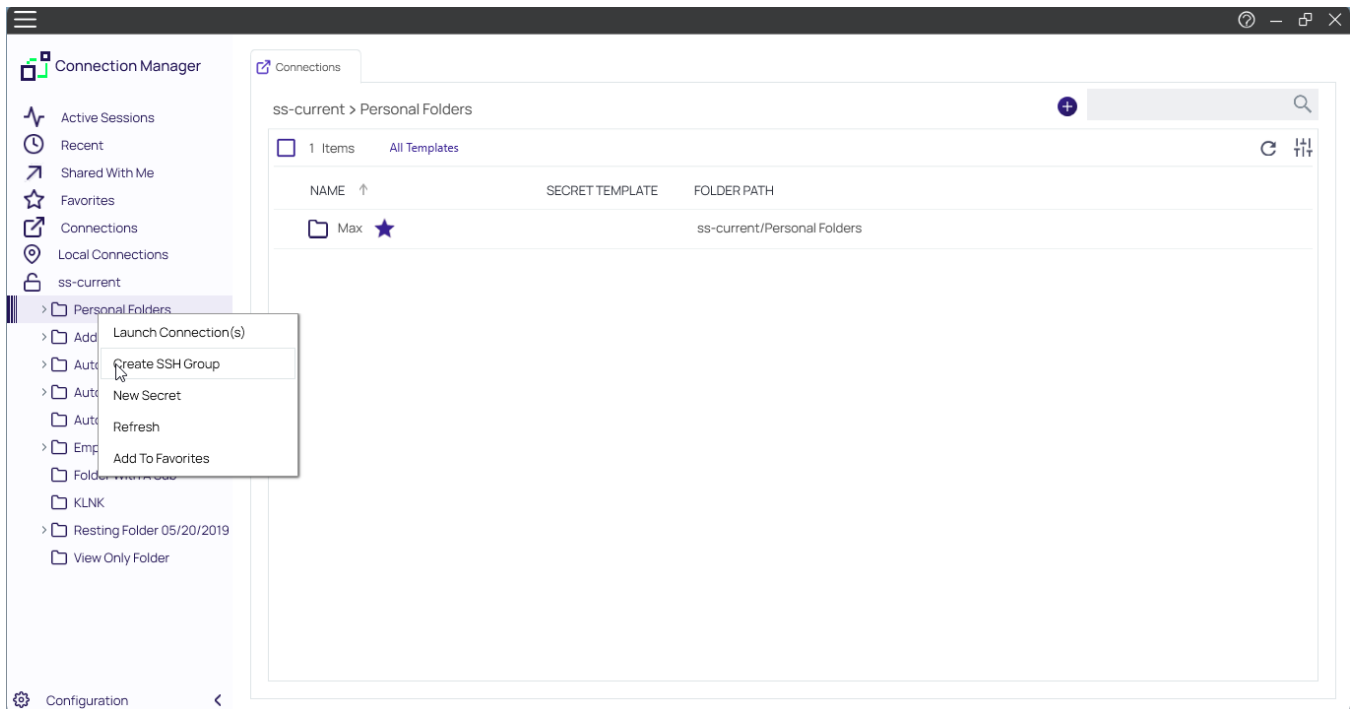
When the SSH Group is created, it opens in its own window with a special Group tab followed by the individual tabs for each SSH session in the group.
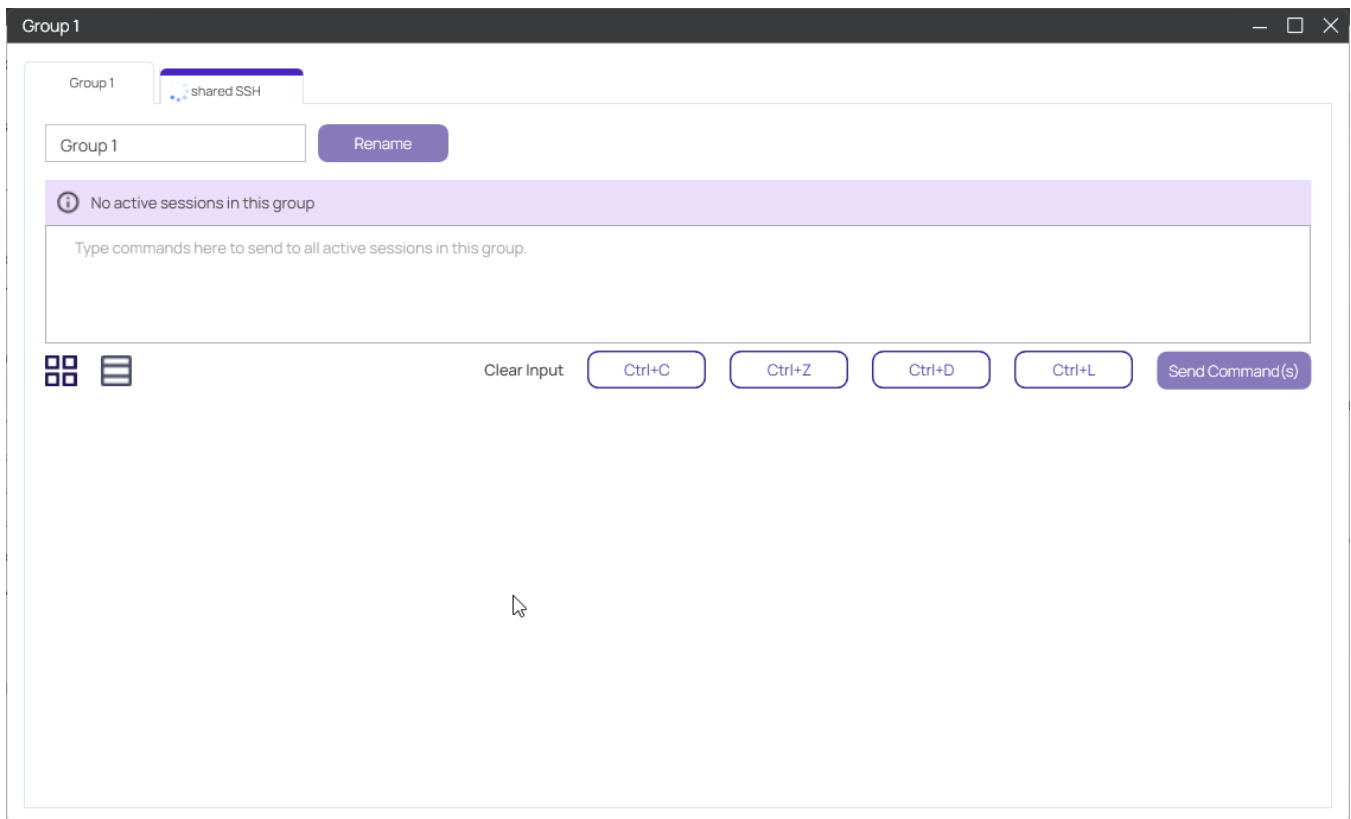
If the user has generated the SSH Group from sessions occupying a single folder, the group tab will be labeled with the name of the original folder. If the user has generated the SSH Group from sessions that did not occupy a single folder, the group tab will be labeled with a generated sequential name such as Group 1, Group 2, etc. The user can always change any group name from the name it was assigned initially.

Sending Commands to the SSH Group

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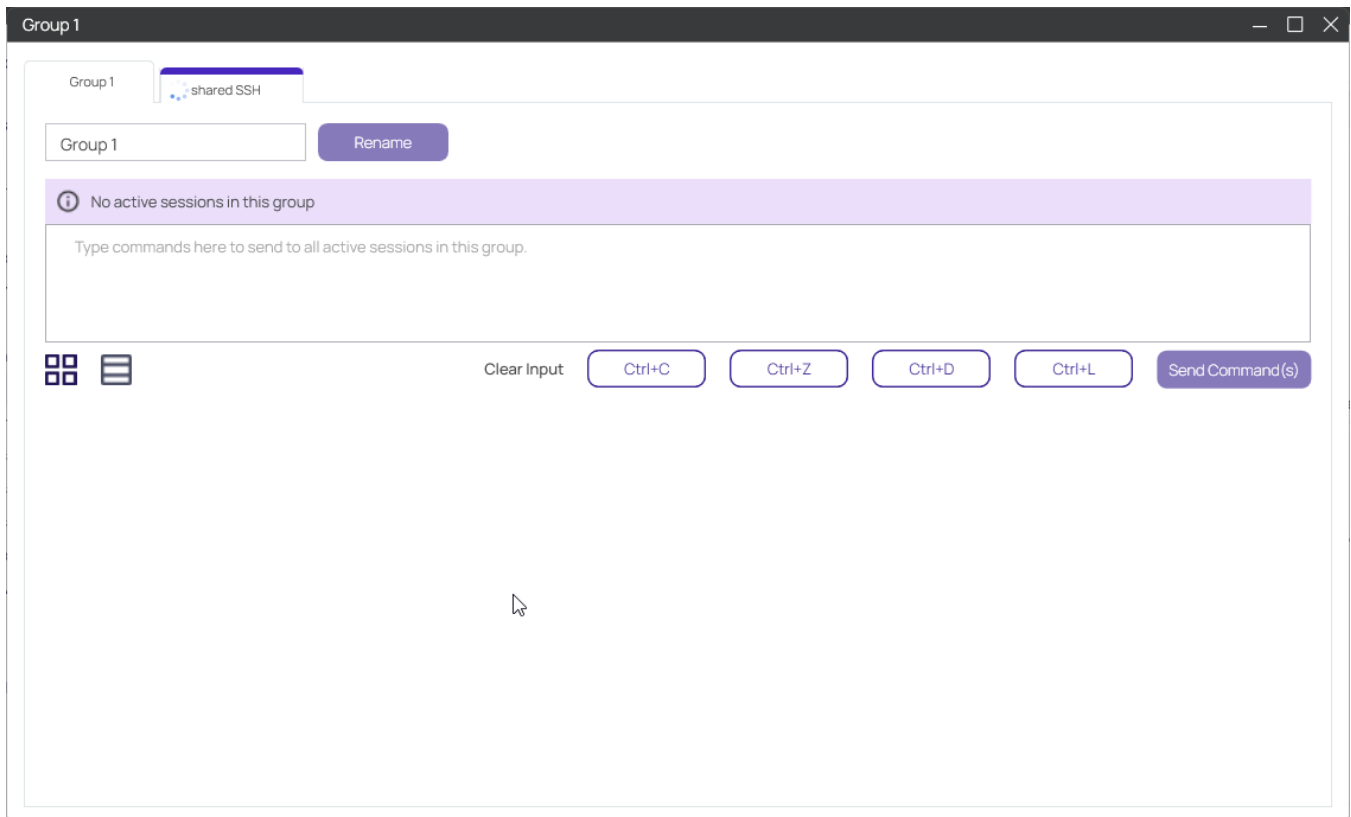
The four commands listed below are built into the user interface as individual buttons:

- **Ctrl+C** Kill whatever you are running. The confirmation alert should be displayed, the command should be broadcast to all sessions, and the top command should be stopped.

- **Ctrl+D** Exit the current shell. The "exit" should be displayed on all SSH sessions in the group; all sessions in the group should be closed, and the Group window should be closed.

- **Ctrl+L** Clear the screen, similar to the Clear command.

- **Ctrl+Z** Send whatever you are running into a suspended background process. fg restores it. The top command should be sent into the background.

Options for Displaying SSH Sessions on the Group Tab

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

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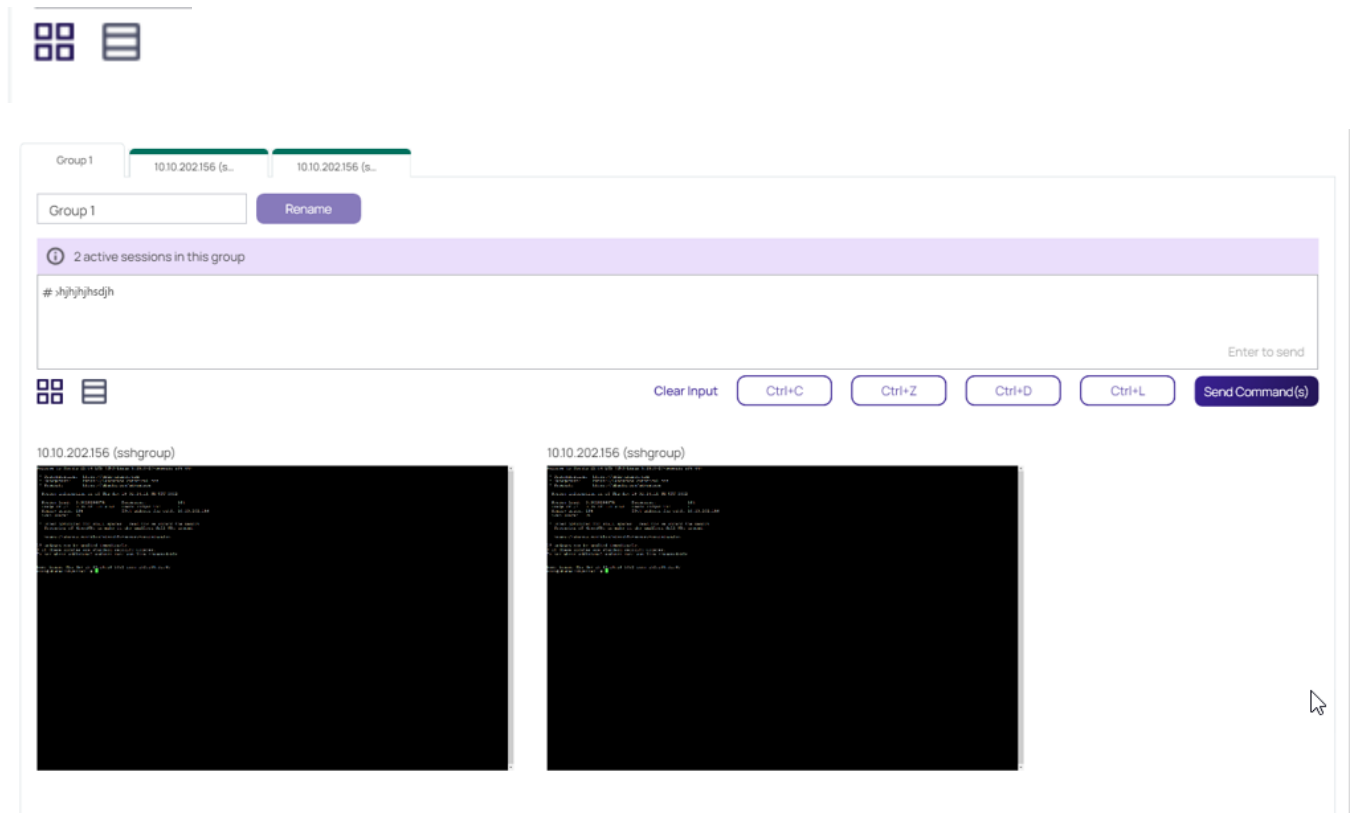
Building an SSH Group

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

Closing an SSH Group

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

Secrets with Workflows

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

- Multi-factor authentication
- Require Comment
- Check in or Check out (Able to check-in a secret if it was checked-out by the same user)
- Change Password on Check-in
- Prompt for Reason or Ticket System
- Request Access
- Double Lock

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

Once the workflow is successful, the connection is established.

Accessing Secrets Guarded by Multi Factor Authentication

Delinea Platform users can access secrets guarded by MFA through Connection Manager. When a user attempts to access a secret guarded by MFA, they will see a message that they must complete an additional MFA challenge:
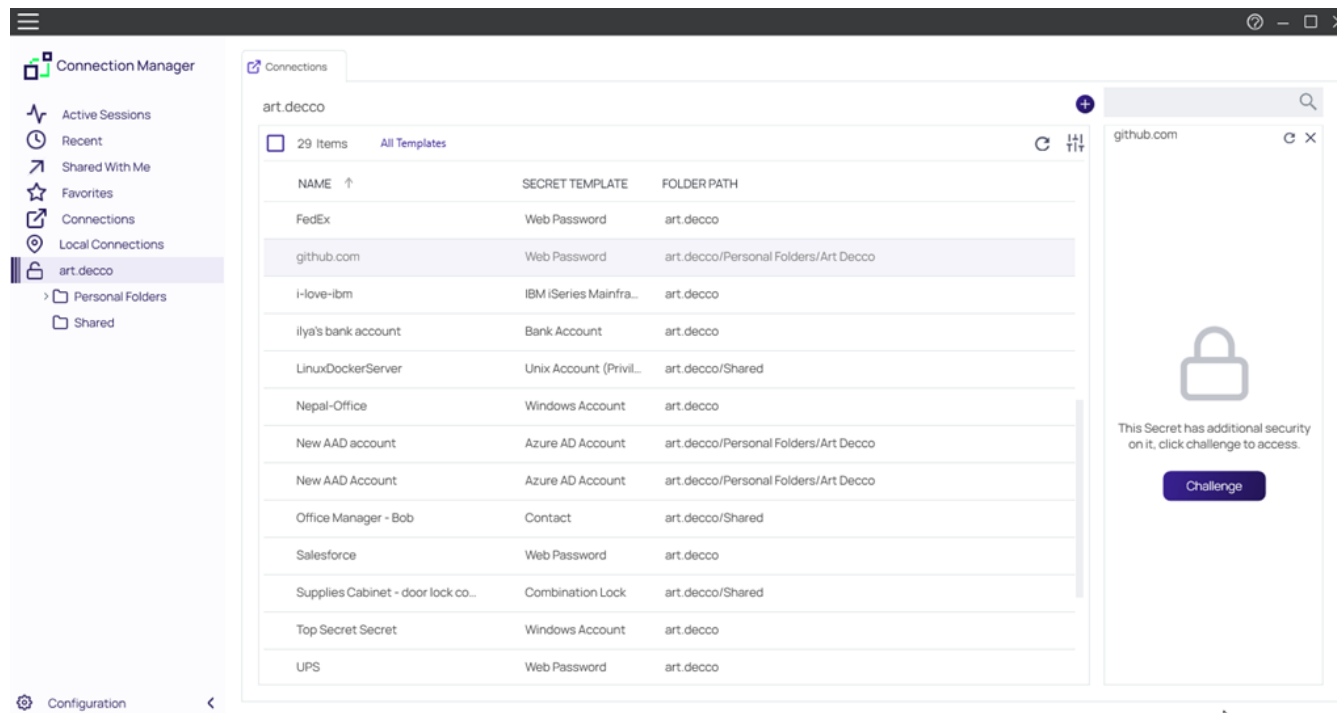
After clicking **Challenge**, users will be prompted to complete the MFA challenge in a separate Connection Manager window. When the MFA challenge has been successfully completed, users can return back to Connection Manager to view or launch the secret.
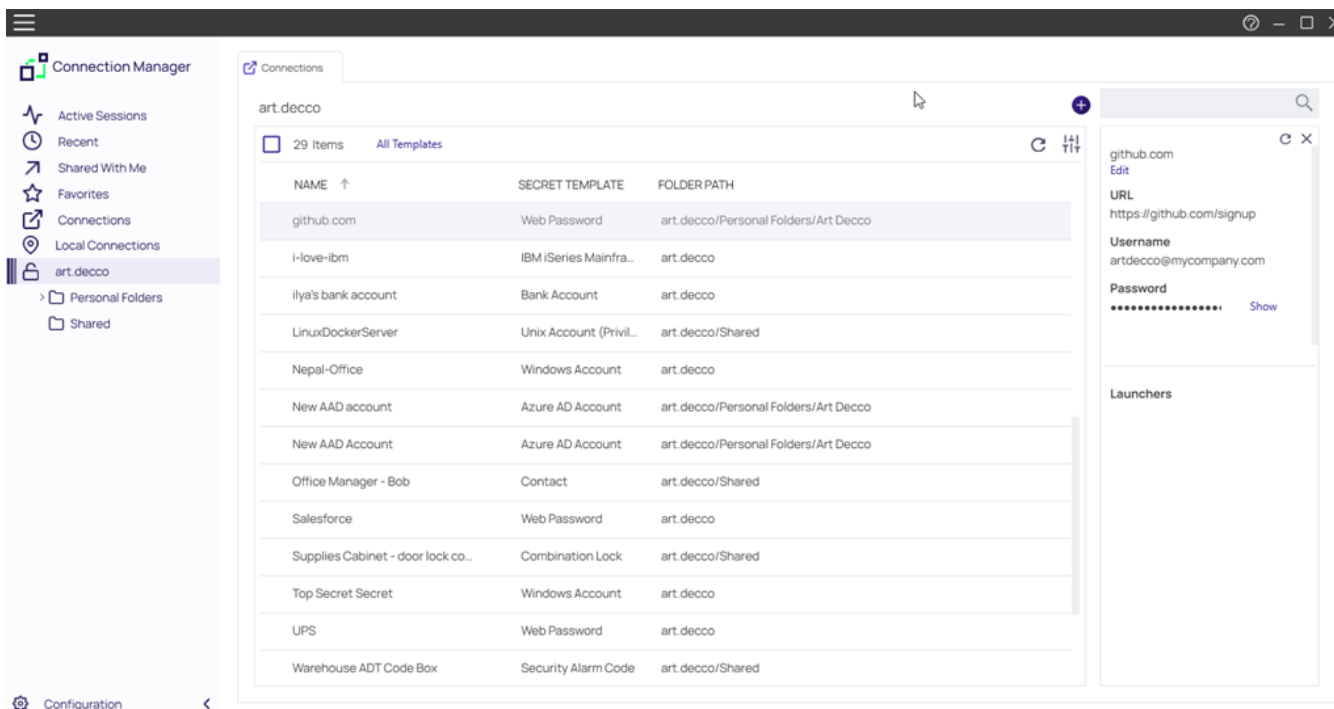
Secret Check Out Timer

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

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

2. If the secret requires check out, click **Check Out**

3. Once you have been granted access to the secret, you will see a timer in the right pane, along with all of the needed information about the secret.
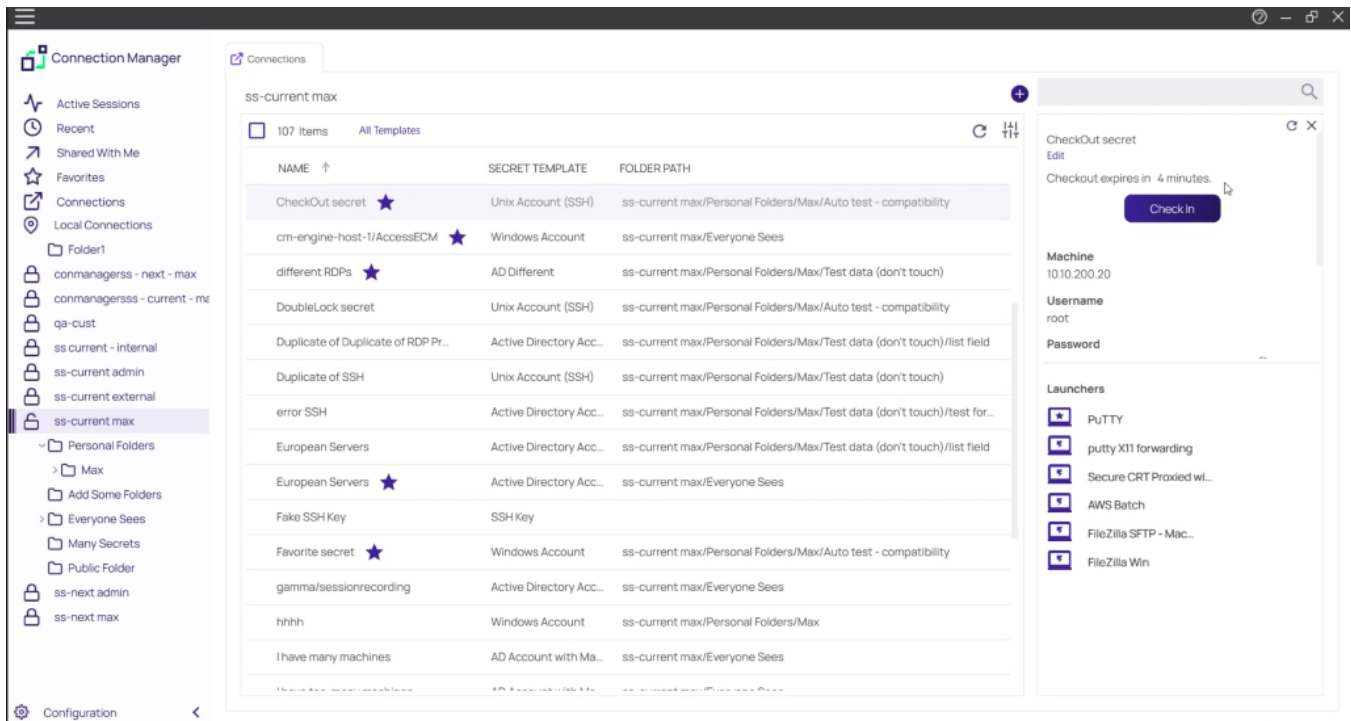
4. When the time remaining with the secret falls below the threshold set in Secret Server, the timer color will turn red to alert users that they are running out of time to access the secret.
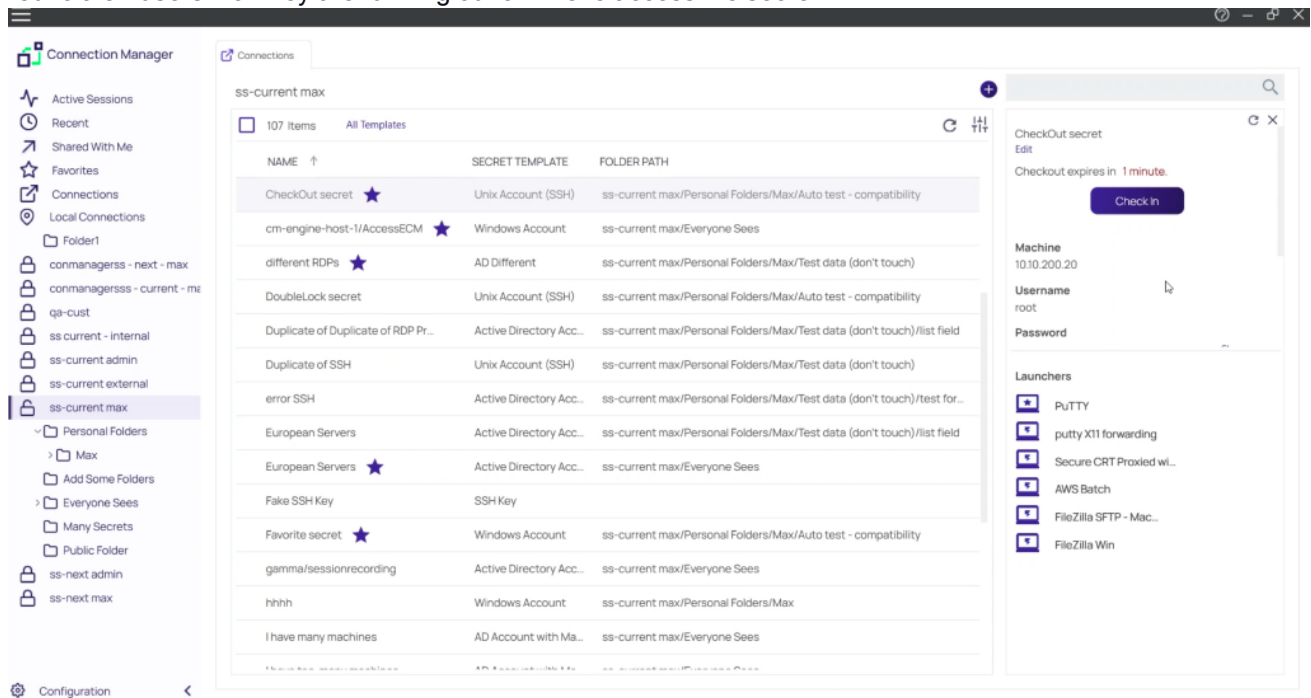
5. Users can extend the secret check out timer by clicking **Extend**. (Optional)

Secrets with Workflows
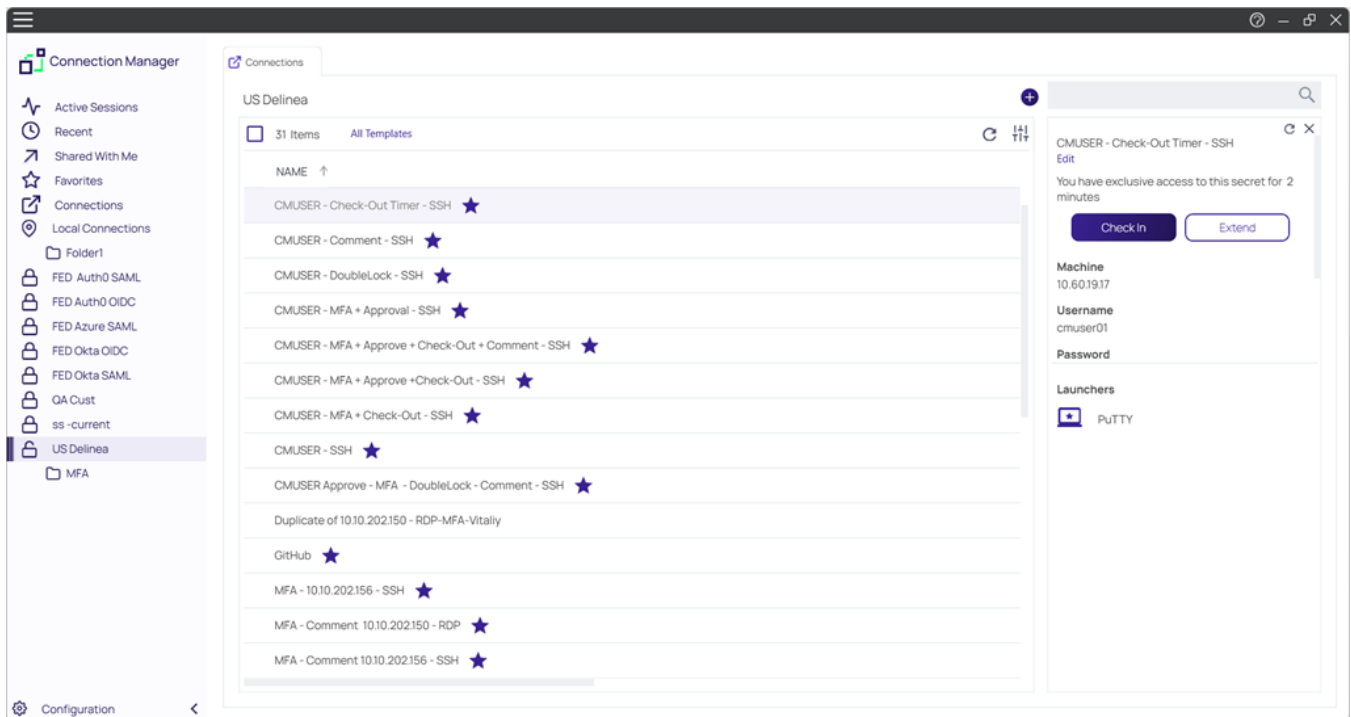
Users must enter a reason for extending the secret check out time
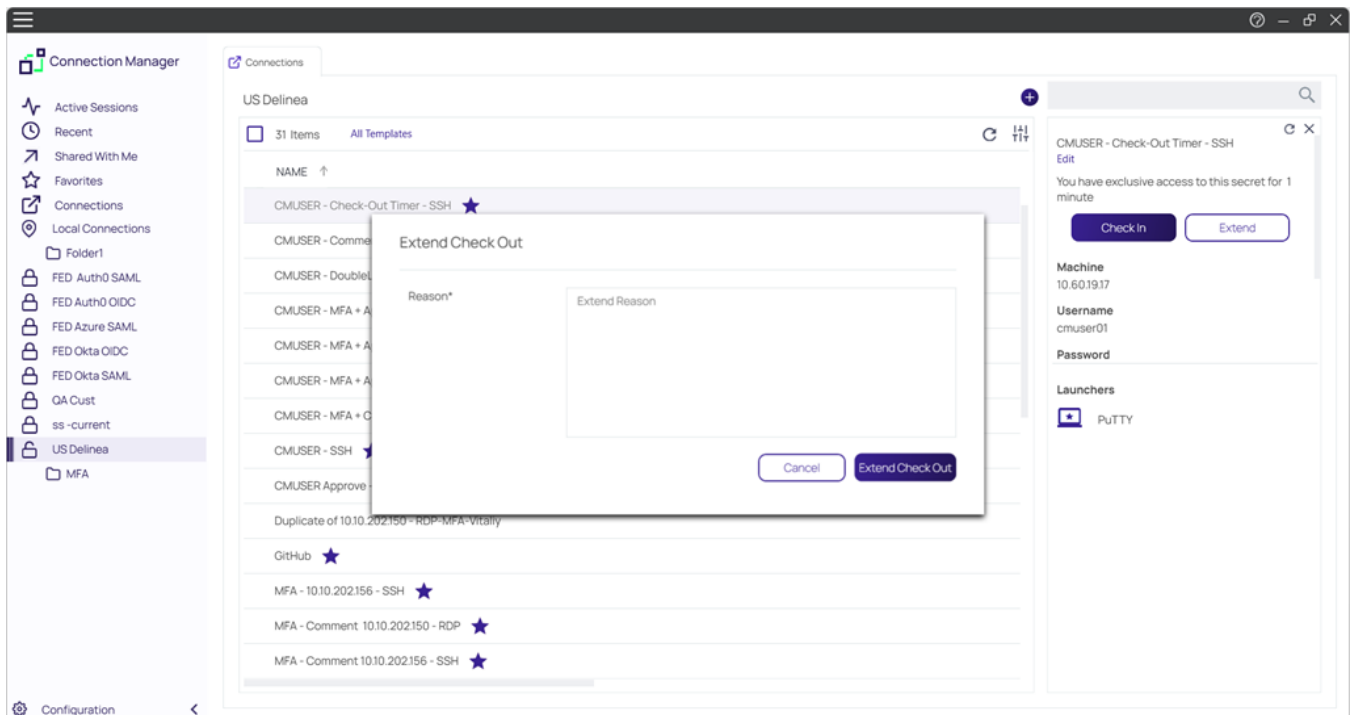
⚠ **Important:** The extend check out functionality needs to be configured in Secret Server.

> **Note:** The extend check out functionality is currently available on Windows only.

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
- Encryption
- Licensing
- Generate Additional Log Entries
- Related Resources

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\Delinea 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>
```

Issues With the Clipboard Functionality

If you are experiencing issues with the clipboard functionality (copy/paste), please try the following:

1. Check if clipboad access is enabled on the secret

.
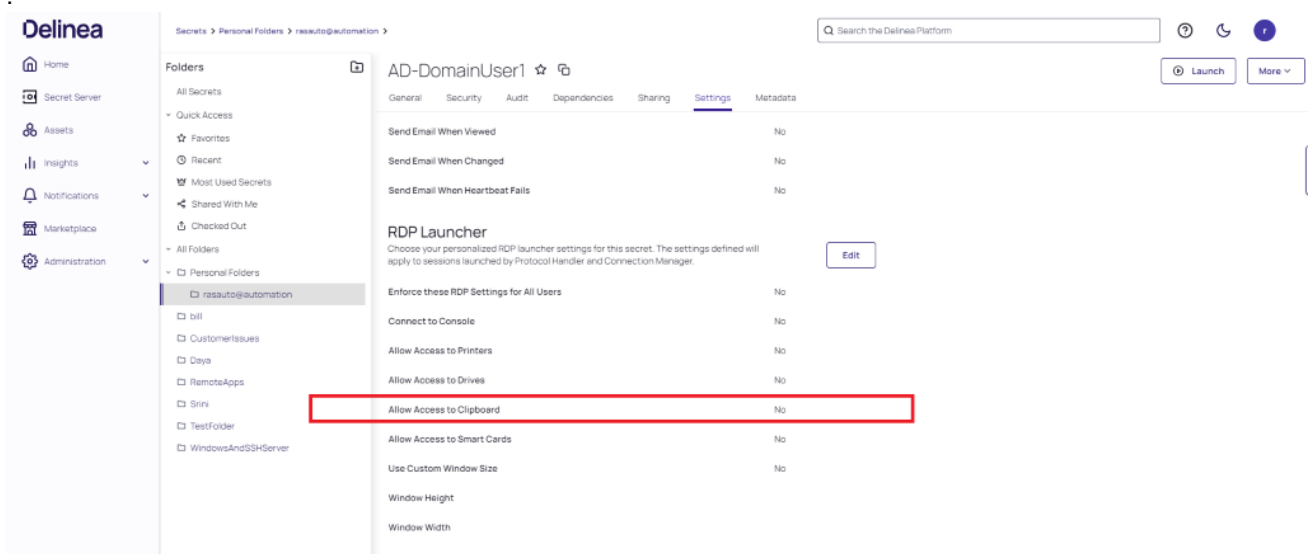
2. Make sure the clipboard functionality is enabled for RDP.

Global Configurations

RDP Global Settings | SSH Global Settings | Preferences | Launcher Settings

Initial Size: Auto

Auto-fill: ☑ This option will trigger an automatic reconnect event when the window is resized.

Color Depth: True Color (24 bit)

Run As Admin: ☐

Local Devices: Select resources to use in remote session:

☐ Printer   ☐ Drives   Specify Drives...

☑ Clipboard   ☐ Smart Cards

Windows Shortcuts: Only when using the full screen

Audio Playback: This Computer

Audio Recording: ☐

Cancel   Save

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

Problem

This is caused when a component that Connection Manager uses for session recording starts caching an invalid license for that component on the client machine. The invalid license causes an rdpwin.exe error for the recorded session when it launches, resulting in the error messages as shown in the examples above.

AVBlocks can call home to a licensing server, here `https://lms.primosoftware.com/`, from the client endpoint where the Protocol Handler is installed and it creates a local cache of the licence in `%temp%\primosoftware.lm.cache`.

If the access to the license server is then blocked, the cached license will eventually expire and cause a PH recording error:

```
ERROR: Invalid Code Highlighting Language
```

This can be seen in 6.0.0.13 and newer logs with verbose logging enabled in `C:\Program Files\Thycotic Software Ltd\Secret Server Protocol Handler\log4net-rdp.xml`.

Workaround

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

CM Crashing When Offline and Checking Certificates

Issue

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

Resolution

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

Encryption

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

General

What are the default locations for the Connection Manager application and log files?

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

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

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

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

Is there a local session timeout for sessions within Connection Manager (CM)?

Yes. - For Local Connections, the Windows default socket connect timeout applies (e.g. standard RDP/SSH remote session timeout). The session timeouts on secrets can be set in Secret Server (SS).

I'm seeing a Connection failed error message while trying to connect to SS

`Connection failed reason: Request to Secret Server failed. Internal server error. An error has occurred.` Seeing this error upon connection to SS means the currently installed version of SS is lower than 10.7.

Is there a way to refresh the SS connections?

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

Where and how is the data for Connection Manager stored?

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

Is there a way to push scripted code out to multiple SSH sessions at one time for updates or commands?

Is there a way to send a scripted file out to multiple PuTTY sessions at once using commands?

There is currently no support to run this type of action from Connection Manager. This is sometimes done with X11, but we do not currently support that connection type. There is a Feature Request in the backlog to add support.

What happens if the SS Heartbeat fails?

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

Is there any current performance data for Connection Manager? Including: general memory, amount of space needed, number of open connections that can be made at one tie, etc.

We are getting more information. Currently we have tested with up to 30 open connections. Some of the performance numbers will depend on the system hardware for the machine that is running Connection Manager.

While recording a session, if a user isn't on tab, what's the behavior? Do we reduce what we record and send? Or does it stay the same? How can we tell if it's the "focus"?

We follow the same behavior as the Secret Server session recording. If a user is not on the Tab, then we record and send less information.

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

Host Names

We follow these general naming conventions and constraints:

https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

An underscore "_" in the host name is not currently supported. The underscore has a special role, as it is permitted for the first character in SRV records by RFC definition, but newer DNS servers may also allow it anywhere in a name. For more details, see: http://technet.microsoft.com/en-us/library/cc959336.aspx

Licenses

Does a current customer drop in the platinum trial license key into their current Secret Server instance to receive the Connection Manager feature?

Yes, if the platinum trial license was created recently.

Does it matter, if Connection Manager is working with a different Secret Server instance than the one aligned with the trial key?

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

Is it okay to add trial license to production server? Will it overwrite or add to the current license?

It should add and run alongside the current license. While the Trial is active, they will have access to Secret Server Platinum level features, but once the trial expires, they will revert to their existing license.

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 files and folders

Remove the specified files and folders at the following paths:

- C:\Users\UserName\AppData\Roaming\Delinea

  (folder **Delinea** must be deleted)

- C:\Users\UserName\AppData\Local\Delinea_Inc

  (folder **Delinea_Inc** must be deleted)

- C:\Program Files\Delinea

  (folder **Delinea Software Ltd** must be deleted)

Clear entries from the Registry

Clear entries from the registry as specified below:

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\sslauncher
- HKEY_CURRENT_USER\Software\Delinea
- HKEY_LOCAL_MACHINE\SOFTWARE\Delinea Inc
- HKEY_CURRENT_USER\Software\Classes\sslauncher
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version Vector
- HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\Version Vector

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

Related Resources

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

Release Notes

Connection Manager Version Compatibility with Secret Server

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

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.

Release Notes History

The following Connection Manager release notes are available:

Changelog

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

Connection Manager Version Compatibility with Secret Server

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

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.

November 2023

- 2.3.1 Release Notes, refer to "2.3.1 Release Notes " on the next page
- 2.3.0 Release Notes, refer to "2.3.0 Release Notes " on page 131

September 2023

- 2.2.0 Release Notes, refer to "2.2.0 Release Notes" on page 132

August 2023

- 2.1.0 Release Notes, refer to"2.1.0 Release Notes" on page 132

July 2023

- 2.0.1 release notes, refer to Release Notes

May 2023

- 2.0.0 release notes, refer to Release Notes

April 2023

- 1.9.7 release notes, refer to Release Notes
- 1.9.6 release notes, refer to Release Notes

January 2023

- 1.9.5 release, refer to Release Notes

September 2022

- 1.9.2 release, refer to Release Notes

April 2022

- 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.

November 2021

- 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.

August 2021

- 1.6.2 release updates, refer to Release Notes for details.

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

July 2021

- 1.6.0 Feature release updates, refer to Release Notes for details.

March 2021

- 1.5.0 Feature release updates, refer to Release Notes for details.

March 2021

- 1.5.0 Feature release notes, refer to Release Notes for details.

December 2020

- 1.4.1 Feature release updates, refer to Release Notes for details.

August 2020

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

July 2020

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

June 2020

- Added two topics to the Troubleshooting section:

  - Application Crash when Editing Existing Secret Server Connection

  - AVBlock Error with Session Recording

2.3.1 Release Notes

November 21st, 2023

Improvements

- *PreferredAuthentications* setting added that allows specifying the SSH authentication methods priority order. Leaving the PreferredAuthentications value as empty will use previous version functionality (2.2) and will not use the new methods.

Bug Fixes

- Fixed an issue with the SSH authentication method selecting.

2.3.0 Release Notes

November 13th, 2023

Features

- Connection Manager now offers support for macOS 14 Sonoma.
- Users are now able to extend the secret checkout timer directly from the Connection Manager UI. (Windows only)
- Connection Manager can now complete logins when MFA is enabled on target machines with the Delinea Privilege Control. (Windows only)

Improvements

- *Auto-fill* has been relabeled to *Auto Resize.*

Bug Fixes

- Fixed an issue where external browser login was not working correctly on Windows Server (Using the Local Group Policy Editor)
- Fixed an issue where users had to complete multiple MFA prompts after upgrading to Connection Manager version 2.0.
- Fixed an issue with a double SAML token request in Connection Manager version 2.0.1 and newer.
- Fixed an issue where the "WinWord Process Launcher" was keeping an RDP connection active, even if the user activated the "Terminate immediately" option.
- Fixed an issue where the Smart Card option was intermittently not being displayed while in an RDP session.
- Fixed an issue where auto-fill was not working correctly when changing a window's size during the launch process.
- Fixed an issue where Connection Manager was not able to launch a URL link with ":" if this symbol was entered manually.
- Fixed an issue where Connection Manager was using a high amount of GPU.
- Fixed an issue where the full screen mode was not actually full screen when using RDP Proxy.

2.2.0 Release Notes

September 27th, 2023

Features

- When using local secrets mapped to vaulted secrets, Connection Manager users can now select any defined proxy site they need to use for connecting with the target specified in the local secret.

Improvements

- The auto-expand feature has been improved to allow customers to automatically resize their remote connection view when working with RDP connections.

Bug Fixes

- Fixed an issue where the check in/check out information was missing from the countdown timer.

- Fixed an issue where users were unable to automatically map headers from imported CSV files.

Windows Specific

- Fixed an issue where Connection Manager did not clean up memory when connections were closed.

- Fixed an issue where users were unable to create a folder using the right click mouse button.

- Fixed an issue where the Connection Manager tab would not close correctly when attempting to exit out of a proxied connection.

- Fixed an issue where an incorrect app name was displayed in the Connection Manager installer.

- Fixed an issue where the Connection Manager remote session name tab did not display the correct machine name.

- Fixed an issue where auto resize was not working consistently when maximizing the Connection Manager window.

- Fixed an issue where a CSV file could not be imported with a tab delimiter.

- Fixed an issue with Connection Manager instability when the RDP reconnect clipboard would fail.

- Fixed an issue where the Connection Manager session tab would freeze because of multiple reconnection attempts when switching between tabs with an active RDP session.

macOS Specific

- Fixed an issue where Connection Manager would display an RDP Error "Unable to connect to Server to verify its HTTPS certificate".

2.1.0 Release Notes

Release Date: August 17th 2023

Features

- Users are now able to access secrets guarded by MFA by completing the MFA challenge from within Connection Manager.

Improvements

- Improved scroll-back buffer size in SSH on Windows. Clients can now use a 32k-line scroll-back buffer out of the box for SSH sessions. The macOS buffer size is unlimited

- The launcher icon and text are now clickable. The hover and alt-text now mirror the label for improved accessibility [Windows]

- Connection Manager now assumes https if the user has not entered a protocol as part of their vault URL (Delinea Platform or Secret Server)

Bug Fixes

- Fixed an issue where Connection Manager's custom launcher was not displaying the correct field name

- Fixed an issue where Connection Manager was displaying an error message and allowing users to open unencrypted DAT files in the DEBUG log

- Fixed an issue where Connection Manager was not accepting SSH keys with a passphrase

- Fixed an issue where Connection Manager was displaying an invalid response when an RDP Launcher session was launched with a server field on Windows

- Fixed an issue where the Connection Manager launcher allowed the prompt to contain an forward slash character

- Fixed an issue where Connection Manager was displaying a warning about the version when using the external browser with Secret Server Cloud

- Fixed an issue where Connection Manager would crash after closing the popup window that is waiting for authentication

- Fixed an issue where Connection Manager was not checking secrets when connected to Secret Server Cloud using the external browser and local connection

- Fixed an issue where Connection Manager was not displaying the version of Secret Server and information text for the *Connection* dialog

- Fixed an issue where Connection Manager was displaying an incorrect URL message error message for Secret Server sites on macOS

2.0.1 Release Notes

Release Date: July 5th, 2023

Improvements

- Connection Manager now supports universal-token based authentication with the Delinea Platform.

Bug Fixes

- Fixed a bug that caused instability with Connection Manager when a secret was checked out by a different user

2.0.0 Release Notes

Release Date: May 24th, 2023

Features

- Users can add connections to their vault by using their Delinea Platform tenant URLs. Connection Manager will connect seamlessly to their Platform tenant vault and users will be able to use secrets in the vault in the same way as they do today with a direct Secret Server vault integration.

Bug Fixes

- Fixed an issue where Connection Manager was only displaying the top 30 secrets of a Secret Server folder containing more than 30 secrets.
- Fixed an issue where Connection Manager was evaluating Batch Launcher Parameters incorrectly.

Known Issues

- Audit session recordings can be found in the vault direct web portal (Secret Server web UI). The ability to send audit session recordings to the Delinea Platform will be added in a future release.
- Users with MFA-enabled secrets (a Platform-only feature) will not be able to use these secrets from Connection Manager version 2.0.0. A future release of Connection Manager will support this capability.
- Connection Manager version 2.0.0 does not currently support a small subset of federated logins related to Azure AD Conditional Access when used with the Delinea Platform. Support for this ability is scheduled for a future release.

1.9.7 Release Notes

Release Date: April 18th, 2023

Bug Fixes

- Fixed an issue on the Mac platform, where Connection Manager would crash when viewing a secret with an active "Hide Password" flag.

1.9.6 Release Notes

Release Date: April 3rd, 2023

Features

- Connection Manager now offers support for the *Preserve SSH Client Process.* This prevents custom launchers that result in single tabbed processes from exiting when multiple launches are pulled into it.

Bug Fixes

- Fixed an issue where a tab would not close after Connection Manager crashed.

- Fixed an issue where an incorrect *Properties* panel was displayed in the secret check-out timer.

- Fixed an issue where Connection manager would close third-party apps after the connection was terminated.

- Fixed an issue where an error message was displayed to the users when a connection was terminated after the secret check-out timer expired.

- Fixed an issue where an incorrect screen was displayed to the users after the secret check-out timer expired.

- Fixed an issue where Connection Manager would crash after updating from version 1.8 to 1.9.5.

- Fixed an issue where Connection Manager would crash when attempting to check-out two secrets.

- Fixed an issue where an incorrect *Properties* panel was displayed if the user was not able to connect to host on the secret.

- Fixed an issue where an error message was not being displayed after the checkout timer expired on a secret.

- Fixed an issue where Connection Manager would crash after clicking the *Check-Out* button.

- Fixed an issue where Connection Manager would crash after clicking *Check-In* on Secret Server in browser.

1.9.5 Release Notes (Windows)

Release Date: January 17th, 2023

Features

- Connection Manager now supports custom launchers using the *Proxied SSH Process* launcher type when the *Preserve SSH Client Process* is selected. Closing the Connection Manager tab for these sessions will no longer enforce terminating the external application, allowing for other connections within the external application to continue uninterrupted.

- Connection Manager now shows a secret checkout timer which allows users to see how much time they have before the checkout expires.

- Connection Manager now offers a new version number which makes it easier for users to see which version of Connection Manager they are using from the *About* menu.

General Improvements

- When creating a new Secret Server connection, the "External browser" option will now be selected as the default connection type. This was implemented to support a security hardening initiative in Secret Server.

Maintenance Improvements

- The EULA link in Help > About was updated to point to Delinea's Master Subscription and License Agreement. Previously the link pointed to the delinea.com website EULA

Bug Fixes

- Fixed an issue where users would encounter an error message after double-clicking on a connection to a Secret Server instance

- Fixed an issue where proxied RDP connections would disconnect when the screen was resized

- Fixed an issue where Connection Manager was preventing users from launching Unix secrets that use "User Input" for the launcher

- Fixed an issue where users would encounter an error when attempting to launch SSH connections from a mapped secret where an Active Directory secret template was used

- Fixed an issue where Connection Manager would crash when clicking on the Favorites folder

- Fixed an issue where the Help button in the 1.8 version of Connection Manager would take users to an old documentation page for the 1.7 version of Connection Manager

- Fixed an issue where Connection Manager would prompt users for credentials if the connection was interrupted

- Fixed an issue where Connection Manager would disable the Alt+F4 keystroke combination across all windows

- Fixed an issue where Connection Manager's RDP clipboard was rendered inoperable with the CrowdStrike Falcon agent installed on Windows

1.9.2 Release Notes

Release Date: September 1st, 2022

Features

- Users can now create a Secret Server connection via an external browser. This resolves issues with limitations in the embedded browser that prevent some SAML logins from completing successfully.

- Users can now automatically see secrets created on new templates without editing connection settings. The 3rd step of the **Edit Connection** dialog now contains two options: one to select all templates including ones created later, and one to select specific templates to view in Connection Manager. The default option for new installations is *All Templates* and can be changed by the user by editing the Secret Server connection.

- Silent installations will now set the selected templates to *All Templates*. This can be changed by the user after installation by editing the Secret Server connection.

General Improvements

- Updated FreeRDP 2.4.0 to the latest version.

Security Improvements

- Updated Coverlet.Collector to the latest version.

- Updated Newtonsoft.Json to the latest version.

- Updated log4net 2.0.13 to the latest version.

Bug Fixes

- Fixed an issue where Connection Manager was not showing the full password.

- Fixed an issue where the 1.8 version of Connection Manager was missing the Refresh button in dark theme.

- Fixed an issue with the RDP Client title bar behavior with RDP Proxy. The title was not showing the target in full screen mode.

- Fixed an issue where the connections list attempted to connect to the wrong server.

- Fixed an issue where users were seeing the wrong font for SSH Local Connection after installing Connection Manager.

- Fixed an issue where users where getting an error message when clicking the **Show** button to show the password.

- Fixed an issue where Connection Manager was not honoring the *Hide Password* setting when adjustments were made at the Secret Template level

iOS Specific

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

1.8.0 Release Notes

Release Date: April 19, 2022

Features

- Delinea Connection Manager now supports:
  - All M1 chipsets
  - Windows 11

- Delinea Connection Manager now allows AD Site Selection.

- This release includes the new Delinea Inc rebranding along with our new company colors and icons.

General Improvements

- Users will now be able to see the ServerName (proxied over "proxy name") in a tab header when connecting through proxy.

- We optimized load performance in larger environments with 65K or more secrets and 40K or more folders. This performance improvement should be especially noticeable on slower connections.

Bug Fixes

- Fixed an issue users were experiencing where the screen size would automatically change from the set desktop size to the one in the secret settings.

- Fixed an issue where Connection Manager command lines did not allow both -disablelocalvault and Secret Server connection switches.

- Fixed an issue where the remote host name is not displayed on the tab for proxied RDP session.

- Fixed an issue where users were unable to scroll inside Connection Manager if there is any text selected.

- Fixed an issue where an update couldn't be automated under local system account (in quiet mode)

- Fixed an issue where Connection Manager cannot be uninstalled with SYSTEM account

iOS Specific

- Fixed an issue with the Clipboard feature macOS users were experiencing, which prevented them from copying from a Mac to an RDP endpoint.

1.7.1 Release Notes

Release Date: November 30, 2021

Bug Fixes

- Fixed an issue where the login URL is not detected properly if SS URL ends with '/'.

- Fixed an issue where an error occurs when connecting to a RDP session when proxy is enabled.

- Fixed issues related to SecretServer URL validation in certain federation scenarios.

- Fixed an issue with SAML login when the Secret Server web services timeout is set to "Unlimited". We do not recommend setting the web services timeout to "Unlimited".

1.7.0 Release Notes

Release Date: November 9, 2021

Product Enhancements

SSH Grouping

- Users can now create one or more groups of active SSH sessions using a new toolbar icon or by using the **Create SSH Group** option in right-click context menus. By creating an SSH group, a user can send a command or series of commands in bulk to all active sessions in the group. See Using SSH Session Groups.

General

- The way Connection Manager takes screen shots of active connections has been optimized for efficient resource usage.

- Users can now drag the left edge of a secret's Properties panel to enlarge the panel.

- Users can now view helpful information about Secrets in pop-up windows by mousing over different parts of a Secret in the main Secrets view.

- On Secret Details screens, users can now manually refresh the display of the secret's information by clicking a Refresh button. The information is refreshed simultaneously in the Properties, Shared With Me, and Favorites panels.

- Using the column picker, you can now add a Heartbeat column to the main Secrets view to display heartbeat results returned by Secret Server.

  The heartbeat value represents a point in time; it is not automatically updated in real time. The user must manually refresh the page yo see the most current value.

- Every password field and Private Key Passphrase field now offers the user an option to show the hidden password characters if you have View permissions. Depending upon permissions in Secret Server, you might be able to copy the password using the Copy icon, without having View permissions.

- WLOG output can now be viewed in Connection Manager debug logs for macOS.

- We added more command line arguments to the Connection Manager documentation and we clarified related content such as which arguments should be used for installation and which should be used for startup.

- We added information to the Connection Manager documentation identifying default folders for macOS.

- We updated and clarified the content in the Connection Manager documentation on Global Configuration options and their related behaviors.

- For secrets protected by both Checkout Required and Enter Comment workflows, users can input their comment text and then simply click the "Enter Comment" button to automatically check out the secret.

Bug Fixes

- We fixed an issue where RDP screen shots came out black when taken in full screen mode.

- We fixed an issue where auto-sizing was not working as expected.

- We fixed an issue where only the first machine was displayed in a secret's Machine field list, rather than the machine connected to when launching from Secret Server.

- We fixed an issue where Connection Manager's Map Secret feature was throwing no authentication method for .ppk (private key) files.

- We fixed an issue that arose when a user using two monitors opened an RDP connection in full screen mode on one monitor, and that monitor's active session screenshot display was black.

- We fixed an issue in the user interface that was preventing some users from connecting to the last Secret Server connection listed in the left navigation panel.

macOS Bug Fixes

- We fixed an issue where a user reconnecting to Secret Server received the error message, "Object reference not set to an instance of an object," followed by Connection Manager crashing.

- We fixed an issue where Connection Manager was crashing after a PuTTY paste with the error message, "Object referenced not set to an instance of an object."

- We fixed an issue where Connection Manager was crashing when a user performed a copy and paste in an SSH session.

- We fixed an issue where macOS (Big Sur v.11.5) was getting stuck when attempting to connect to Secret Server via Connection Manager.

Known Issues and Workarounds

- Connection Manager "Local Login" allows users to log in with their username, but if they try to log in with their UPN, the login fails.

- Connection Manager does not generated a token when the URL for a web login ends on a /.

1.6.2 Release Notes

Release Date: August 17, 2021

Bug Fixes

- Fixed an issue on macOS when using SSH (Putty) launcher with cut/copy/paste causing the error "Object Referenced Not Set to an Instance of an Object"

- Fixed a redirect issue when using Jumpcloud integration

Known Issues and Workarounds

- **Intermittent Issue**: On macOS when run in Protocol Handler mode, cut/copy/paste does not work. The app does not crash. If the app is "unlocked," cut/copy/paste actions work. To unlock the app, expand the left navigation panel and double-click the "lock" icon for your Secret Server connection.

- **Intermittent Issue**: On macOS, while connected to any Secret Server, if the user edits the same Secret Server name (via the Secret Server Connections menu), the app could get stuck in a "connecting" state (Web login only).

- **Intermittent Issue**: On macOS, some users may experience issues connecting to Secret Server via web login (SAML) where the connection stays in a "connecting…" state.

- **Upgrade Issues**: In some situations, after the update is downloaded, the installer may not start the install process. In that case, please download the files from the links below or via Secret Server and run the installer manually or using a software deployment tool.

  - **On macOS**: When upgrading from v1.6.0, the automatic update process fails to launch the installer.

  - **On Windows**: The auto update may not launch the installer on some Windows systems

Links for downloading the installers:

- **macOS**: https://downloads.cm.delinea.com/Thycotic.ConnectionManager.MacOSInstaller.pkg

- **Windows**: https://downloads.cm.delinea.com/Thycotic.ConnectionManager.WindowsInstaller.msi

Connection Manager and Secret Server Version Compatibility

CM Version	What Will Work	What Will Not Work	Resolution Steps
1.6.0 and earlier	CM can launch secrets in Protocol Handler mode	If using Secret Server v11.0 or newer, Connection Manager v1.6.0 will display an error accessing and/or launching any secrets except when used in Protocol Handler mode. Operation of CM v1.6.0 with earlier versions of Secret Server is unaffected.	If you are using Secret Server v11.0 or newer, OR you are a cloud customer, please upgrade to Connection Manager v1.6.2 or newer.
1.6.1 (rel. Aug 10, 2021)	Access and launch for most secrets	If using Secret Server v11.0 or newer, Connection Manager v1.6.0 and earlier cannot access or launch secrets with Lists. Operation of CM v1.6.0 with earlier versions of Secret Server is unaffected.	If using Secret Server v11.0 or newer, upgrade to Connection Manager v1.6.2 or newer for **Lists** support.
		If using Secret Server v11.0 or newer, Connection Manager v1.6.1 cannot access or launch secrets with Lists. Operation of CM v1.6.1 with earlier versions of Secret Server is unaffected.	If using Secret Server v11.0 or newer, upgrade to Connection Manager v1.6.2 or newer for **Lists** support.
		Connection Manager's built-in upgrade feature does not work when upgrading to v1.6.1. This issue affects both Mac and Windows versions of Connection Manager.	Download and run the Connection Manager installer for the desired version. Manual installation and installation using a software deployment tool are equally effective.
		Connection Manager v1.6.1 does not function correctly on macOS Big Sur. Connection Manager crashes when user provides the password for their local data store.	Upgrade to Connection Manager v1.6.2 or newer.
1.6.2 (rel. Aug 17, 2021	Access and launch for all secrets	Connection Manager's built-in upgrade feature does not work when upgrading to v1.6.2 for some users. This issue affects both Mac and Windows versions of Connection Manager.	Download and run the Connection Manager installer for the desired version. Manual installation and installation using a software deployment tool are equally effective.

Underlying Causes of Issues

API Response Changes in Secret Server v11.0:

- **Workflow/checkout**: A data structure returned from API did not change, but the range of values returned in a data field changed to accommodate new functionality. Connection Manager did not handle the change correctly.

- **Lists**: API includes a new field type in returned data to provide new Lists functionality in Secret Server 11.0. API consumers must make an additional call to retrieve list data. Connection Manager does not include support for this new feature until v1.6.2.

1.6.1 Hotfix Release Notes

Release Date: August 10, 2021

Bug Fixes

- Fixed an issue for macOS where users were getting the error message, "Object reference not set to an instance of an object" after losing connection and attempting to reconnect to Connection Manager.

- Fixed an issue for macOS where users were unable to use the Control or Shift keys when connecting to a remote machine via RDP.

- Fixed an issue for macOS where the RDP session was not disconnecting when the user selected "Disconnect" from the menu.

- Fixed an issue where users were getting the error message, "Error accessing Secret" on secrets with checkout enabled.

- Fixed an issue where users would get a 404 error when attempting to launch pre-saved local connections after an in-place upgrade from Connection Manager version 1.5.0.

Connection Manager and Secret Server Version Compatibility

CM Version	What Will Work	What Will Not Work	Resolution Steps
1.6.0 and earlier	CM can launch secrets in Protocol Handler mode	If using Secret Server v11.0 or newer, Connection Manager v1.6.0 will display an error accessing and/or launching any secrets except when used in Protocol Handler mode. Operation of CM v1.6.0 with earlier versions of Secret Server is unaffected.	If you are using Secret Server v11.0 or newer, OR you are a cloud customer, please upgrade to Connection Manager v1.6.2 or newer.
		If using Secret Server v11.0 or newer, Connection Manager v1.6.0 and earlier cannot access or launch secrets with Lists. Operation of CM v1.6.0 with earlier versions of Secret Server is unaffected.	If using Secret Server v11.0 or newer, upgrade to Connection Manager v1.6.2 or newer for **Lists** support.
1.6.1 (rel. Aug 10, 2021)	Access and launch for most secrets	If using Secret Server v11.0 or newer, Connection Manager v1.6.1 cannot access or launch secrets with Lists. Operation of CM v1.6.1 with earlier versions of Secret Server is unaffected.	If using Secret Server v11.0 or newer, upgrade to Connection Manager v1.6.2 or newer for **Lists** support.

CM Version	What Will Work	What Will Not Work	Resolution Steps
		Connection Manager's built-in upgrade feature does not work when upgrading to v1.6.1. This issue affects both Mac and Windows versions of Connection Manager.	Download and run the Connection Manager installer for the desired version. Manual installation and installation using a software deployment tool are equally effective.
		Connection Manager v1.6.1 does not function correctly on macOS Big Sur. Connection Manager crashes when user provides the password for their local data store.	Upgrade to Connection Manager v1.6.2 or newer.
1.6.2 (rel. Aug 17, 2021	Access and launch for all secrets	Connection Manager's built-in upgrade feature does not work when upgrading to v1.6.2 for some users. This issue affects both Mac and Windows versions of Connection Manager.	Download and run the Connection Manager installer for the desired version. Manual installation and installation using a software deployment tool are equally effective.

1.6.0 Release Notes

Release Date: July 6, 2021

New Features

- For added security, administrators and users can now disable storage of connection credentials and passwords in a local data vault. When 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 are permanently deleted and the user will only be able to access 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.

- Users can now import RDP and SSH connections in CSV format from a file created in a third party platform, including Devolutions, Microsoft Remote Desktop, and Royal TS. Connection Manager automatically detects the CSV file format, checks field mappings for ConnectionType, Name, Host, and CredentialUsername, concatenates the "CredentialsDomain" column with the "CredentialsUsername" column, and provides a confirmation message when the import is complete.

- Users can now customize the display of columns in the secret list window, including which columns are displayed, the width of each column, and the order in which items appear in each column (alphanumerical or reverse alphanumerical). The custom settings can also be saved together as a default.

- Users can now use SSH Proxy to make a local connection to Secret Server using mapped credentials,a capability previously available only for RDP Proxy.

- Users can now use Windows key combination shortcuts in an RDP session. These settings can be configured per connection or globally.

- Organizations can now upload their own logo to replace the Delinea logo in the Connection Manager application interface.

- Users can now pre-select Secret Server connections to automatically launch and authenticate on startup.

- Users can now create and edit secrets in Secret Server using a link in Connection Manager.

- Users can now search for secrets by the template they are based on.

Automation and Improved Workflows

Connection Manager now provides guided workflows and automated default behaviors that simplify the processes of connecting to Secret Server and searching for secrets.

- In previous releases of Connection Manager, the user could not search for a secret without first selecting a folder to search in. Now Connection Manager automatically selects the top-most folder (connection) and performs an exhaustive downward search from there, covering every file in the folder selected, and every file in every level of subfolder. This is already the default search behavior when mapping a secret to a local connection in the Mapping dialog. If the user selects a folder to begin their search, Connection Manager performs an exhaustive downward search from there.

- When connecting from previous releases of Connection Manager to Secret Server, users could select individual secrets to create connections from. Now users can also choose to select all secrets at once, then deselect any individual secrets that are not needed. This feature saves time for users who need to create initial connections using all or most secrets from a large collection of secrets.

- When a user initiates a connection using a secret that requires checkout, Connection Manager now presents a notification reminding the user to check in the secret when they are finished using it. This behavior, which mimics the user experience that Secret Server has provided for some time, helps to prevent secrets from being unnecessarily unavailable to others for 24 hours or longer.

- If you begin to search for a secret and you have active connections to Secret Server but you haven't chosen one, Connection Manager now automatically chooses an active connection for you. If you begin to search for a secret but you have no active connection to Secret Server, Connection Manager reminds you to set up an active connection before your search can proceed.

- When a user is launching multiple sessions simultaneously, Connection Manager now offers a one-click option to select a single launcher for all sessions.

- Users can now open more than one instance of Connection Manager per user on each server.

- Users can now use the same DAT file on Windows and Mac systems.

Product Enhancements

- In the process for launching a single local connection/secret, the "Connect" action is now named "Launch Connection" in the interface.

- Under Global Configurations, a *Preferences* tab has been added enabling users to choose how server names and secret names appear on tabs and thumbnails.

- When a user is proxying from local connections, the name of the server connected to now appears first, in the following format: *[ServerName] - Proxied over [DE Name]*

Bug Fixes

- The name of the Connection Manager installer file is now correctly identified as `Thycotic.ConnectionManager.WindowsInstaller`

- Users can now use Web Login with Multi-Factor Authorization apps such as Duo without getting errors or multiple redirects.

- Users on Unix Mac machines can copy newline characters via SSH proxy and the characters are now preserved.

Known Issues

- When using some versions of Connection Manager on a Mac to launch a secret through Secret Server, the connection fails. To fix this issue, try upgrading to the newest version of Connection Manager.

Maintenance

- Upgraded the embedded Chromium Browser to version 89.0.17 to support the latest stable channel of Chromium.

General Information

- Connection Manager does not support Windows Server 2003.

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

Connection Manager and Secret Server Version Compatibility

CM Version	What Will Work	What Will Not Work	Resolution Steps
1.6.0 and earlier	CM can launch secrets in Protocol Handler mode	If using Secret Server v11.0 or newer, Connection Manager v1.6.0 will display an error accessing and/or launching any secrets except when used in Protocol Handler mode. Operation of CM v1.6.0 with earlier versions of Secret Server is unaffected.	If you are using Secret Server v11.0 or newer, OR you are a cloud customer, please upgrade to Connection Manager v1.6.2 or newer.
		If using Secret Server v11.0 or newer, Connection Manager v1.6.0 and earlier cannot access or launch secrets with Lists. Operation of CM v1.6.0 with earlier versions of Secret Server is unaffected.	If using Secret Server v11.0 or newer, upgrade to Connection Manager v1.6.2 or newer for **Lists** support.

CM Version	What Will Work	What Will Not Work	Resolution Steps
1.6.1 (rel. Aug 10, 2021)	Access and launch for most secrets	If using Secret Server v11.0 or newer, Connection Manager v1.6.1 cannot access or launch secrets with Lists. Operation of CM v1.6.1 with earlier versions of Secret Server is unaffected.	If using Secret Server v11.0 or newer, upgrade to Connection Manager v1.6.2 or newer for **Lists** support.
		Connection Manager's built-in upgrade feature does not work when upgrading to v1.6.1. This issue affects both Mac and Windows versions of Connection Manager.	Download and run the Connection Manager installer for the desired version. Manual installation and installation using a software deployment tool are equally effective.
		Connection Manager v1.6.1 does not function correctly on macOS Big Sur. Connection Manager crashes when user provides the password for their local data store.	Upgrade to Connection Manager v1.6.2 or newer.
1.6.2 (rel. Aug 17, 2021	Access and launch for all secrets	Connection Manager's built-in upgrade feature does not work when upgrading to v1.6.2 for some users. This issue affects both Mac and Windows versions of Connection Manager.	Download and run the Connection Manager installer for the desired version. Manual installation and installation using a software deployment tool are equally effective.

1.5.0 Release Notes

Release Date: March 2, 2021

Features

- Protocol Handler Improvements
  - Administrator option to have Connection Manager register itself as the default Protocol Handler for all users
  - Preserve the default Protocol Handler selection during an upgrade.
  - Ability to have users switch between **Connection Manager** and **Legacy Protocol Handler**
  - Administrator option to install/uninstall the **Legacy Protocol Handler** as the default for all users
  - Ability for a non-admin user to switch between **Connection Manager** and **Legacy Protocol Handler**
- Customize the colors used in a SSH Session.
  - Users will be able to choose colors used in an SSH session for the background, foreground, bold and underlined text

- Users will have a **Global Configuration** option as well as the ability to override and choose a different set of colors * for each local connection.

- Both Windows and Mac users will also be able to use the full color palette available on both systems.

- Users will be able to select from a preset color set or define a custom color set.

- Global configuration will be applied to new local connections only. Does not impact existing local connections or secret server connections.

■ Ability to choose local drives for mapping in an RDP session.

- Users will be able to select the drives they wish to map in an RDP session instead of choosing **All Drives** only.

- Global configuration will be applied to new local connections only. Does not impact existing local connections or secret server connections.

■ Auto-click the **Generate Token** button

- Added ability to automatically have **Generate Token** clicked for the user when connecting to Secret Server or when re-establishing a connection to make that process seamless to the customer.

■ Added capability to manage the connection to Secret Server during intermittent loss of internet connectivity.

- By setting a longer timeout if there is intermittent loss of internet connectivity, Connection Manager will hold on to the session allowing the user to resume without having to reconnect manually to secret server.

- Connection Manager will also automatically re-authenticate to Secret Server when connectivity has been re-established or give the user the option to manually re-authenticate.

- The reconnect notification dialog will be visible for about 3 minutes after which the dialog will close and the Connect dialog will open allowing the user to connect when internet connection has been re-established.

■ Enhanced searching in a machine list

- Users will be able to search from a long list of machine names and the list will filter as they type. Example typing "Ser" will narrow the results to all Server1, Server2 and Server3

■ Renamed *Whitelist* to *Allowed List* and *Blacklist* to *Blocked List*.

- To match the naming convention in Secret Server, we renamed the wording *Whitelist* in Connection Manager to *Allowed List* and *Blacklist* to *Blocked List*.

Maintenance

■ Upgraded FreeRDP library to 2.2.0 (Should resolve unexplained RDP connection interruptions in Connection Manager for Mac)

■ General Maintenance Updates

- Set copyright image to 2021 (Win/Mac)

- Resolved issues with a stuck connection with Connection Manager for Mac

- Added configuration option to disable automatic checking for update on startup.

- Set RDP session to stay in Full Screen mode after reconnecting if previous mode was full screen.

- A custom DAT file created in 1.4 will be usable in 1.5.

Name Changes

- We made some updates to our naming conventions. Instead of using the term "Whitelist" we will use "Allowed List". Also, instead of using "Blacklist" we will use "Blocked List".

Bug Fixes

- Resolved issues when the Mac app showed "null" certificate and the FreeRDP library crashes when connecting to a windows server (Mac)

- Fixed an issue when mapping a local SSH connection to a Secret resulted in the error **A supplied password or username is incorrect**.

- Resolved unexplained RDP connection interruptions in Connection Manager for Mac

- Resolved issues related to the Protocol Handler on a Mac. Full Screen and menu items now work with Protocol Handler (Mac)

- Resolved an issue where the **Connect to Secret Server** dialog would hang if the connection was physically disconnected (Mac)

- Resolved issues with High CPU utilization on a Mac (Mac)

- Fixed issues related to Connection Manager crashing after a .json file import.

- Resolved unrecoverable error connecting to Secret Server cloud via web login.

- Fixed issues where Connection Manager could not switch back to the legacy protocol handler (Secret Server Launcher) for non-admin users.

- Resolved issues related to installing/uninstalling Connection Manager, using the legacy Protocol Handler (Secret Server Launcher) to launch secrets. Also see features under *Protocol Handler Improvements* above.

Known Issues

- Periodic black video in SSH session recording

- RDP Connections may not stay open when Connection Manager auto-reconnects after a brief interruption in the internet connection.

- Connection Manager not requesting a token refresh when TOTP is enabled.

- In a Citrix environment when connecting via SSH Tunnel Proxy, you may in some cases get the error, **Failed to configure RDP component. The specified socket is already in use**.

- SSL Certificate bypass is not possible when using the Web Login method to connect to Secret Server.

- Some users may get redirected to the Secret Server web page instead of Connection Manager when using the TOTP method and web login to connect to Secret Server or Secret Server cloud.

- When used as a Protocol Handler, cannot open more than one instance per system.

- When launching a secret from secret server on a Mac, connection fails with **Unexpected DTD declaration** error in the logs.

1.4.1 Release Notes

Release Date: 15-December-2020

Enhancements

▪ Users can now open connections in bulk by selecting multiple connections across multiple folders and clicking once to open them all, or by moving multiple connections into a folder and clicking the folder once to open all connections in the folder.

▪ Users can now click and drag a session tab to undock it from the main Connection Manager window. The tab becomes a standalone window that users can move to a different monitor or to a different position on their desktop. Users can also re-dock the window as a tab next to any of the other tabs in the main Connection Manager window.

▪ Users can now open an RDP session in full screen mode on a second monitor.

▪ Users can now reorganize Local Connections by dragging and dropping folders.

▪ Users can now duplicate an existing connection using copy/paste, then rename it or save it in a different folder.

▪ Users can now edit Local RDP or SSH connections in bulk.

▪ Added Run as Admin support for RDP sessions.

▪ A new "Shared with me" section in the navigation lists all secrets/sessions shared with you from a Secret Server connection.

▪ When a session is connecting using a proxy, the remote host name appears on the session tab at the top of the screen.

▪ Users can now enable the microphone option on an RDP connection (not the same as session recording)

▪ Devolutions import now provides improved error message handling.

▪ Users can now see the Secret name on the Select Launcher dialog.

▪ Users can now mark multiple items as Favorites using the Context menu.

▪ An icon has been added to the Connection tab for maximizing the window.

Bug Fixes

▪ Renaming the default launchers in Secret Server no longer causes an error in Connection Manager on session launch.

▪ Connection Manager no longer freezes or crashes when SSH proxy is turned on in Secret Server.

▪ Users no longer receive frequent requests to re-authenticate while the RDP session is open.

▪ The Generate token button now works correctly after upgrading to a newer version.

▪ Connection Manager now displays the endpoint name when used as an RDP launcher.

▪ Connection Manager UI now appropriately restores to full screen and to the previously resized window.

▪ Connection Manager now supports "Proxied SSH process" launcher types.

▪ On the Connecting with an invalid certificate warning, Connection Manager now saves the selection to "bypass this error and connect anyway" (Mac OS).

▪ When connecting to Secret Server, long template names are no longer truncated (Mac OS)

▪ Fixed an issue related to exporting local connection folders.

Known Issue

- Clicking on "X" to close an undocked session window, then immediately trying to move the window back to the docking area could lock the other tabs.

  Workaround: Close and re-start Connection Manager.

1.3.2 Release Notes

Release Date: 2020-08-11

Bug Fixes

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

MacOS Specific

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

1.3.0 Release Notes

Release Date: 2020-07-28

> **Note:** Installer versions:

- Windows: 1.3.0
- macOS: 1.3.1

Enhancements

- Ability to import connections from third party platforms in CSV format.
  - Adding option to import from CSV.
  - Includes "Import" dialog which allows mapping of fields in CSV to Connection Manager fields.
  - Imported connections import as Local connections.
  - Import can generate 2 reports:
    - Failed items – This report can be imported again to retry just the failed items.
    - Informational report – This report provides information for any fields that were set to use "default" values.
- Improve dynamic resizing for RDP sessions when tab window is expanded beyond original size (resizing session for larger windows/full screen).
- Added "About" screen to display version number, EULA and docs links.
- Added support for "Favorites":

- Favorites tab/page to view items that are marked as Favorites.

- Launch connections from Favorites page.

- Mark Local connections/Secrets/Folders as Favorites and add them to the Favorites page.

- Dark theme support for Mac and Windows (determined by OS).

- Improving validation for basic import/export file in JSON format.

- Added a back-off delay for Connection Manager login, which allows 3 attempts before adding a 5 second delay, increasing the delay by 5 seconds on each following attempt up to 25 second.

- Enforce Secret Server connections to use HTTPS (and not allowing HTTP).

- Added support for smart card passthrough for Secret Server based RDP connections.

- Additional options/settings for using Connection Manager as a protocol handler for Secret Server.

- Setting in CM to switch between using CM as SS protocol handler or SS as the protocol handler.

- Connection Manager build package will ship with Secret Server (to act as the SS Mac protocol handler).

Bug Fixes

- Fixed an issue that prevented Connection Manager from fully launching a session using the protocol handler on macOS.

- Fixed the size of the file download dialog not being correct (too small) when updating the application.

- Resolved CefSharp (CVE-2020-6418) vulnerability in web browser for Secret Server login.

- Fixed an issue for launching Secrets that connect using RPD proxy.

1.2.1 Release Notes

Release Date: 2020-04-28

BUGS

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

MacOS Specific

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

1.2.0 Release Notes

Release Date: 2020-04-14

Enhancements

- Added ability to create a new Local Storage file (for Local Connections) directly from the Connection Manager Sign In dialog.

- Updated the User Interface so the Navigation section can be resized.

- Updated the general style for the Properties tab (bolding the headers, and text formats).

- When a large number of tabs are open, double-clicking on the left or right scroll arrows will jump to the far end of the tab list (in either direction).

- Added ability to login to Secret Server using the Secret Server web login (for SAML support).

- Added ability to launch Secret Server Secrets that use other Launcher types. Connection Manager will support any launcher that is supported by Secret Server and includes, but is not limited to: PowerShell, CmdLine, MS Word, Notepad, Excel. These launchers also support opening a tab in Connection Manager, session recording, and workflows.

- Added the ability to launch a Secret in the Secret Server UI and have the protocol handler open and run the launcher in Connection Manager. The Secret needs to be configured to use the protocol handler, and then launching it will use Connection Manager if it's available. When Connection Manager opens it will be in a "Locked" state where only the Secret Server launched session(s) are available.

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

- Added support for two new Secret Server settings. Changing these settings in Secret Server will globally enforce the changes for Connection Manager applications that are connected. The Secret Server Settings are:

  - Allow Local Connections - Allows or disables the saving of credentials for any Local Connections. By default, this is set to Yes.

  - Allow Saving Credentials - Allows or disables the saving of credentials for any Secret Server connections. By default, this is set to Yes.

Bug Fixes

- Fixed an issue, where if you selected the first row in the main Work area the context menu options (on right-click) did not display all of the available options.

- Fixed an issue, where if the Secret Server URL contained "v1" in the path it was replaced with "v2".

- Fixed an issue with Integrated connections (a local connection with a Secret Server Secret for credentials) where a Local SSH connection was retuning an "incorrect username or password" message if the Secret uses Secret Server Proxy.

1.1.2 Release Notes

Release Date: 2020-01-28

Bug Fix (for both Windows and macOS)

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

1.1.1 Release Notes

Release Date: 2020-01-13

Bug Fix (for both Windows and macOS)

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

1.1.0 Release Notes

Release Date: 2020-01-08

New Features (for both Windows and macOS)

- Added ability to make an Integrated Connection: a Local Connection that uses a Secret from Secret Server for credentials.

- Added ability to perform Global Search when at the root for Local Connections or at the root of a Secret Server connection.

- Made loading of Folder, Connection, and Secret data dynamic when a folder is selected.

- Displayed Personal Folders folder at the top of a Secret Server connection.

- Added support for screen resolution size down to 1280x720.

- Added ability to refresh a Secret Server connection or folder from the navigation bar.

- Allow expanding and collapsing of Secret Server connections or Local Connections (at the root) in the navigation bar.

- Included Computer Name value in the tab title and tab tool-tip pop-up.

- Added support for a client PC running in FIPS mode.

- On the Recent page, added a Connection Source column to identify if a connection is Local or from Secret Server.

- On the Recent page, added a Connection Type column to identify whether Local Connection are SSH or RDP, or list the Secret template for Secret Server connections.

- Secret connections from Secret Server will be listed on the Recent page.

- When opening a Secret Server connection from the Recent page, a notification will be presented if the Secret has been deleted.

- Secret connections that use the Check-In/Check-Out workflow will display a Check-In button if the Secret is currently checked out by the user.

- The properties panel for Secret connections that use the Access Request workflow have been updated so the Access Request pop-up more closely matches the Access Request dialog from Secret Server.

- If a Secret connection from Secret Server uses an empty allowed list, launching a connection will open a text box to enter a value.

- If a Secret connection from Secret Server uses an SSH proxied session, Connection Manager will respect the Secret Server option to only record the SSH keystrokes from the session.
- If no Secret Server connection exists in Connection Manager, opening the Secret Server Connections configuration will open directly to the Connect to Secret Server dialog.
- Display user information message when a user has been disconnected from a remote session due to another user logging in.
- Improved error message handling when attempting to create a connection to Secret Server.
- When installing Connection Manager, allow for users to set a different location to store the local storage data file.
- In the File menu for Connection Manager, added a quick link to the documentation.

Bug Fix

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

1.0.1 Release Notes

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

1.0.1 Release Notes

Release Date: 2019-09-27

Bug Fix

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

1.0.0 Release Notes

Release Date: 2019-09-17

This is for the initial release of Connection Manager.

New Features

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

Connection Manager – Free Tool

Remote Sessions

- Able to create ad-hoc connections for RDP sessions.
- Able to create ad-hoc connections for SSH sessions using PuTTY sessions.
- Encrypt and store the credentials and general connection information for any Local connections.

- RDP Session - Add additional RDP session options (standard RDP options) when making a connection, including Windows Mode options (desktop size, color depth and auto window resizing) and Local Resource options (sharing of local devices, including audio).

- RDP Session - When editing a Local RDP connection, users should be able to change: the password, Windows Mode options and Local Resource options.

- SSH Session - Add additional SSH session options (standard SSH options) when making a connection, including Advanced SSH options (character set, font and font size).

- SSH Session - Add ability to specify a private key file and password to use when connecting to SSH session.

- SSH Session - Add ability to set and specify multiple Tunnel (using values for: Port, Destination server and Destination Port) for SSH sessions.

- SSH Session – When editing a Local SSH session, users should be able to change: the password, Advanced options (font size, type and character set), Private Key options and Tunnels.

- When Local sessions for RDP or SSH are launched the remote session will open as a new Tab in the work area.

- Remote sessions (RDP or SSH) have the ability to expand to a "Full Screen" mode.

User Interface

- Added left-hand tree style navigation bar.

- Create Local folders to store, manage and sort Local connections.

- Added breadcrumb navigation to the top of the work area.

- RDP and SSH session types are marked by different colors for the tabs.

- Added a Properties panel to the right inside the main work area when users select a connection or folder.

- In the properties panel for Local connections, allow users to view the password for that connection.

- Local connections can be launched using two methods: Double-click on the connection row in the work area or click the launcher icon in the properties panel.

- Existing Local connections and folders can be edited by right-clicking on the row in the work area or by clicking an "Edit" button in the properties panel.

- When editing a folder under the Local connections section the folder name can be changed.

- Add ability to Remove any Local connections or folders.

- Added ability to view a list of any "Recent" sessions by selecting "Recent" in the navigation bar.

- Sessions can be launched by double-clicking on a connection in the "Recent" page.

- Add ability to view a list/display of all active remote sessions on an "Active Session" page

- Show a screen view of a session on the Active Session page from the last time the session was accessed.

- Allow users to quickly navigate to a active session from the Active Session page by double-clicking on the session image.

- Add a scroll bar to the Tabs section of the work area so if multiple tabs are open and extend beyond the page, a user can scroll over to them.

- Add a Search bar to the top right of the work area so users can run a search on the current folder for a connection.

- Add a "Configuration" menu to the bottom of the navigation bar for application options.

- Make Global options for RDP and SSH sessions available for modification from the Configuration > Global Configuration option in the navigation bar.

- Add a set of Global RDP sessions options (using Windows Mode options and Local Resource options) that are used for new sessions by default.

- Add a set of Global SSH sessions options (using Advanced options [font size, type and character set], Private Key options and Tunnels) that are used for new sessions by default.

- Make Global options for RDP and SSH sessions available for modification from the Global Configuration option in the navigation bar.

- Add ability to Export existing Local connections and folders to an output file (JSON format).

- Make export action for Local connections available by right-clicking in the navigation bar or by right-clicking on a folder/connection in the workspace.

- When exporting a connection, users should have the option to include the Password (This will be in Clear Text so the file can be imported later).

- Add ability to Import a set of folders and connections (using the JSON format from the Export) under the Local Connections section.

- Make the import action only available from the navigation bar.

- The import action should add all folders and connection details specified in the JSON file under the specific folder location that was selected when selecting the option.

Connection Manager – Secret Server Integration

Integration

- Add ability to connect to a specific Secret Server instance (On-prem or Cloud).

- Add ability to add multiple Secret Server connections to a single Connection Manager instance.

- Display a list of all Secret Server connections under Configuration > Secret Server Connections.

- When connecting to Secret Server, allow for multi-factor login options (pin-code, duo push, duo phone call, none) to be used.

- When connecting to Secret Server add ability to select Secret templates to fetch for displaying Secrets.

- When a connection is established with Secret Server the folder structure containing the Secrets that can be accessed for the logged in user should be displayed in the navigation bar.

- Add ability to edit an existing Secret Server connection including the "friendly" name for the connection, password, domain field, multi-factor options and modify the list of templates.

- Add ability to remove a Secret Server connection.

- When selecting a Secret Server folder in the navigation bar, the work area should display all the Secrets and folders that are available to the user.

- Display a "Locked" icon when a Secret Server connection has not been authenticated and an "open lock" icon when it has been authenticated (for easy viewing).

- Add ability to launch a Secret with RDP or SSH credentials as a remote session similar to how Local connections are launched.

- When selecting a Secret from a Secret Server connection, do not display the Password field for the Secret in the properties panel.

- If a Secret doesn't have all the necessary fields to launch a remote RDP/SSH session, a dialog should open that prompts the user to enter the missing values (like machine name/IP).

- When selecting a Secret from a Secret Server connection, do not display the Password field for the Secret in the properties panel.

- Add ability to support Secret Server workflows including Check-In/Check-Out, Change password on Check-In, Double Lock, Prompt for Reason or Ticket System, Request Access and Require Comment.

- When accessing Secrets that use workflows, display a prompt for the workflow in the properties panel.

- Add support for Session Recording that is set on Secrets from Secret Server following the standards that Secret Server uses for Session Recording.

- When viewing a Secret in the work area that has Session recording set in the Secret, display a "Record" indicator on the launcher icon in the properties panel.

- When launching a Session that has Session recording set in the Secret, display a "recording" icon in the session tab.

- When Session recording for a remote session is active or completes, send all session information back to Secret Server for processing.

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