Enterprise Connect Passwordless for Windows Installation Guide v4.3.1

For Enterprise Connect Passwordless Server v5.8.2 and above

Table of Contents

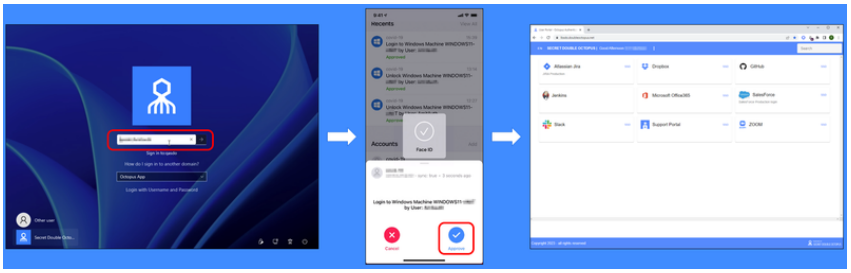
Preface

This document provides step-by-step installation instructions for Enterprise Connect Passwordless for Windows.

Product Overview

Enterprise Connect Passwordless replaces passwords altogether with a high assurance, password-free authentication paradigm. Using the Enterprise Connect Passwordless Windows Credential Provider in conjunction with standard interfaces to Active Directory, the password-free solution seamlessly replaces AD passwords with a stronger, more secure alternative. As a result, the security posture of the AD domain is enhanced, user experience and productivity improve, and password management costs are dramatically lowered.

The standard flow for passwordless authentication to Windows via the Authenticator mobile app is summarized in the diagram below.



Prerequisites

Before beginning installation, verify that:

- Enterprise Connect Passwordless Authentication Server **v5.8.2 (or higher)** is installed and operating with a valid enterprise certificate. Please install (or upgrade to) the latest Server version **before** installing Enterprise Connect Passwordless for Windows.
- **For Active Directory or Entra ID**:
    - Your Corporate Active Directory Server or Entra ID Server is operating with Admin rights and an AD LDAP root certificate to establish a secure LDAPS connection.
    - Corporate domain Windows machines (user PCs) are available.
- **For other Directory types**: Windows machines with local users are set to work with a non-AD directory (e.g., PingDS, Oracle).
- Enrolled users are assigned to use one or more authentication methods -- PingID Mobile Authenticator, ForgeRock Mobile Authenticator, FIDO authentication, etc.
- Workstations support TPM version 2.0.
- Visual C++ **2022 (or later)** Redistributable (x64)/(x86) - 14.32.31332 is installed.

Enterprise Connect Passwordless for Windows supports the ability to control availability of the credential provider after installation, allowing for gradual deployment of the solution within your organization. For more information, refer to Enabling / Disabling the Enterprise Connect Passwordless Authentication CP Post-installation.

Enterprise Connect Passwordless for Windows supports Windows 10 and 11 and Windows Servers 2016, 2019 and 2022.

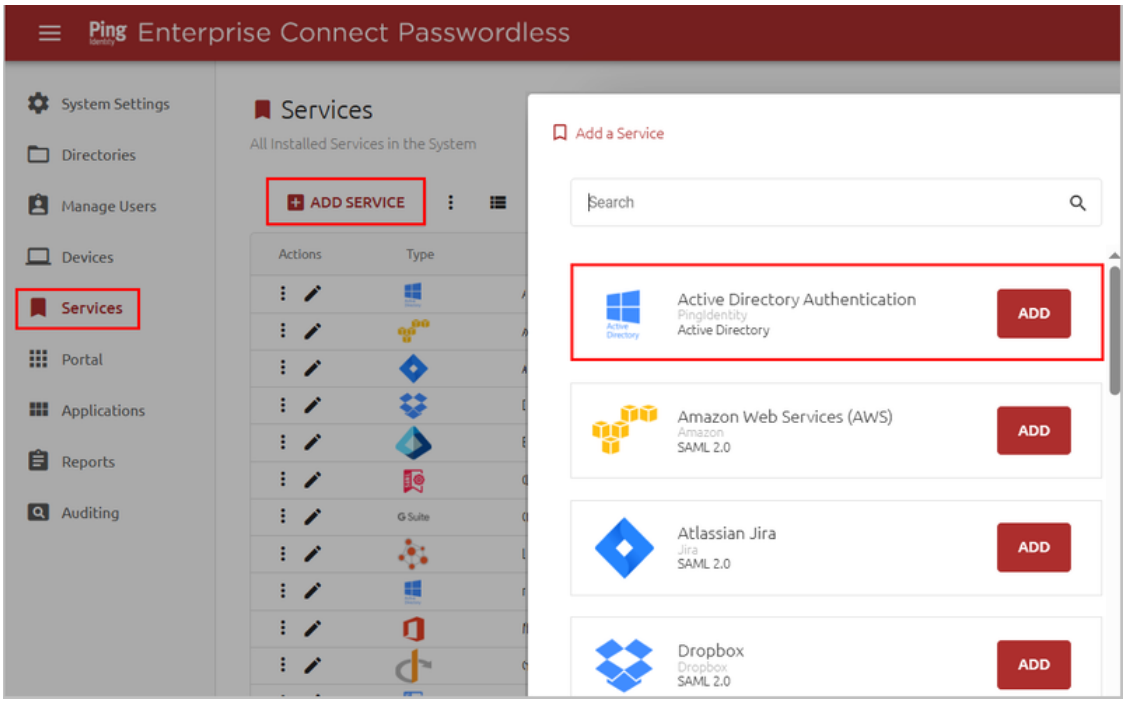
Creating the Active Directory Authentication Service

To enable installation of Enterprise Connect Passwordless for Windows, you need to create an Active Directory Authentication service in the Management Console, as described in the procedure below.

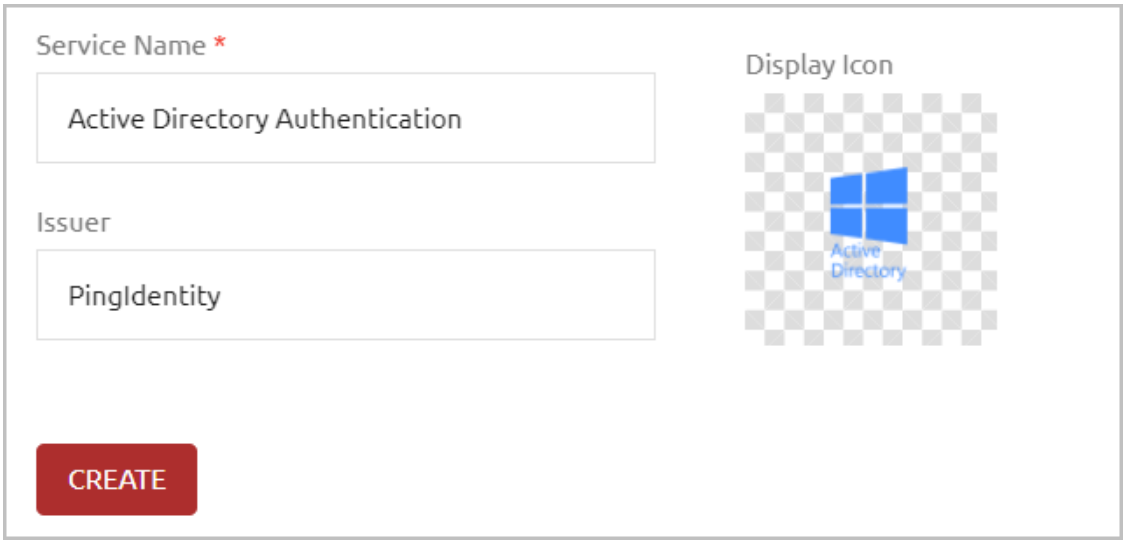
IMPORTANT: Before starting this procedure, verify that you have integrated your Corporate Active Directory or ForgeRock directory with the Management Console. Refer to the Management Console Admin Guide for detailed instructions on integrating Active Directory and other directory types.

To create the Active Directory Authentication service:

1. From the Management Console, open the **Services** menu and click **Add Service**.
2. In the **Active Directory Authentication** tile, click **Add**.



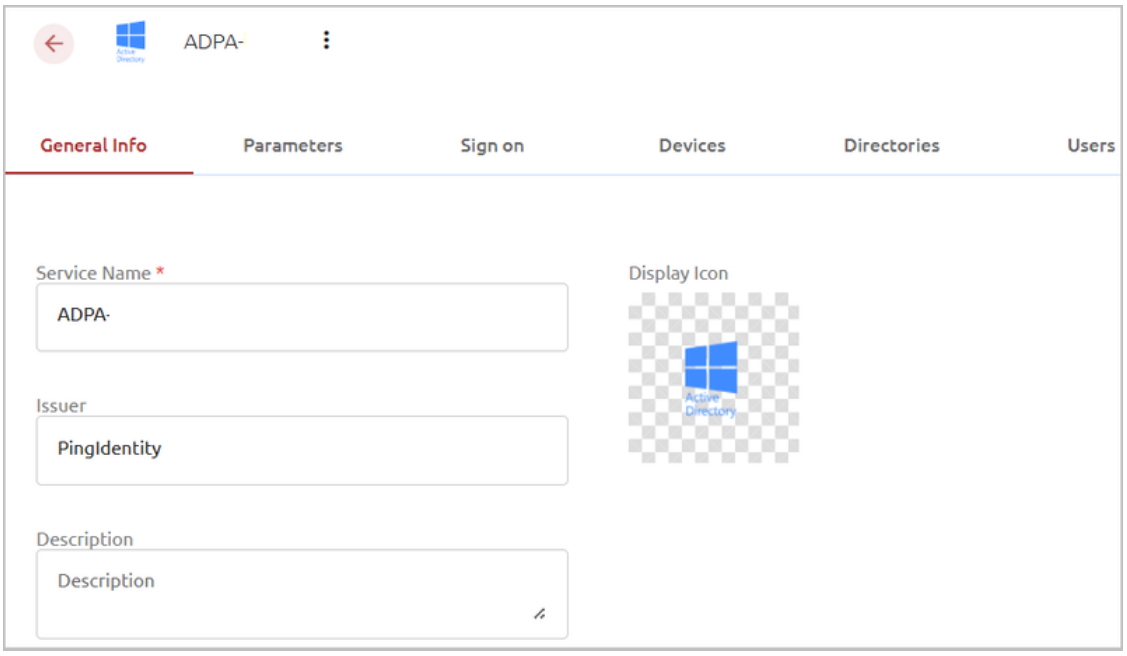
Then, in the dialog that opens, click **Create**.



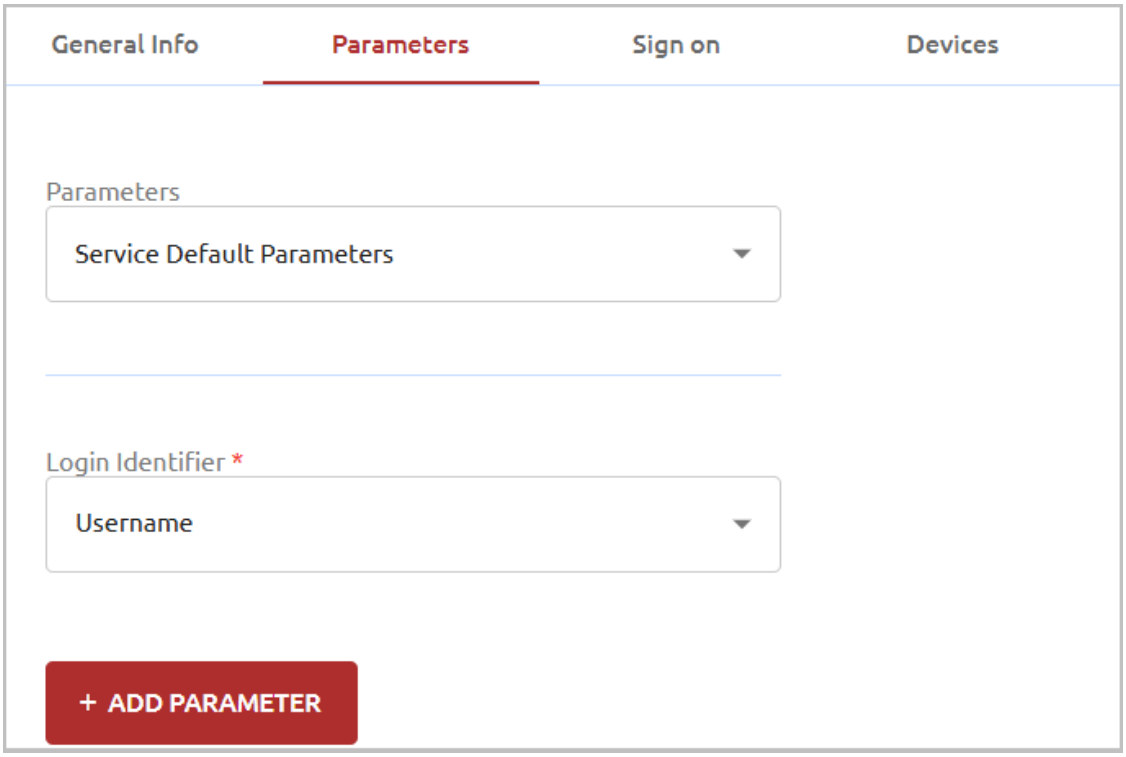
3. Review the settings in the **General Info** tab. If you make any changes, click **Save**.

Setting	Value / Notes
Service	Change the default values if desired

Setting	Value / Notes
Description	Enter a brief note about the service if desired.
Display Icon	This icon will be displayed on the Login page for the service. To change the default icon, click and upload the JPG or PNG file of your choice. Supported image size is 128x128 pixels.



4. Open the **Parameters** tab. From the **Login Identifier** dropdown list, select the credential type that will be sent by the user for the authentication (usually **Username** for AD and **UPN** for Entra ID).

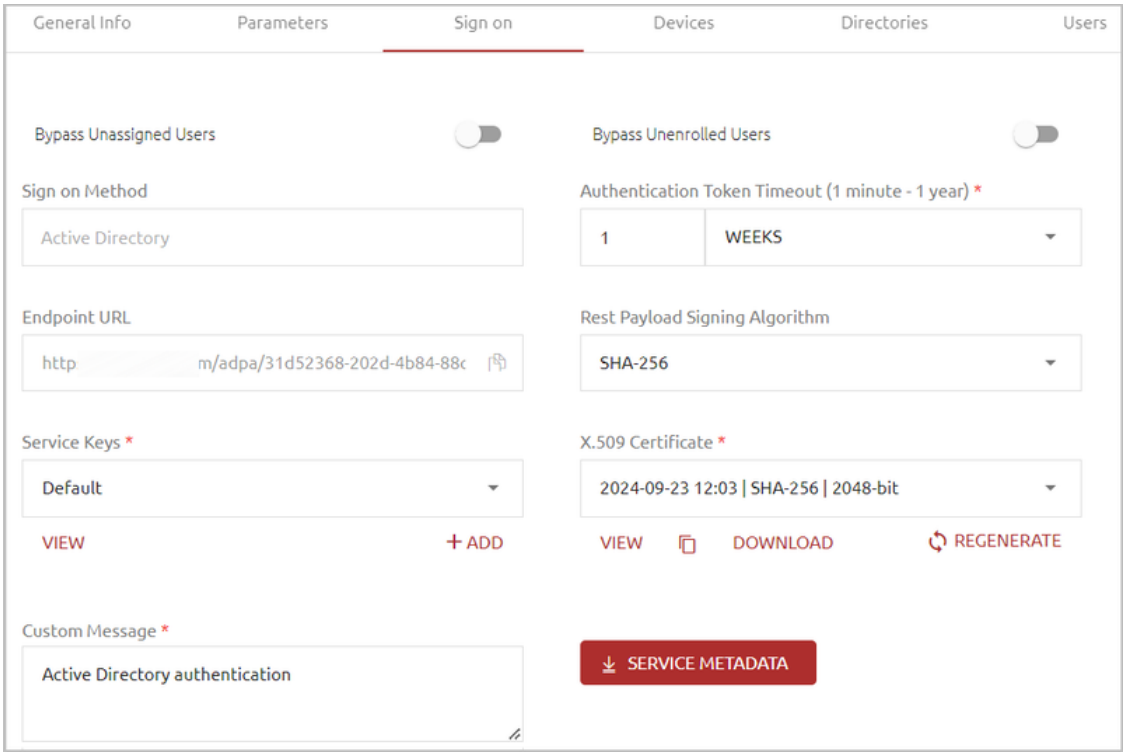


Then, click **Save**.

5. Open the **Sign on** tab and review / configure the following settings:

Setting	Value / Notes
Bypass Unassigned Users	When enabled, users who are not assigned to the service will be allowed to login with username and password (without MFA). By default, this option is disabled. The option is usually used on a temporary basis only, during gradual rollouts of Enterprise Connect Passwordless.
Bypass Unenrolled Users	When enabled, users who are known to the system but have not yet enrolled a mobile device or workstation will be allowed to login with username and password (without MFA).
Sign on Method	The authentication method used for the service (not editable).
Endpoint URL	The access URL from the Windows client to the Authentication Server (not editable). Click the Copy icon to copy the value.

Setting	Value / Notes
Service Keys	Key used by the service to authenticate via the Authentication Server. The following options are available: • Click **View** to open a popup from which you can view and copy all active service keys. • Click **Add** to create a new service key. For more information about service keys, refer to the Management Console Admin Guide.
Custom Message	Message shown to the user on successful authentication.
Authentication Token Timeout	Time period after which the authentication token becomes invalid. The value can range from one minute to one year.
Rest Payload Signing Algorithm	Signature of the generated X.509 certificate. Select **SHA-1** or **SHA-256**. **Note:** SHA-1 is not supported for Red Hat Enterprise Linux 9.3.
X.509 Certificate	The public certificate used to authenticate with Enterprise Connect Passwordless Authenticator. • Click **View** to display the content of the certificate in a popup. The popup provides both Copy and Download options. • Click **Download** to download the certificate as a .PEM file. • Click **Regenerate** to replace the certificate. You will be prompted to select the signature algorithm and size before regenerating.



6. In the lower right corner of the **Sign on** tab, click **Save** (if the button is enabled).
7. Open the **Directories** tab and select the directories that will be available for the service. Then, click **Save**.

8. Open the **Users** tab and click **Add**.

   A popup opens, with a list of directories displayed on the left.
9. For each directory, select the groups and users to be added to the service. After making your selections, click **Save** (in the upper right corner) to close the dialog.

   The groups and users you selected are listed in the **Users** tab.

10. From the toolbar at the top of the page, click **PUBLISH** and publish your changes.

Windows Client Installation with MSIUpdater

MSI is a tool that allows you to deploy Enterprise Connect Passwordless for Windows in a silent installation that can be pushed to all clients by IT. This installation type should be used for enterprise and other large-scale deployments.

The following sections present the actions required for a successful deployment with MSI:

- Installing the MSIUpdater Client
- Configuring the MSIUpdater
- MSI Deployment of Enterprise Connect Passwordless

Installing the MSIUpdater Client

The MSIUpdater client provides an update tool for basic MSI with the Corporate Enterprise Connect AD Authentication configuration. This enables MSI silent installation to corporate Windows clients.

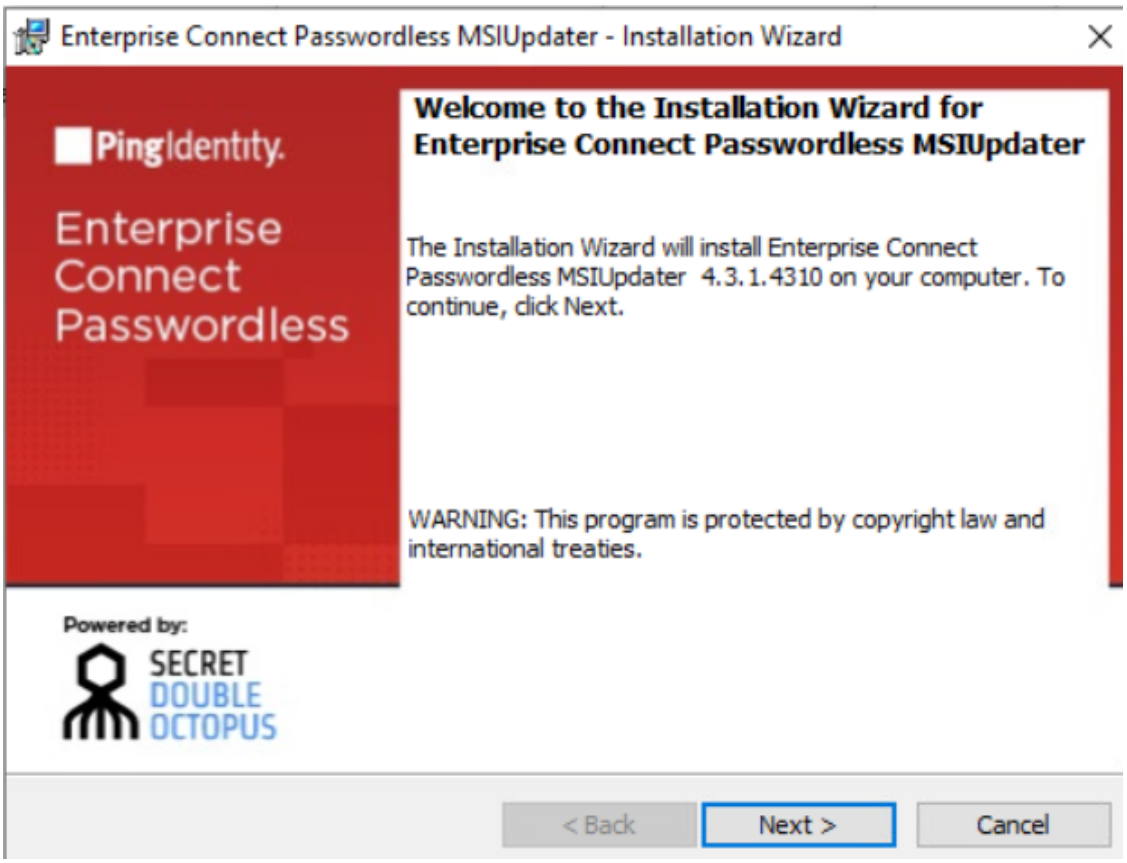
MSIUpdater can run on any Windows client running the following versions: Windows 10, Windows 11 and Windows Server 2016, 2019 and 2022.

Before beginning, verify that all system requirements and prerequisites are met. For details, refer to Prerequisites.

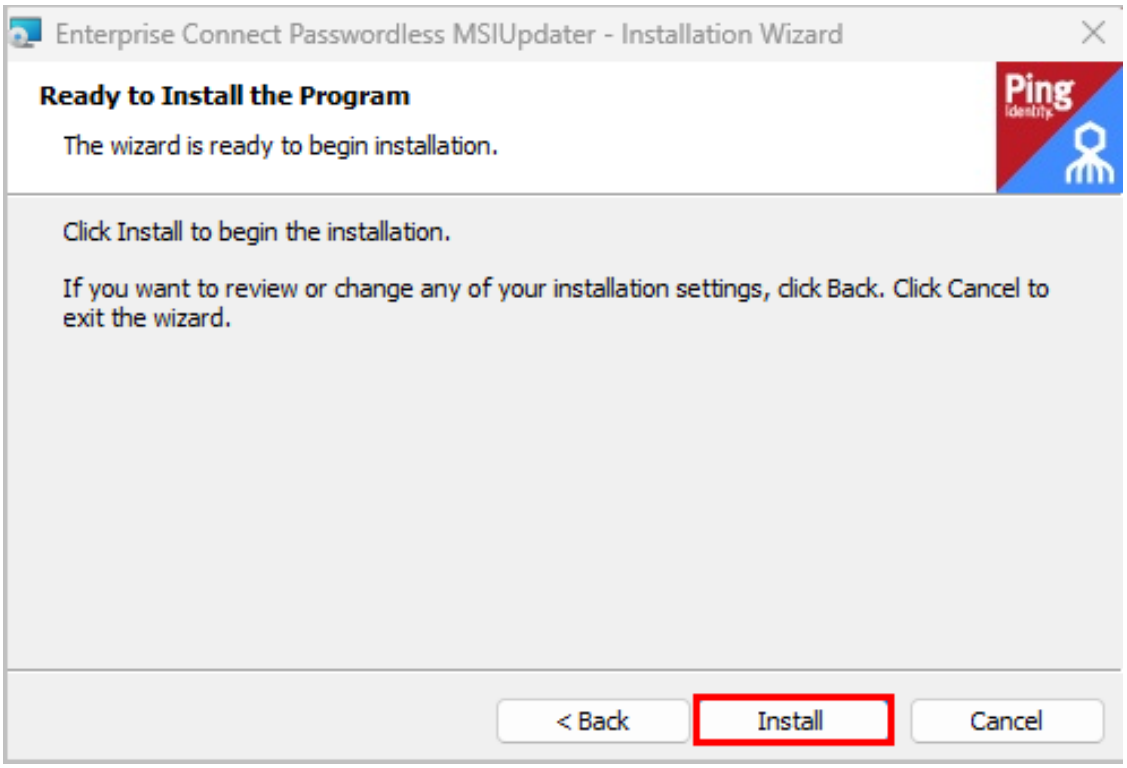
To install the MSIUpdater client:

1. Run **Enterprise Connect Passwordless MSIUpdater.exe** as Admin.
2. If the Microsoft .NET Framework is not installed, an installer opens.

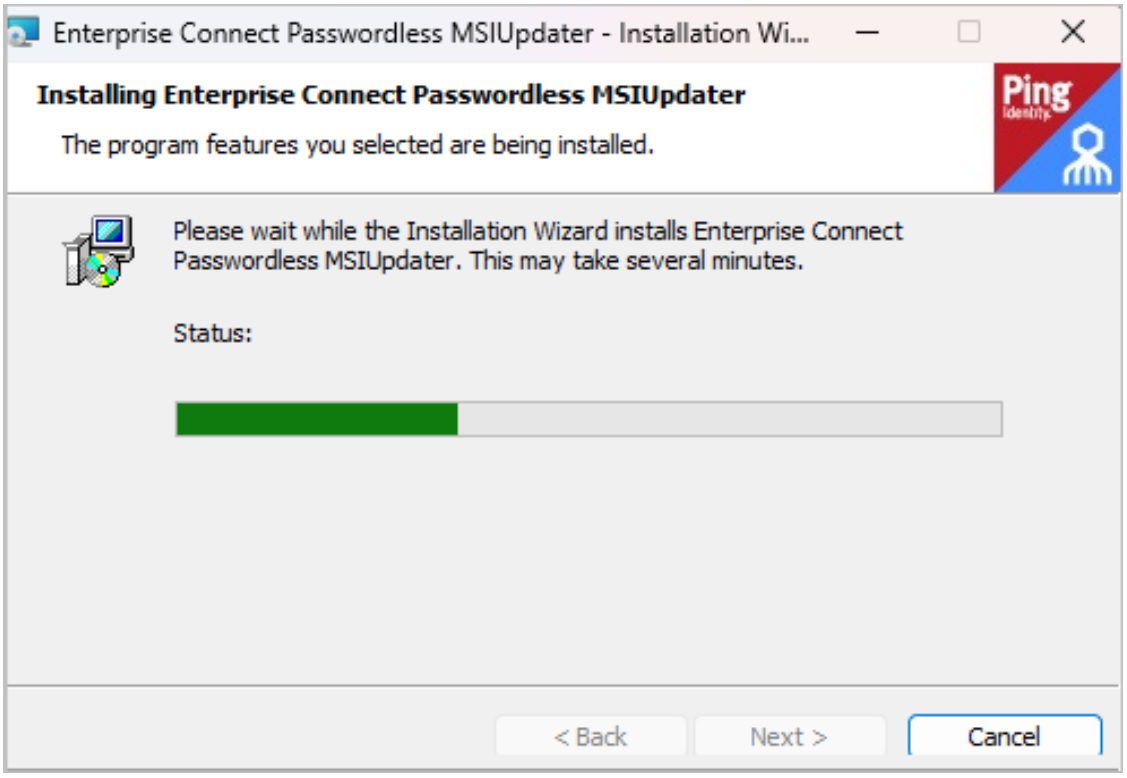
   To launch the wizard, click **Install**.
3. On the **Welcome** page, click **Next**.



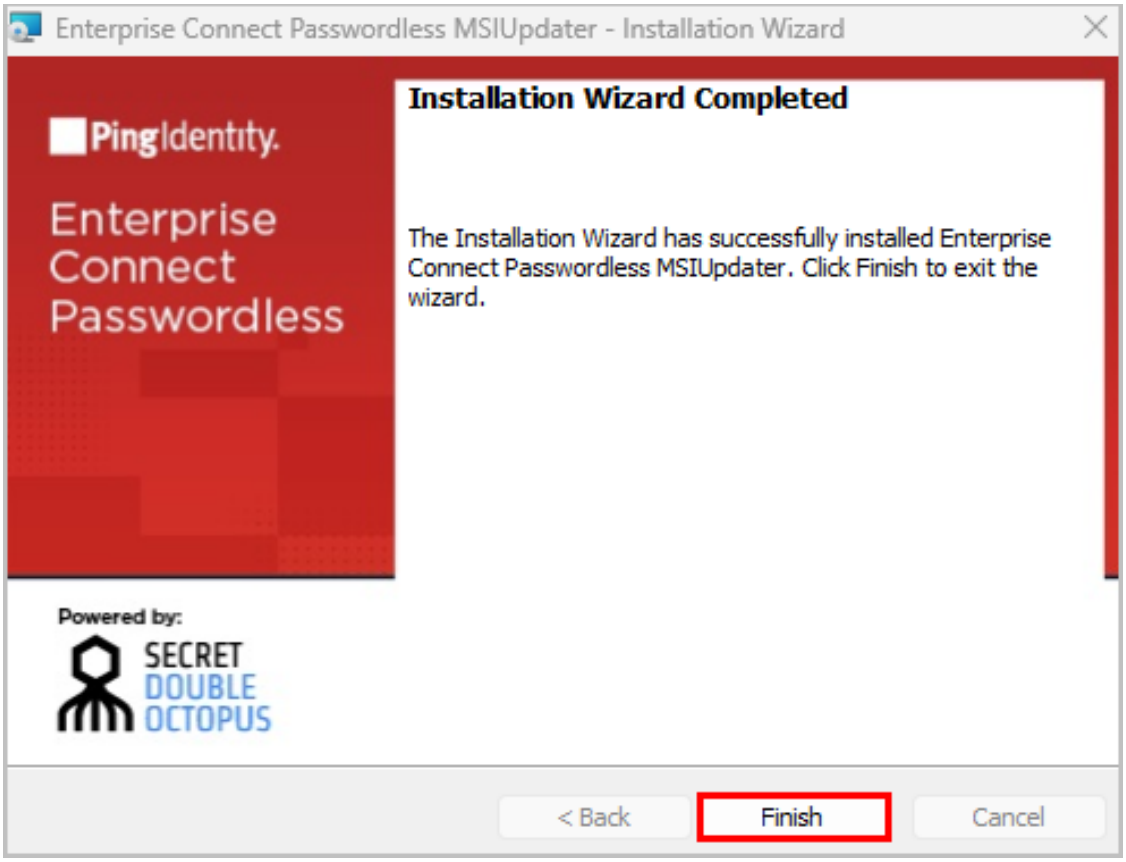
4. To start installation, click **Install**.



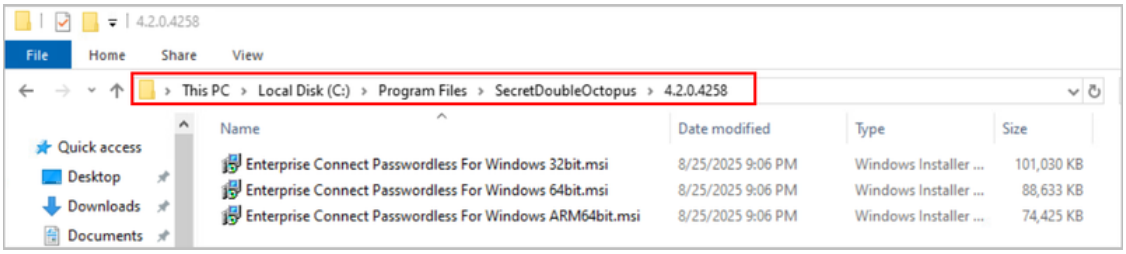
A progress bar is displayed during the installation process.



5. To exit the wizard, click **Finish**.



Upon successful installation, a folder named with the installed version number is created under **C:\Program Files\SecretDoubleOctopus**. This folder contains the **Enterprise Connect Passwordless for Windows** MSI files for 32-bit and 64-bit architecture.



When you quit the installation wizard, the MSIUpdater Client will auto launch, allowing you to configure the relevant MSI file with the corporate Active Directory Authentication Sign-on details. For more information, refer to Configuring the MSIUpdater Client.

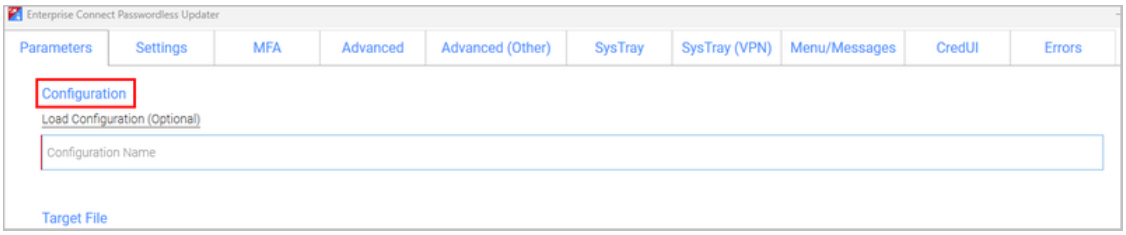
Configuring the MSIUpdater Client

The MSIUpdater, which launches automatically after you quit the MSIUpdater installer, updates the Enterprise Connect Passwordless for Windows MSI file with the corporate Active Directory Authentication Sign-On details and allows you to configure various settings related to authentication and the Windows login experience.

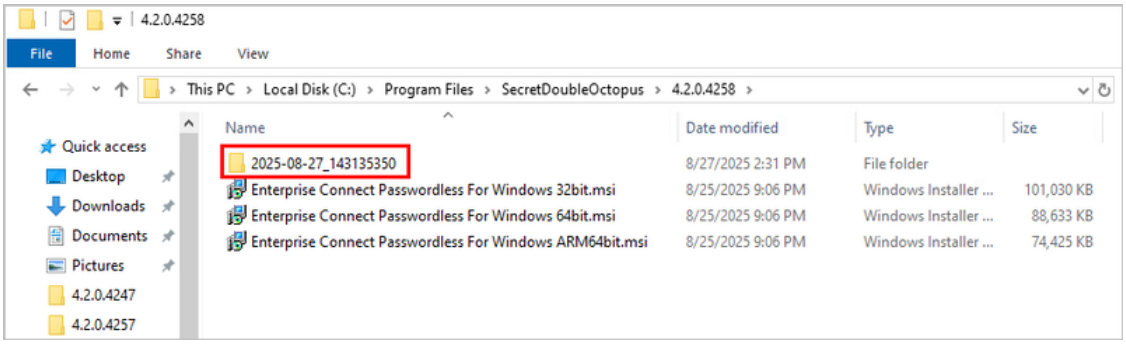
Specifying the MSI Configuration

Enterprise Connect Passwordless for Windows supports the ability to create multiple MSI configurations for the same version. This allows you to deploy a customized configuration of Enterprise Connect Passwordless for different target groups. You can create as many configurations as you need, and then use the relevant configuration for each deployment.

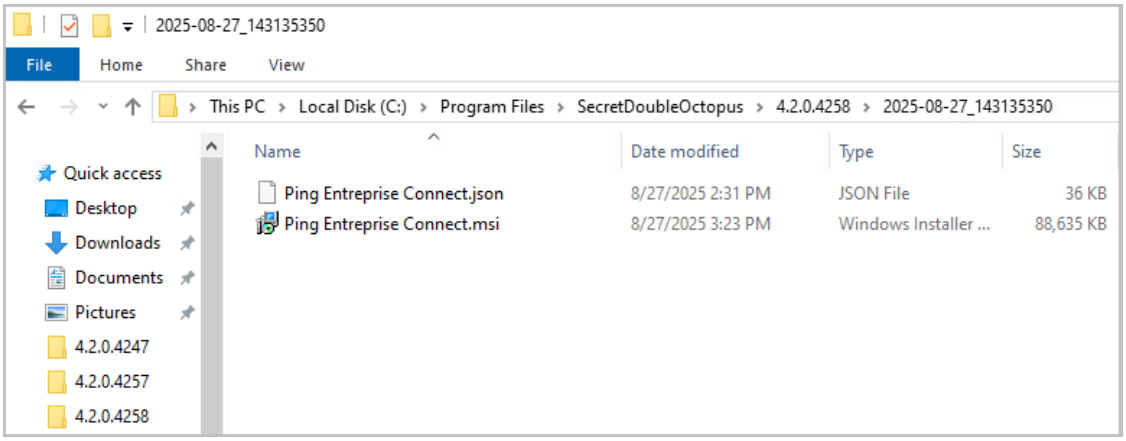
The MSI configuration is set in the **Parameters** tab of the MSIUpdater. When configuring MSIUpdater client settings for the first time, a name for the initial configuration needs to be entered in the **Configuration Name** field.



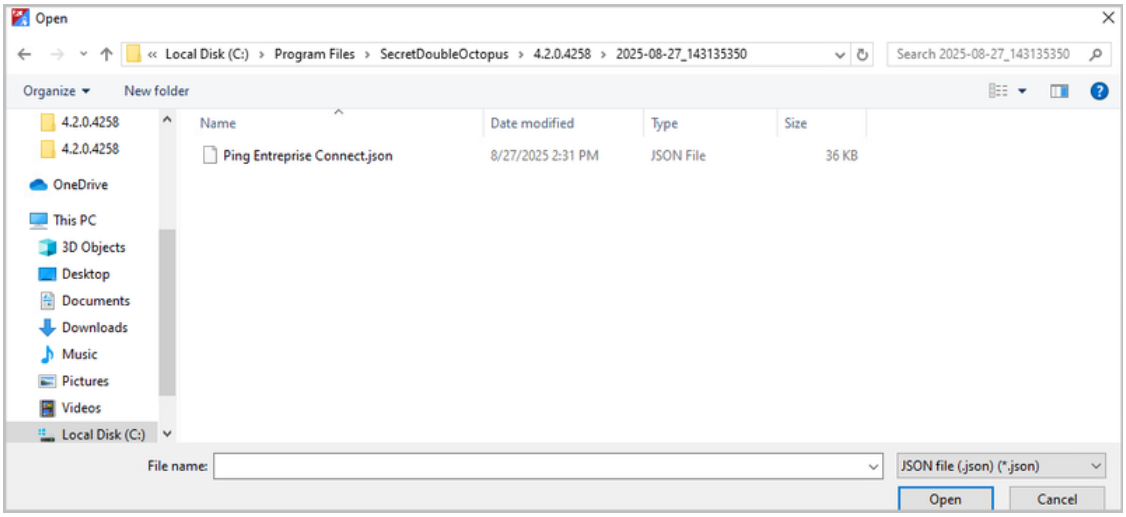
After setting the configuration and generating the updated MSI file (as explained in the procedure below), a new folder is created in the version installation folder. This folder is automatically named with the timestamp of its creation. For example:



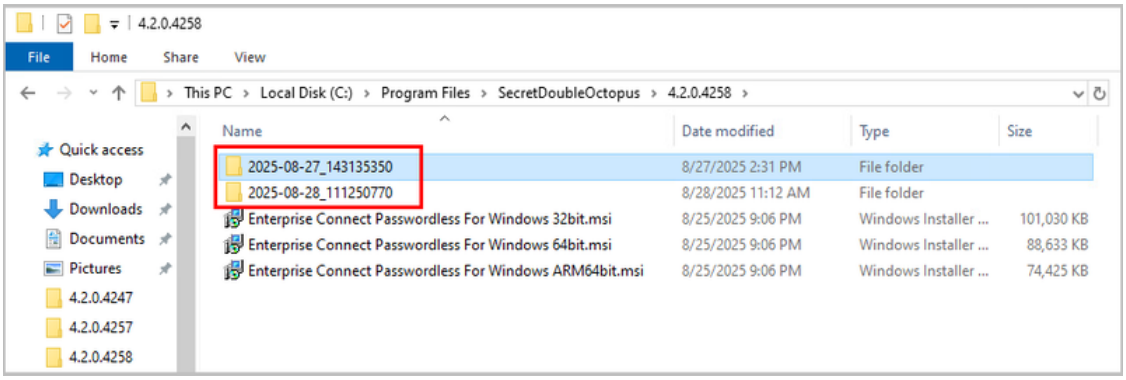
The timestamp folder contains the installation file as well as a JSON file that delineates the associated MSIUpdater configuration. Both files are named according to the **Configuration Name** that was entered in the **Parameters** tab of the MSIUpdater. For example:



To create additional configurations for the version, simply configure the MSIUpdater Client again with the required settings. If you need another configuration that is similar to one you've already created, you can click the **Load Configuration** link in the **Parameters** tab and then open the appropriate JSON file.



This loads the settings of the selected configuration into the MSIUpdater, so you can quickly make the required changes and generate the modified file. Each configuration you create is automatically saved in its own timestamped folder to maximize clarity and avoid errors.



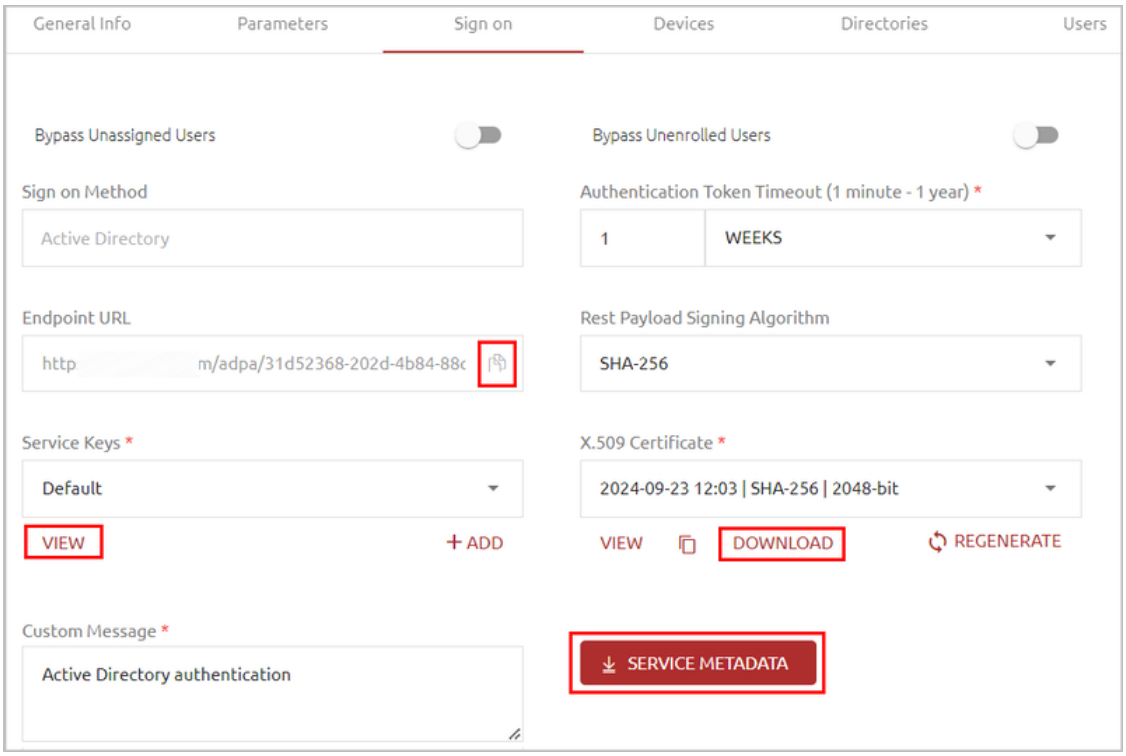
Preparing Service Settings

Before you begin working with the MSIUpdater, verify that you have access to the following elements. They can be copied or downloaded from the **Sign on** tab of the Active Directory Authentication service that you created in the Management Console.

- **Endpoint URL:** Click the Copy icon to copy the URL.
- **Service Key:** Click **View**. Then, in the popup that opens, click the Copy icon to copy the key.
- **X.509 Certificate:** Click **Download** to download the **cert.pem** file.

Alternatively**,** you can download all the service metadata at once by clicking **SERVICE METADATA**. The metadata will be saved in the **Metadata.xml** file.

> **Note**
>
> If you work with multiple client certificates, click the Browse icon on the **SERVICE METADATA** button and select the certificate to be downloaded.



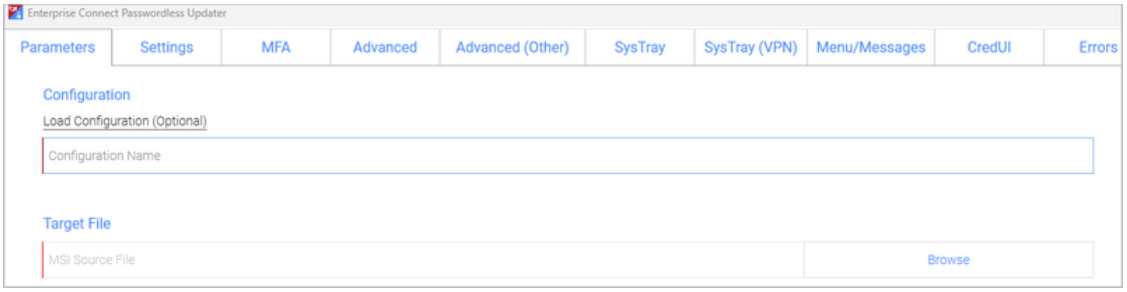
Creating the MSIUpdater Configuration

You are now ready to begin working with the MSIUpdater. Keep in mind that although the MSIUpdater tool can appear complicated, most of the options presented are not mandatory, and in general it is not necessary to change any of the default settings. The procedure below explains how to choose the settings required to set up the standard passwordless authentication flow. A few of the most commonly configured optional

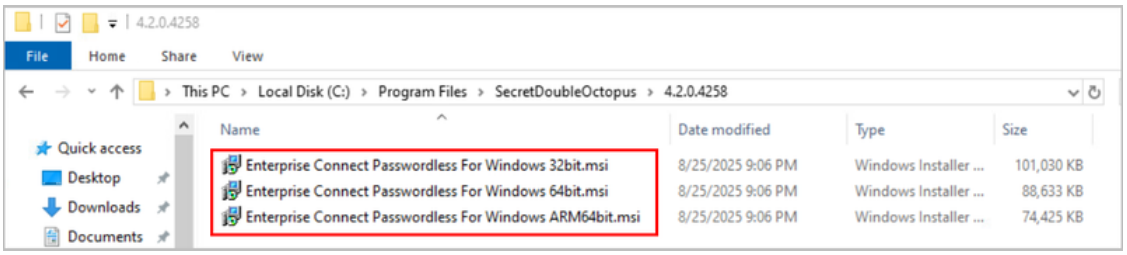
features are also presented. For details about the many additional options available, refer to Understanding MSIUpdater Advanced Settings.

To configure the MSIUpdater client:

1. At the top of the **Parameters** tab, under **Configuration**, enter a name for the new configuration. To load settings of a saved configuration, click **Load Configuration** and select the relevant JSON file. (For more details, refer to Specifying the Configuration.)



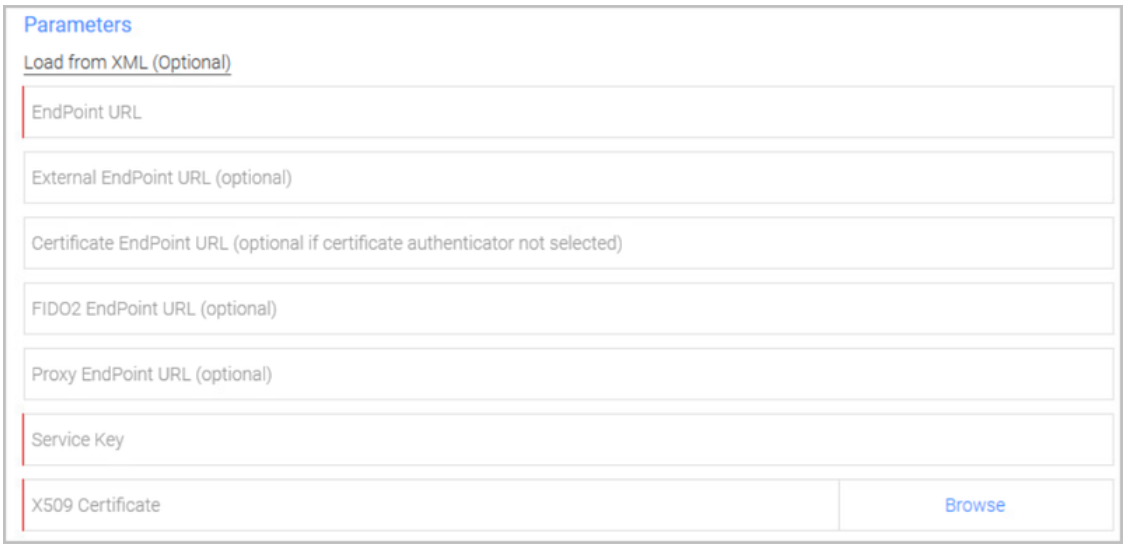
2. Under **Target File**, click **Browse** and then select the Enterprise Connect Passwordless for Windows MSI file to be updated (32bit or 64bit).



3. Under **Parameters**, configure the following mandatory parameters:

Setting	Value / Notes
EndPoint URL	The **Endpoint URL** copied from the Active Directory Authentication service.
Service Key	The **Service Key** copied from the Active Directory Authentication service.
X509 Certificate	Click **Browse** and select the downloaded X.509 certificate file.

Important: If you downloaded a **Metadata.xml** file from the Active Directory Authentication service, you can populate these settings automatically by clicking **Load from XML**. If the XML file contains a client certificate, the **Certificate Endpoint URL** field will also be populated.

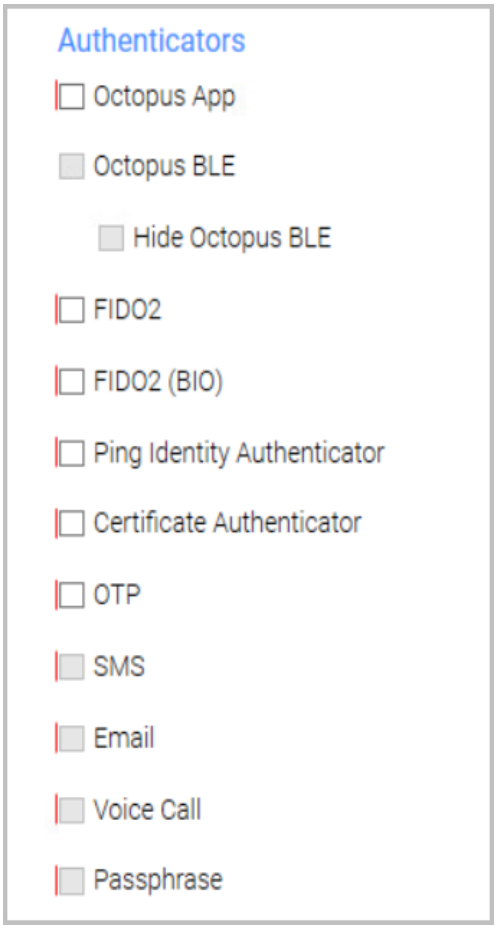


4. If relevant, enter the following optional parameter(s):
    - **External EndPoint URL:** Allows the Windows agent to access different URLs according to connection type (within the organization or outside of it). Enter the External Endpoint URL in the field.
    - **Certificate EndPoint URL:** Allows the Windows agent to access client certificates (relevant for smart card authentication). Enter the full address of the load balancer where your root certificate is stored, followed by the listening port.
    - **FIDO2 EndPoint URL:** Allows the Windows agent to access an alternate URL for FIDO enrollment.
    - **Proxy EndPoint URL:** Allows the Windows agent to connect via web proxy. You can use either a static or dynamic proxy.
        - **Static proxy:** Enter the address of the proxy server in the field.
        - **Dynamic proxy:** Enter the full address of the location where your proxy configuration file (**proxy.pac**, **wpad.dat**, etc.) is stored, followed by the listening port.
5. At the bottom of the **Parameters** tab, select at least one authenticator.

Note: To enable the **SMS**, **Email**, **Voice Call** and **Passphrase** options, open the **MFA** tab of the MSIUpdater and select the **Enable Multi-Factor Authentication** checkbox.

Authenticator	**Description / Notes**
Octopus App	Octopus Authenticator mobile app (iOS/Android)

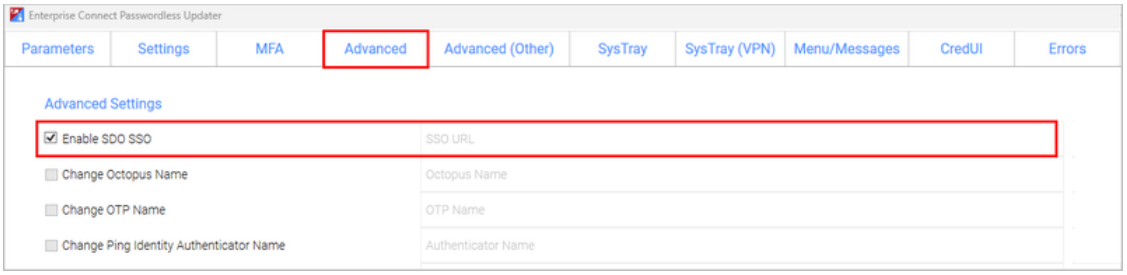
Authenticator	**Description / Notes**
Octopus BLE	Select this checkbox to enable Octopus Bluetooth authentication. (**Octopus App** must be selected to enable this option.) If you do not want the BLE option to be displayed on the Windows Login screen, select the **Hide Octopus BLE** checkbox.
FIDO2	FIDO authenticator from Yubico or Feitian
FIDO2 (BIO)	FIDO authenticator with biometric fingerprint
Ping Identity Authenticator	Select this checkbox to enable login to Windows using Ping Identity (PingID or ForgeRock) mobile authenticators.
Certificate Authenticator	Select this checkbox to enable authentication using smart cards signed by your organization's root Certificate Authority (CA). **Note:** This feature requires configuration of relevant settings in the Management Console.
OTP	Select this checkbox to enable authentication with Ping Identity OTP, hardware OTP tokens, or or Octopus-generated OTP.
SMS	Select this checkbox to enable authentication with OTP over SMS.
Email	Select this checkbox to enable authentication with OTP over email.
Voice Call	Select this checkbox to enable two-factor authentication over voicecall.
Passphrase	Select this checkbox to enable two-factor authentication with a user-selected passphrase.



Important: If you configured an External Endpoint URL (in Step 4), users will need to enroll FIDO devices using the **internal** URL only. Following enrollment, they may authenticate using either the internal or external URL.

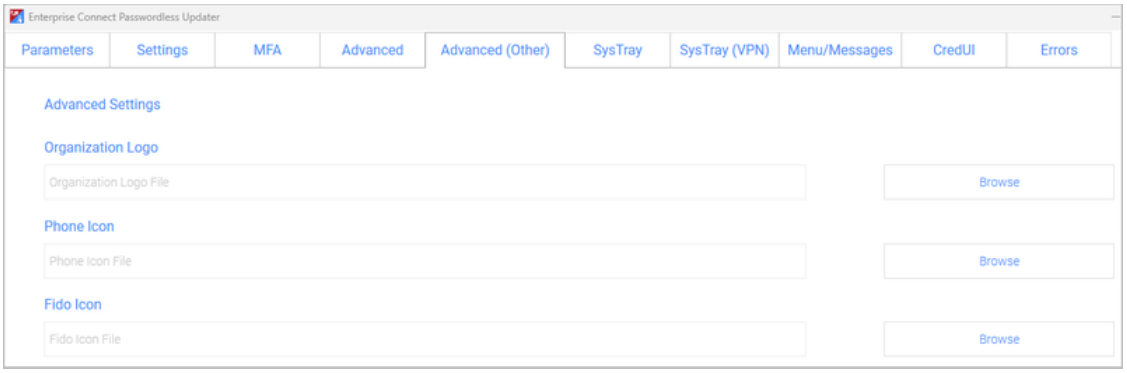
6. If desired, configure single sign-on to the User Portal:

   At the top of the **Advanced** tab, select the **Enable SDO SSO** checkbox. Then, enter the URL of the User Portal in the field to the right.



In runtime, the portal will open in the default browser. Users will be automatically logged in and be able to view all assigned services.

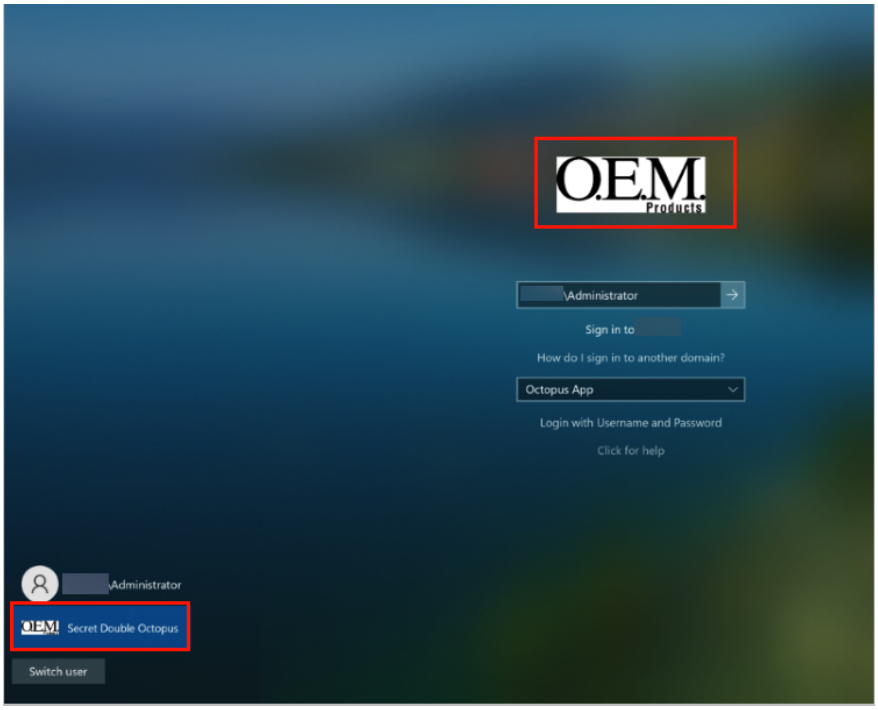
7. Optionally, use the features at the top of the **Advanced (Other)** tab to customize the Windows login experience by replacing the default logo and icons with your own images.



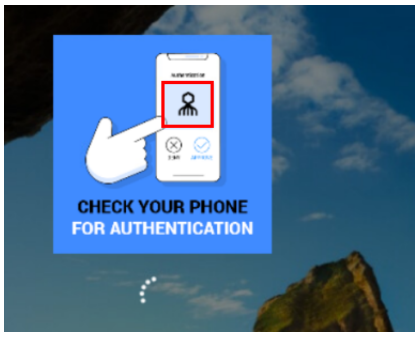
IMPORTANT: The images must be 448x448, in 24-bit BMP format. For Windows Servers, the images must be 448x448, in 16-bit BMP format.

The following options are available:

- **Organization Logo:** Displays your company's logo on the Windows Login screen instead of the default Enterprise Connect Passwordless logo. For example:



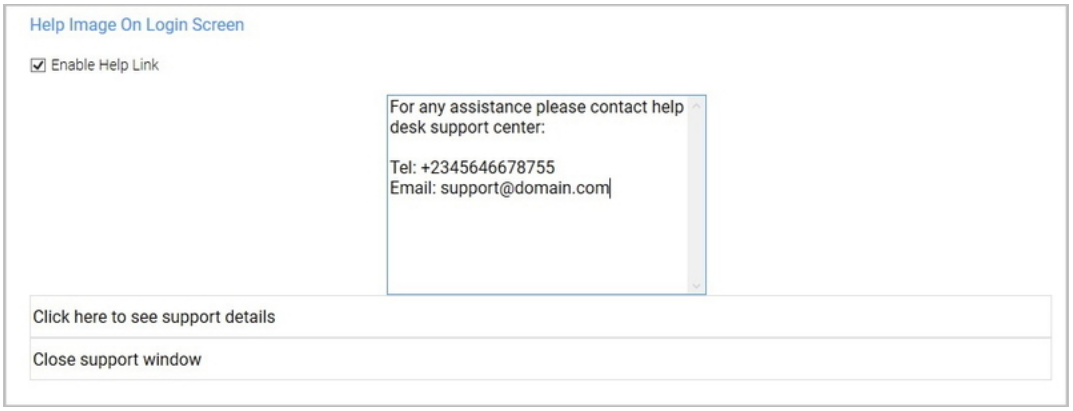
- **Phone Icon:** Displays the icon of your choice on the **Check Your Phone** prompt instead of the default Enterprise Connect Passwordless icon.



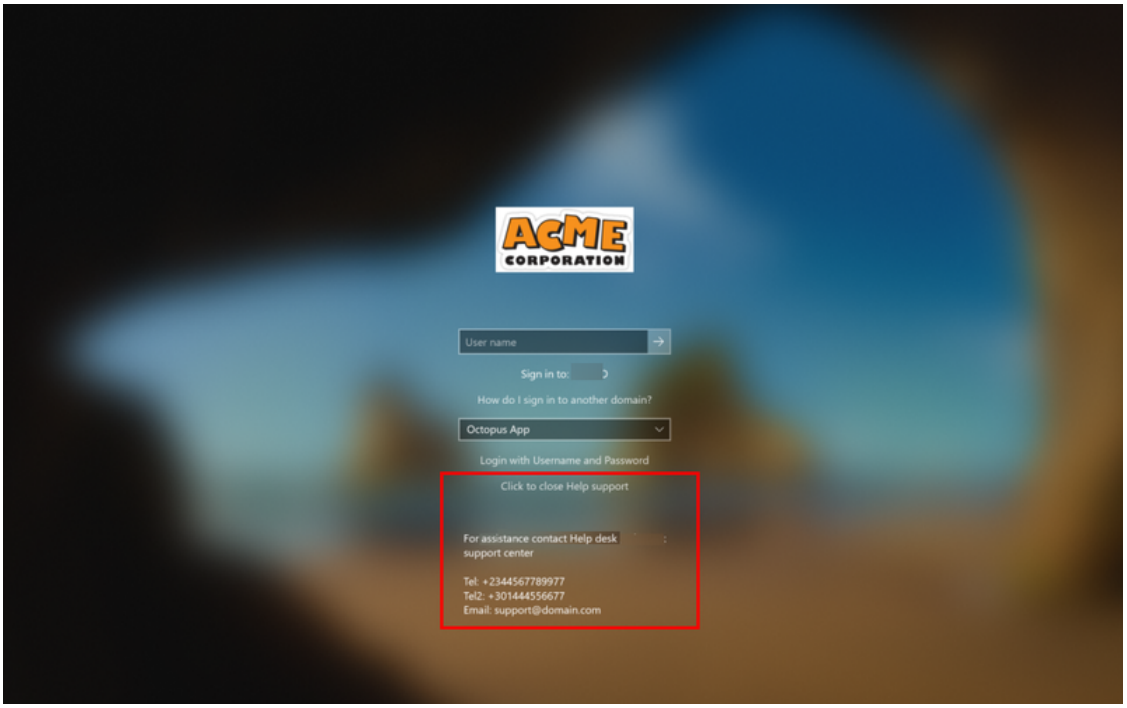
- **Fido Icon:** Displays the icon of your choice on the prompt to touch the Fido key.

8. To display support resources on the Windows Login screen, select the **Enable Help Link** checkbox. Then complete the following free text fields:
    - **Help Message:** Instructions about how to obtain assistance
    - **Open Help Message Text:** Prompt for showing the Help Message
    - **Close Help Message Text:** Prompt for hiding the Help Message

    For example:

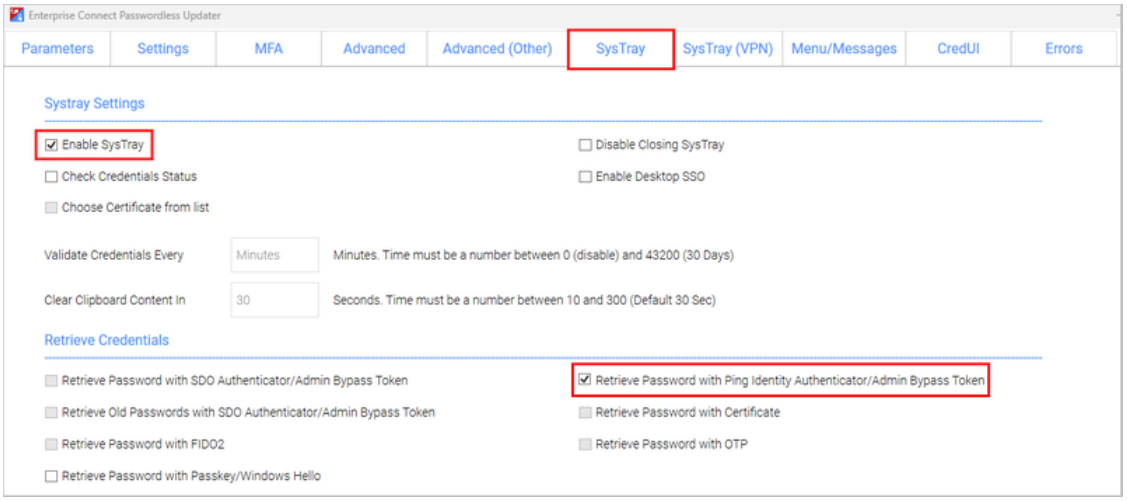


    In runtime, users will be able to open, view and close the Help Message.



9. If desired, configure the ability for users to copy the AD password from the Windows systray:

   At the top of the **Systray** tab, select the **Enable SysTray** checkbox. Then, under **Retrieve Credentials**, select the **Retrieve Password with Ping Identity Authenticator/Admin Bypass Token** checkbox.



   In runtime, users will be able to view and copy the AD password after performing authentication on the PingID or ForgeRock mobile authenticator. Admin users in Bypass mode will need to enter the temporary token to retrieve the password. (For more information about Bypass mode, refer to the Management Console Admin Guide.)

Important

If you enable the systray, it is strongly recommended to follow the best practice of disabling Microsoft Office Clipboard to prevent sensitive data from being exposed.

10. Select the **Errors** tab. At the bottom of the tab, click **Apply**.

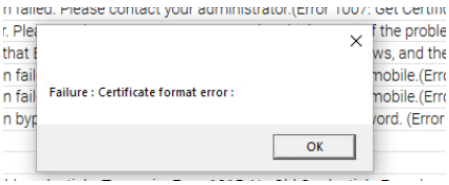
    A new JSON file and MSI file are created and stored in a folder named with the timestamp of creation. The files are named according to the **Configuration Name** assigned in the MSIUpdater. Verification messages are displayed upon creation of each of the files. Click **OK** to close these popups.

Troubleshooting Tips

- If one or more mandatory settings are missing from the MSIUpdater client, the **Apply** button will be disabled. Hover over the button to view a list of the missing settings. For example:

  After correcting the settings, the **Apply** button is enabled, and a **No errors** tooltip is displayed.

- If you receive a Certificate Format error (as shown below), download the service metadata again (Preparing Service Settings) using any browser **except Firefox**. If the error continues to be generated, please contact our support team.



Understanding MSIUpdater Advanced Settings

The MSIUpdater client offers a very extensive selection of options for configuring and controlling various aspects of the authentication flow. However, the vast majority of these options are not mandatory, and some are not even relevant for most customers (as they were designed to accommodate specific organizational requirements). The following sections (organized according to the tabs of the MSIUpdater tool) can be used as a reference to familiarize yourself with the optional features provided in the MSIUpdater.

- Settings tab: Contains a variety of miscellaneous options, mainly related to login flow configuration, security settings and troubleshooting features (e.g., logging)

- MFA tab: Contains settings related to setup of multi-factor authentication
- Advanced tab: Contains settings that control presentation of the authentication options and other features displayed on the Windows Login screen
- Systray tab: Allows you to select which self-service actions will be available to users from the Windows systray
- Menu/Messages tab: Enables you to customize the text of actions / messages displayed to users in the Windows systray
- CredUI tab: Allows you to select scenarios in which Enterprise Connect Passwordless authentication is bypassed and users need to login with username and password
- Errors tab: Enables you to customize the text of error messages displayed to users

Settings Tab Options

This tab contains numerous options, mostly relating to login flow, security features and troubleshooting. Enable the settings as required by selecting the relevant checkboxes.

For convenience, settings are divided into relevant categories. The settings are:

Setting	Description / Notes
General Settings	
Show Default Credential Providers	Determines whether Windows default credential providers (Windows and Active Directory) are displayed when logging into Windows.

Setting	Description / Notes
Change Password on Unlock	When selected, password changes are allowed on Unlock as well as on Login to the workstation. This option is relevant for Passwordless only.
Skip User Interface when Unlocking Workstation	Determines whether there is Auto Login for AD users from the Lock screen. When the setting is enabled, AD users receive a push notification from the PingID mobile authenticator immediately after pressing **<Ctrl> <Alt> <Del>**.
Use Last Username on Logon	When selected, the username of the user who logged in most recently is saved and automatically presented for the next login.
Enforce MFA	When selected, users must authenticate with mobile (2nd factor) when using domain username and password. This setting is not relevant for FIDO users.
Change Password on RDP	When selected, password changes on RDP sessions are allowed. This option, which is relevant for Passwordless only, is used mainly for admin users using RDP sessions that do not login to Windows machines.
Local User Support	When selected, Enterprise Connect Passwordless for Windows will be enabled for Local users and will verify that the Local user matches the mapping with the Authentication Server user. **Note: This setting is relevant for non-domain users only**.
POC Mode	When selected, Enterprise Connect Passwordless for Windows will not check the certificate with the server. This setting is used mainly for POC, when using a self-signed certificate on the Authentication Server.
Password Free Experience	Select this checkbox to enable a Passwordless authentication experience for MFA users. When selected, users are required to provide a password for the first authentication. Subsequent authentications will be Passwordless, until the password is changed. **Note: To use this feature, the Enforce MFA checkbox must also be selected**. For more details about this feature and its configuration, refer to Enabling the Password Free Experience.
Enable Trace	Select this checkbox to enable the logs by default immediately after installation.
Do Not Launch SSO Portal on Login	When selected, the User Portal is not automatically opened after login.

Setting	Description / Notes
Demand AD Password Change when Password Expired or Account Locked	When selected, the Windows Agent sends a password reset request to the Authentication Server if the password has expired / is due to expire, or if the user's account is locked. The user must then approve an additional strong authentication request in order to successfully login. **Important** This feature requires that the **Automatic Password Sync** toggle in the settings of the relevant directory in the Management Console be enabled. (This toggle is enabled by default.)
Hide Login with Username and Password Link	When selected, the **Login with Username and Password** option does not appear on the Windows Login screen.
Start BLE Automatically	In default system operation, BLE on the workstation starts upon a BLE login attempt, even when BLE was previously turned off by the user. To prevent BLE from starting under these circumstances, make sure that the **Start BLE Automatically** checkbox is cleared.
Support VDI Gold Image	Select this checkbox to enable deployment of Enterprise Connect Passwordless when utilizing a VDI golden image.
Do not Display Full Username on Unlock Screen	When selected, the full name of the Login User is hidden on the Unlock screen.
TLS Min Version	This setting is enabled when the **Use Synchronous HTTPS** checkbox is selected. The default selection is **TLS 1.2**. Select **TLS 1.3** to enforce a higher level of security. Note that if you select **TLS 1.3**, users will not be able to authentication to workstations running versions lower than 1.3.
Bypass from NLA Login	When selected, users who are members of the Bypass Group(s) will not require authentication when using NLA login. For more information, refer to Configuring NLA Login Bypass.
Bypass from NLA Login Using Push	This setting is available when the **Bypass from NLA Login** checkbox is selected. When selected, members of the Bypass Group(s) will not be presented with the Login screen, but they will need to authenticate via push notification.

Setting	Description / Notes
Wait for Password Sync	This setting is relevant when the Windows Agent detects a password mismatch and sends a password reset request to the Authentication Server. The setting determines how many seconds the Agent waits before sending a second request to the Server in the event that no response is received. If the second request also receives no response, no additional requests are sent and authentication fails.
Force Lock After Offline	When selected, workstations of users working offline are automatically locked when they go back online, to force users to perform online authentication.
TPM Support	If TPM 2.0 is enabled, selecting this option allows TPM to store the private key for BLE password encryption.
Force CAD on Reboot	When selected, users must press **Ctrl + Alt + Del** upon system reboot only. In other scenarios (e.g., to unlock the machine), the CAD action is done automatically.
Use Other Credential Provider as Default	When selected, the standard Windows credential provider is displayed on the Login screen as the default authentication option.
Legacy Server Support	Select this checkbox only when recommended by the Ping Identity support team, to enable backward compatibility with Authentication Server version 5.4.4.
DirectAccess Support	Select this checkbox to enable support of the DirectAccess VPN.
Network LogonUser	Select this checkbox to use an alternate Windows API in certain rare circumstances. (Contact the support team for details.)
Bypass Credentials Check	When selected, an alternate Windows API will be used in the event of rare timeout issues in password-free mode.
Wrap Check Point Credential Provider	Select this checkbox to enable Enterprise Connect Passwordless Authenticator to work together with the Check Point Full Disk Encryption credential provider.
Do not Check Credentials Before RDP	This setting is relevant for handling Event Viewer issues on very specific workstations. Select the checkbox only when recommended by the Ping Identity support team.
Bypass Enterprise Connect Passwordless for Login	When selected, the Enterprise Connect Passwordless option is hidden on the Windows Login screen. (Only the default credential provider is displayed.)

Setting	Description / Notes
Allow BLE under Defender and Intune restrictions	When selected, Windows Defender and Microsoft Intune are automatically configured to allow BLE.
Use Last Username on Unlock	When selected (default setting), the username of the user who logged in most recently is automatically presented on the Unlock screen and cannot be changed to a different user. If the checkbox is cleared, the functionality is set according to default Microsoft behavior.
Support Windows Hello for Business	When selected, users are able to perform various Systray actions using the Windows Hello sign-in configured for their workstations. For details, refer to Configuring Windows Hello Support for Systray Actions.
Shared Account Settings	
Shared Account Support	When selected, the Windows Agent is able to handle authentication of multiple users to a single generic shared account. This configuration is useful when groups of personnel (such as IT, DevOps, manufacturing floor workers, etc.) use a shared workstation. For more details about this feature and its setup, refer to Enabling Shared Account Login.
Allow Switching Between Shared and Regular Accounts	When selected, the Windows Login screen will support both the shared account login flow and the standard authentication flow (to a non-shared account). This setting is enabled only when the **Shared Account Support** checkbox is selected.
Use Regular Account as Default in Shared Account Enabled	When selected, the standard authentication flow (to a non-shared account) is displayed on the Windows Login screen initially by default. However, if the last login / unlock was to a shared account, the shared account login flow continues to be displayed for the next login / unlock, unless the **Fallback to Regular Account with Shared Account Enabled** checkbox is also selected.

Setting	Description / Notes
Fallback to Regular Account with Shared Account Enabled	When selected, the Windows Login display always returns to the standard (regular account) login flow, even when the last login / unlock was to a shared account. Note that the *initial* display will show the shared account flow, unless the **Use Regular Account as Default in Shared Account Enable d** checkbox is also selected. **Important** Fallback behavior is activated by clicking the **Remove Shared Account** link. (The link needs to be clicked only once to enable regular account fallback.) If you want the standard login flow to always be displayed, we recommend selecting all the checkboxes in the Shared Account Settings.
Do not Save Last Account Name	When selected, the username of the guest user who most recently accessed the shared account will be hidden on the Login and Unlock screens. (Guest users will need to enter a username every time they access the account.)
FIDO Settings	
FIDO2 User Presence Required	When selected (default setting) , FIDO2 users are required to touch the token after entering their PIN. To disable this requirement, verify that the checkbox is NOT selected. This checkbox is enabled only when the **FIDO2** authenticator is selected in the **Parameters** tab. **Important** This feature requires configuration of relevant settings in the Management Console.
Allow Use of FIDO2 (PIN) with FIDO2 (BIO)	By default, if fingerprint identification fails for three consecutive attempts, users are prompted to authenticate using a PIN code. If you do not want the PIN option to be presented after biometric failure, make sure this checkbox is **NOT** selected.
Use FIDO2 without Username	When selected, users authenticating with an enrolled FIDO token will be able to perform login without entering a username.

Setting	Description / Notes
Automatically Lock on Removing FIDO Key	When selected, the workstation becomes locked when the FIDO token used for the most recent login or unlock is taken out or dislodged. If a FIDO key *not* used for the last login / unlock is removed, or if the last login / unlock was done with an authentication method other than FIDO, the workstation will not be locked.
Automatically Unlock on Inserting FIDO Key	When selected and a FIDO token is inserted, the **CTRL + ALT + DEL** flow is skipped, and users are immediately prompted to use the FIDO key to unlock the workstation. **IMPORTANT:** The flow described takes place only when the most recent login was done using FIDO authentication. If a different method was used for the last login, the **CTRL + ALT + DEL** flow is skipped, and users then need to choose an option from the list of authentication methods.
Reattempt authentication using other enrolled devices	When selected, and the inserted token fails authentication, the system automatically tries to authenticate against additional keys with which the user is enrolled.
Certificate Settings	
Use Certificate without Username	When selected, users authenticating with an integrated smart card will be able to perform login without entering a username.
Get Username from Certificate	When selected, the **Username** field on the Login screen is populated automatically with the username associated with a selected certificate (relevant for shared accounts).
Certificate Offline using RSA PCKS1	This setting is required for certain smart card configurations. Select the checkbox when advised by the Enterprise Connect Passwordless support team.
Entra ID Settings	
Entra ID AD Joined Machine	Select this checkbox when the workstations are configured to connect with the Entra ID AD domain. When the setting is selected, users will be prompted to login with UPN and not Username.
Support AD joined RDP on Entra ID joined	When selected, Entra ID joined machines are able to connect to RDPs outside of the Entra ID domain. This setting is enabled only when the **Entra ID Joined Machine** checkbox is selected.

Configuring NLA Login Bypass

When the **Bypass from NLA Login** checkbox is selected, users who are members of the specified bypass group(s) will not be required to authenticate when establishing a remote session. If the second checkbox is selected as well, members of the bypass group(s) will need to authenticate via push notification, but they will not need to enter credentials on a Login screen.

To configure NLA login bypass:

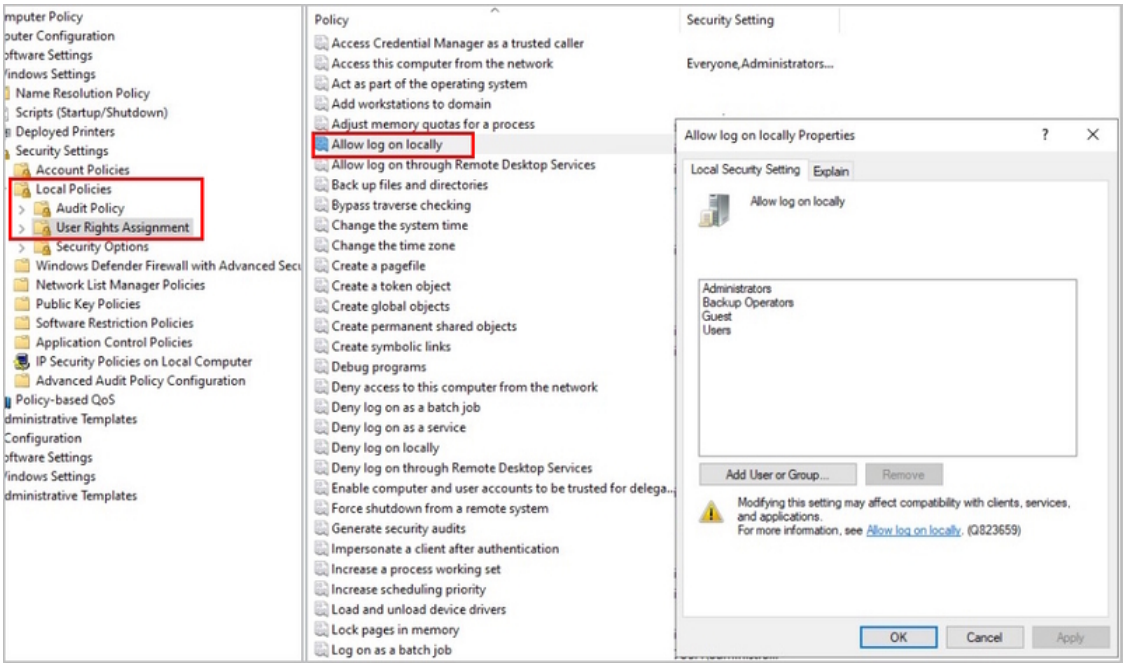
1. Select the **Bypass from NLA Login** checkbox, and enter the group name(s) in the required syntax in the field to the right.

   If relevant, select the **Bypass from NLA Login using Push** checkbox.

2. After the Windows Agent is successfully installed, grant local access permissions to members of the bypass groups:

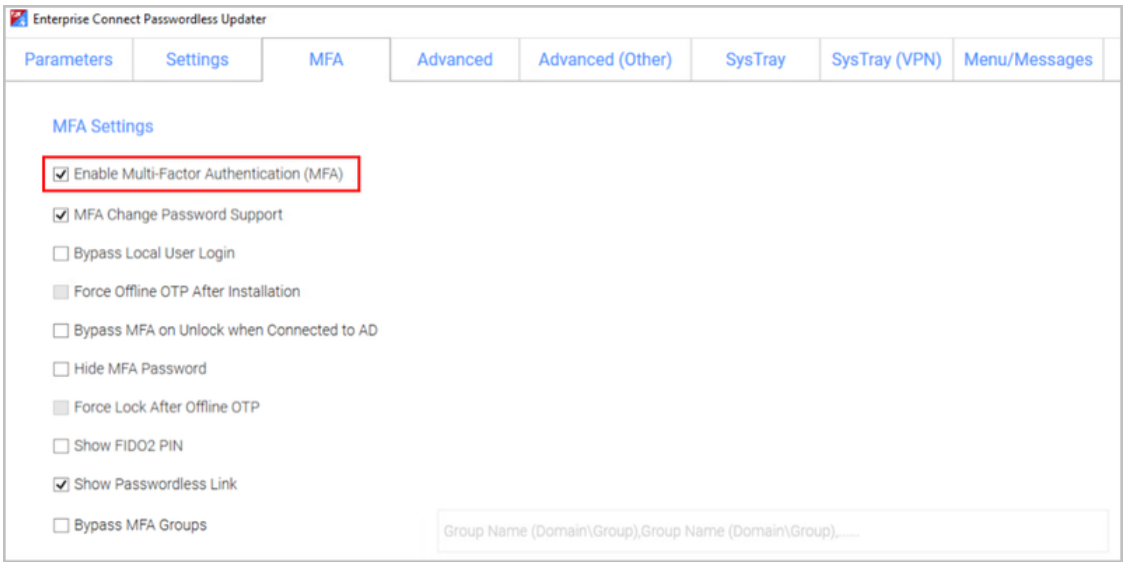
   a. In the Active Directory, navigate to **Security Settings > Local Policies > User Rights Assignment**, and select the **Allow log on locally** policy.

   b. In the dialog that opens, add the relevant groups to the policy.



MFA Settings

When multi-factor authentication (MFA) is enabled, users need to enter their AD passwords in order to receive a push notification from the PingID or ForgeRock mobile authenticator. If you want to use MFA for logging into Windows, select the **Enable Multi-Factor Authentication (MFA)** checkbox. (When the checkbox is not selected, Windows login will be Passwordless.)



When MFA is activated, you may enable the following options as required by selecting the relevant checkboxes:

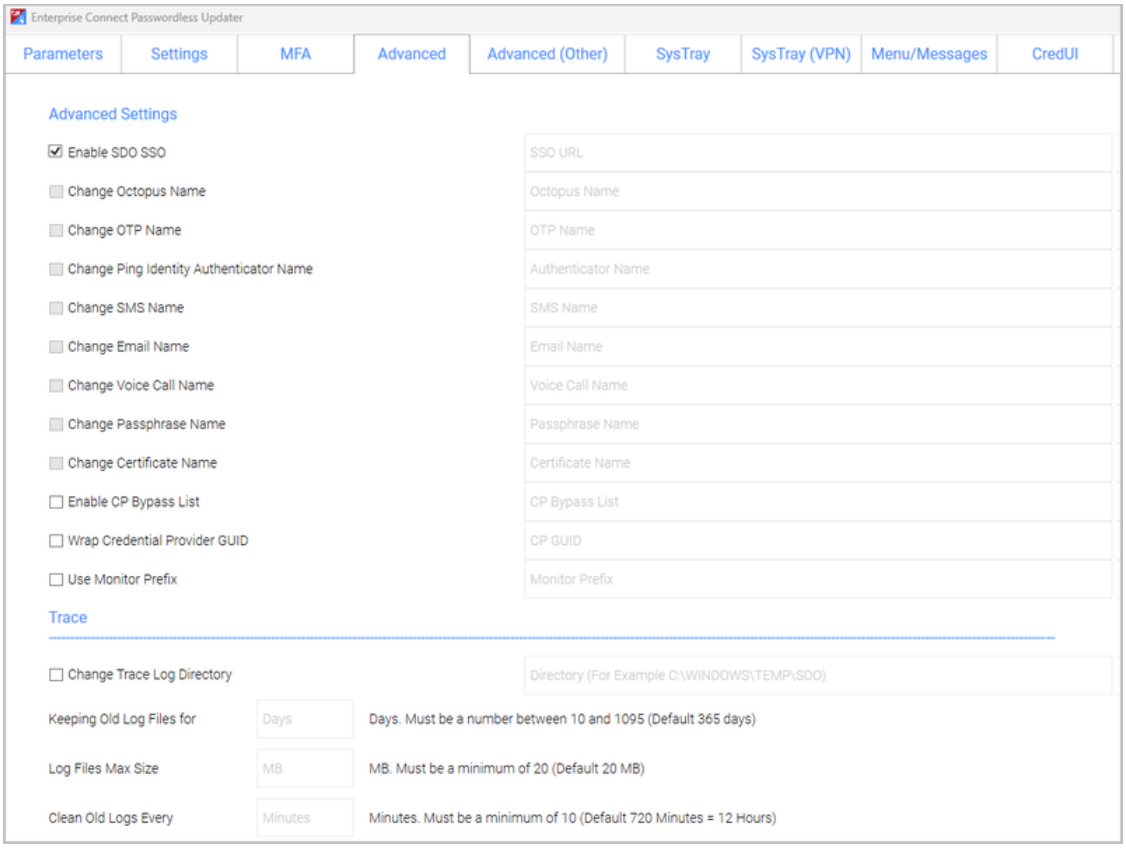
Setting	Description / Notes
MFA Change Password Support	When selected, users are able to change the password on the Windows workstation without the Enterprise Connect Passwordless credential provider (CP) intercepting the process. When the checkbox is cleared, the Enterprise Connect Passwordless CP controls the password change process.
Bypass Local User Login	When selected, administrators with a Local user account bypass Enterprise Connect Passwordless authentication and login with username and password.
Force Offline OTP After Installation	When selected, users are unable to perform offline authentication until they have had at least one successful online login.

Setting	Description / Notes
Bypass MFA on Unlock when Connected to AD	When selected, users connected to the enterprise network who have already authenticated with MFA are not required to authenticate with 2nd factor again when unlocking the workstation. This will work as long as you are inside the network (no time limit). **IMPORTANT:** When selecting this option, verify that the **Bypass MFA Groups** checkbox is **NOT** selected.
Hide MFA Password	When selected, the Windows Agent does not send the password to the server. This option is used when a third party authenticator does not require the password.
Force Lock After Offline OTP	When selected, workstations that were unlocked using an Offline OTP and then connected back to enterprise network (online) are automatically locked and the user is asked to authenticate. This setting prevents users from using weak authentication to log into the enterprise network (online).
Show FIDO2 PIN	When selected, an additional field is displayed on the Windows Login screen to enable users to enter the PIN associated with the FIDO key used for authentication. **IMPORTANT:** If your users have PINs set for their FIDO keys, **this checkbox must be selected** to enable them to successfully login using MFA.
Show Passwordless Link	When selected, an **Administrator Access Only** link appears on the Login screen. This link enables authorized users to login with Passwordless authentication (instead of MFA).
Bypass MFA Groups	When selected, you may specify ONE group in the AD that will not require MFA authentication. Enter **<Domain>\>Group Name>** in the field to the right. **IMPORTANT:** When selecting this option, verify that the **Bypass MFA on Unlock when Connected to AD** checkbox is **NOT** selected.

Miscellaneous Advanced Options

The **Advanced** tab is divided into the following sections:

- **Advanced Settings:** Contains settings for controlling presentation of authentication methods and other features displayed on the Windows Login screen
- **Trace:** Contains settings related to various aspects of log file storage management



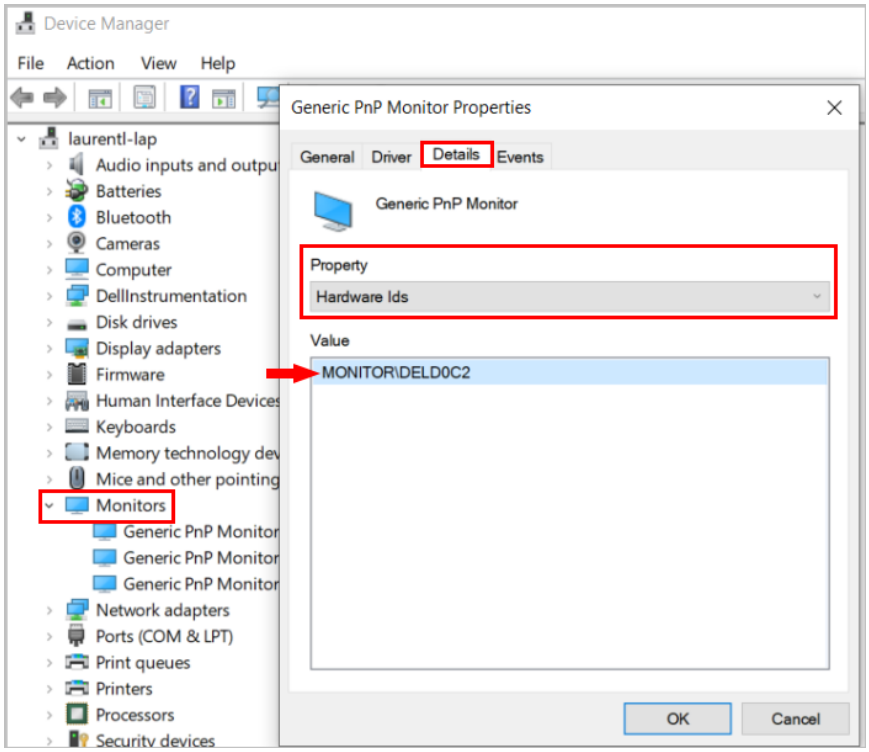
The **Advanced (Other)** tab is a separate tab containing options allowing you to customize the Windows Login screen with your organization's logo, icons and support information. For details, refer to Creating the MSIUpdater Configuration.

Managing Login Screen Labels and Features

The upper portion of the **Advanced** tab contains the following settings:

Setting	Description / Notes
Enable SDO SSO	After selecting the checkbox, enter the URL of the User Portal in the field to the right. In runtime, the portal will open in the default browser. Users will be automatically logged in and be able to view all assigned services.
Change Octopus Name	Allows you to change the default name (**Octopus Authenticator**) displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field. This setting is available only when the **Octopus App** checkbox in the **Parameters** tab is selected.

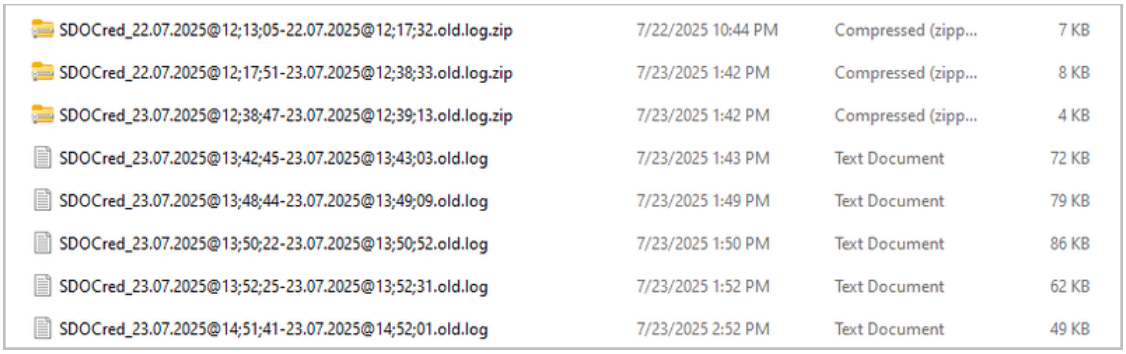
Setting	Description / Notes
Change OTP Name	Allows you to change the default name of the OTP displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field. This setting is available only when the **OTP** checkbox in the **Parameters** tab is selected.
Change Ping Identity Authenticator Name	Allows you to change the default name of the third party authenticator displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field. This setting is available only when the **Ping Identity Authenticator** checkbox in the **Parameters** tab is selected.
Change SMS Name	Allows you to change the default name of the SMS option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Change Email Name	Allows you to change the default name of the Email option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Change Voice Call Name	Allows you to change the default name of the Voice Call option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Change Passphrase Name	Allows you to change the default name of the passphrase option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Change Certificate Name	Allows you to change the default name of the certificate option displayed in the Windows credential provider's login authentication method selection list. After selecting the checkbox, enter the desired name in the field.
Enable CP Bypass List	Allows you to specify credential providers that will available for Windows login. After selecting the checkbox, paste the registry key(s) representing the relevant credential provider(s) in the field to the right. The specified providers will be displayed as login options on the Windows Login screen.

Setting	Description / Notes
Use Monitor Prefix	When selected (and when there is a prefix match), the Windows Login screen presents users with the Enterprise Connect Passwordless Authenticator login option only. If a prefix is specified but there is no match, users are presented with the FIDO2 (BIO) or FIDO Bypass login options. For more information, refer to Enabling FIDO BIO User Bypass. After selecting the checkbox, enter the monitor prefix in the field to the right. You can find the prefix in the Windows Device Manager. Under **Monitors**, open the properties of the monitor. Then, in the **Details** tab, select the *Hardware Ids* property. 
Change Trace Log Directory	Allows you to change the default log file location. After selecting the checkbox, enter the desired file path (e.g., **C:\temp\logs**) in the field to the right. This setting is available only when the **Enable Trace** checkbox in the **Settings** tab is selected.

Configuring Trace Log Storage Settings

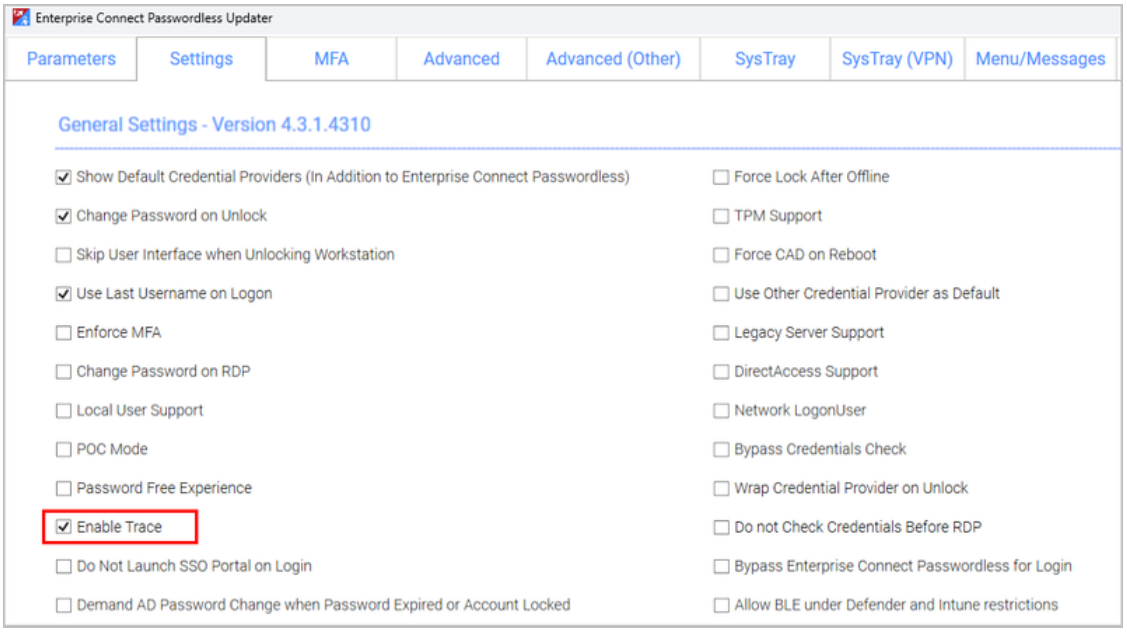
In the lower portion of the **Advanced** tab, you can configure settings related to log file storage management. You can change the default storage location and define a maximum size for the directory. In addition, you can create a schedule for automatically cleaning log files. In this process, **.log** files are converted to **.oldlog** files after a

configurable number of minutes. The old logs are then compressed to save disk space, and are removed from the system after a specified period of time.

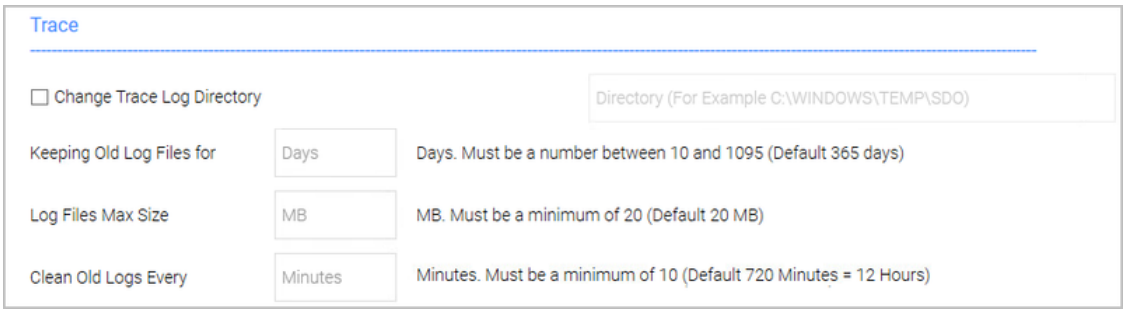


To manage trace log storage:

1. From the **Settings** tab, select the **Enable Trace** checkbox.



2. At the bottom of the **Advanced** tab, configure all or some of the settings in the **Trace** section.



The settings are:

- **Change Trace Log Directory:** To change the default log file location, select the checkbox and enter the desired file path (e.g., **C:\temp\logs**) in the field to the right.
- **Keep Old Log Files For:** The period of time (in days) after which old compressed log files (logs with a file format of **.oldlog.zip**) are deleted. The supported range is **10 - 1095**.
- **Log Files Max Size:** The maximum size (in MB) of the *directory* in which the log files are stored. The minimum supported value is **20**.
- **Clean Old Logs Every:** The period of time (in minutes) after which a log file is designated as an older file by changing the format from **.log** to **.oldlog**. The minimum supported value is **10**. The default value is **720** (12 hours).

Enabling Systray Settings

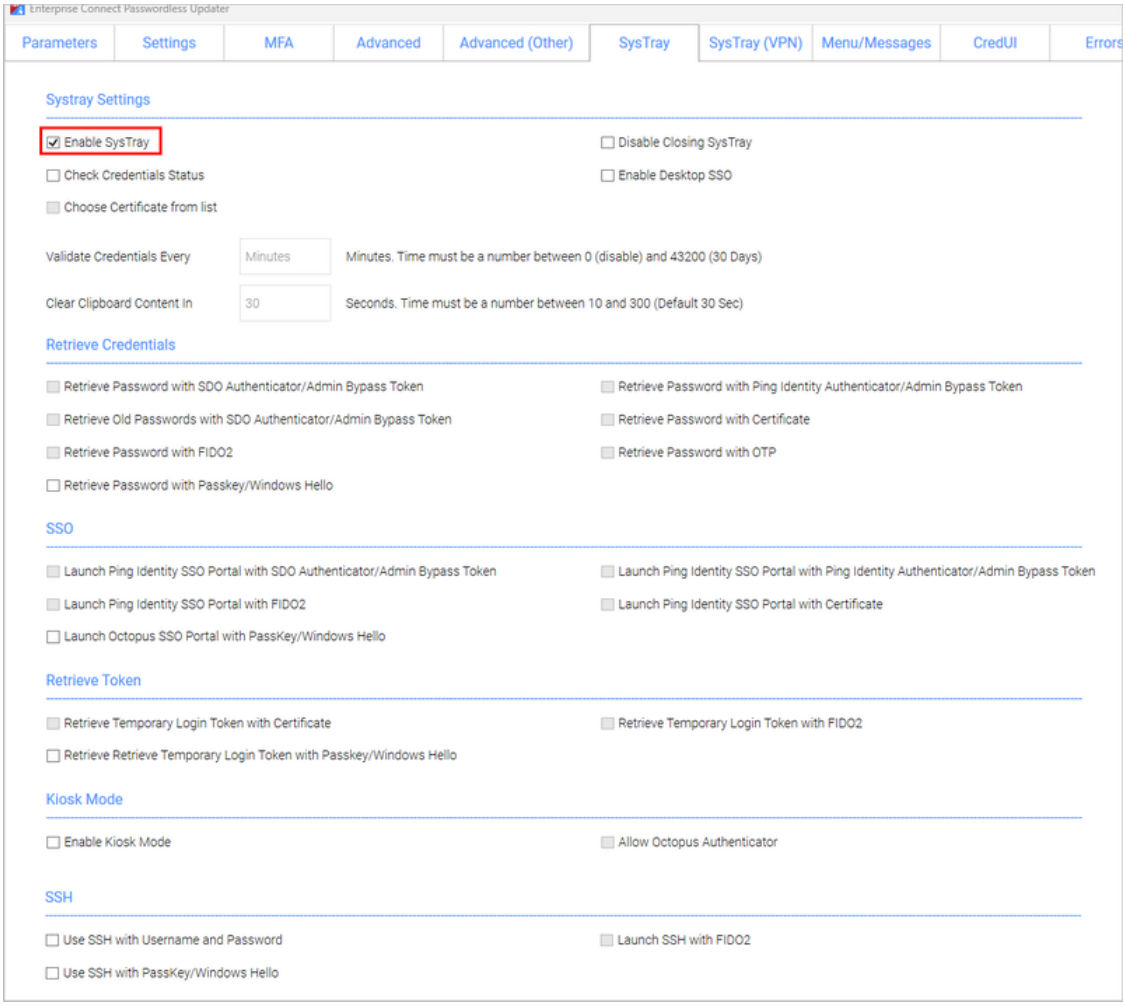
The **Enable SysTray** setting (at the top of the **SysTray** tab) determines whether users will be able to access self-service actions from the Windows systray. When this setting is activated, you can choose which actions will be available.

After users initiate a systray action, the systray is automatically locked for 30 seconds. (Multiple actions are not supported.)

Important

If you enable the systray, it is strongly recommended to follow the best practice of disabling Microsoft Office Clipboard to prevent sensitive data from being exposed.

The **SysTray** tab contains a variety of user self-service actions, such as password and token retrieval, User Portal access, and more. VPN connection options are offered in the separate SysTray (VPN) tab.



For convenience, systray settings are divided into relevant categories. The options are:

Action	Description / Notes
Systray Settings	
Check Credentials Status	When selected, users are able to view the time remaining until password expiration.
Choose Certificate from list	When selected, users are able to select any certificate integrated with the system, and are not required to use the one utilized for the initial logon. This setting is useful in cases where users sharing an account need to access legacy applications after login. The checkbox is enabled when **Certificate Authenticator** is selected as an authenticator in the **Parameters** tab.
Disable Closing SysTray	When selected, the **Close App** systray action is hidden.

Action	Description / Notes
Enable Desktop SSO	When selected, users are able to access specific applications that are integrated with the Enterprise Connect Passwordless platform without having to reauthenticate. The applications and other relevant settings are configured in the **Applications** menu of the Enterprise Connect Passwordless Management Console. **IMPORTANT:** Desktop SSO is supported for Enterprise Connect Passwordless Authentication Server **version 6.6** (and higher). For further information, please refer to the Enterprise Connect Passwordless Management Console Admin Guide.
Validate Credentials Every	Allows you to specify a value (in minutes) for the frequency at which the system tray checks whether the user is connected to AD and whether the password is still valid. Valid values can range from **0** (disabled) to **43200** (30 days. Once the password expires, users will need to login within the organization network or via the VPN in order to reauthenticate.
Clear Clipboard Content in	Allows you to specify the number of seconds for which the AD password / login token is available for viewing / copying.
Retrieve Credentials	
Retrieve Password with SDO Authenticator/Admin Bypass Token	When selected, users are able to view and copy the current AD password after performing passwordless authentication on the Octopus Authenticator mobile app. Admin users in Bypass mode need to enter the temporary token to retrieve the password.
Retrieve Old Passwords with SDO Authenticator/ Admin Bypass Token	When selected, users are able to view and copy previously used AD passwords after performing passwordless authentication on the Octopus Authenticator mobile app. Admin users in Bypass mode need to enter the temporary token to retrieve the passwords.
Retrieve Password with Ping Identity Authenticator/ Admin Bypass Token	When selected, users are able to view and copy the AD password after performing passwordless authentication on the Ping Identity mobile app. Admin users in Bypass mode need to enter the temporary token to retrieve the password.

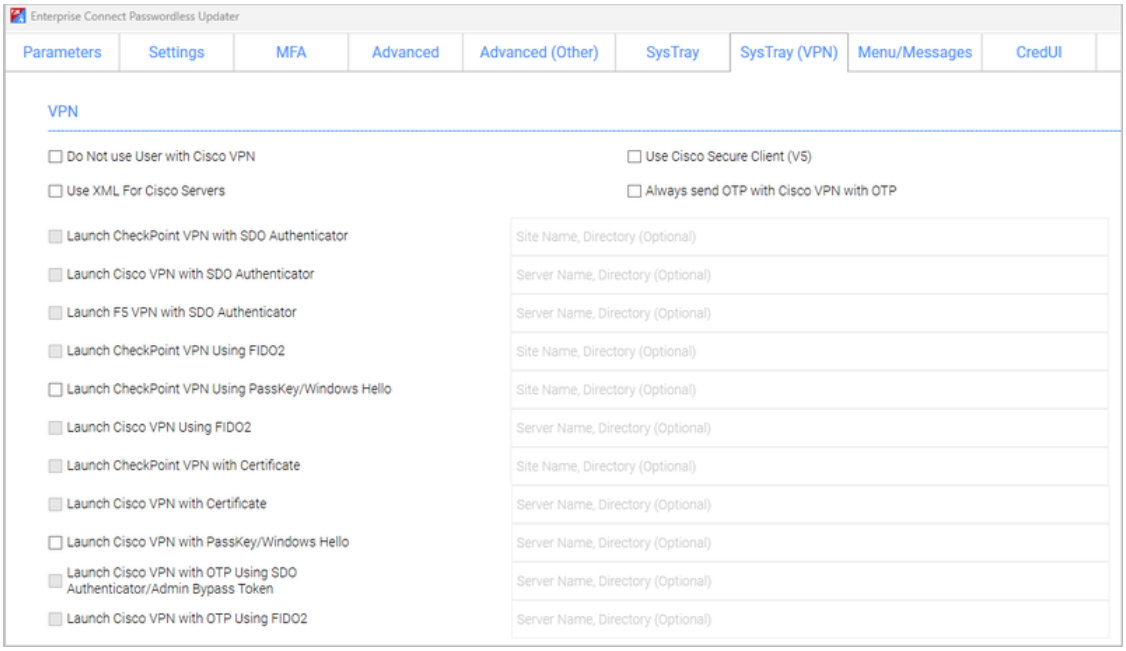
Action	Description / Notes
Retrieve Password with FIDO2	When selected, users are able to view and copy the AD password after performing passwordless authentication using a FIDO key.
Retrieve Password with Certificate	When selected, users are able to view and copy the AD password after performing authentication using a smart card signed by the organization's root CA.
Retrieve Password with Passkey/Windows Hello	When selected, users are able to view and copy the AD password either using the Windows Hello sign-in configured for the workstation, OR after performing authentication using a passkey that is integrated with the user's workstation or smartphone. To retrieve the password using a passkey, the following conditions need to be met: • The FIDO Authenticator in the Management Console is enabled and connected. • The **Enable Passkeys** toggle in the **FIDO2 Authentication Settings** of the relevant directory is enabled. • The user has enrolled the passkey in the system. **Important** This feature is supported for Windows 11, version 22H2 and higher only.
Retrieve Password with OTP	When selected, users are able to view and copy the AD password after performing authentication by means of a software OTP code or a hardware OTP token. This checkbox is enabled when **OTP** is selected as an authenticator in the **Parameters** tab.
SSO	
Launch Ping Identity SSO Portal with SDO Authenticator / Admin Bypass Token	When selected, users are able to open the User Portal from the desktop after performing passwordless authentication on the Octopus mobile app. Admin users in Bypass mode need to enter the temporary token to launch the Portal.
Launch Ping Identity SSO Portal with FIDO2	When selected, users are able to open the User Portal from the desktop after performing passwordless authentication using a FIDO key.

Action	Description / Notes
Launch Ping Identity SSO Portal with Certificate	When selected, users are able to open the User Portal from the desktop after performing authentication using a smart card signed by the organization's root CA.
Launch Enterprise Connect Passwordless SSO Portal with Ping Identity Authenticator/Admin Bypass Token	When selected, users are able to open the User Portal from the desktop after performing passwordless authentication on the PingID mobile app. Admin users in Bypass mode need to enter the temporary token to launch the Portal.
Retrieve Token	
Retrieve Temporary Login Token with Certificate	When selected, users are able to retrieve the temporary token required for RADIUS login after performing authentication using a smart card signed by the organization's root CA.
Retrieve Temporary Login Token with FIDO2	When selected, users are able to retrieve the temporary token required for RADIUS login after authenticating with a FIDO key.
Retrieve Temporary Login Token with Passkey/ Windows Hello	When selected, users are able to retrieve the temporary token required for RADIUS login using the Windows Hello sign-in configured for the workstation. For details about setting up Windows Hello integration, refer to Configuring Windows Hello Support.
Kiosk Mode	
Enable Kiosk Mode	When selected, users in the organization are able to perform the following actions from a workstation to which they are not currently logged in: • Retrieve their AD passwords • Retrieve the temporary token required for RADIUS login When users select these options from the systray, they will be prompted to authenticate using a FIDO key (BIO or PIN) or a hardware OTP token. (These settings, in the **Retrieve Credentials** / **Retrieve Token** sections of the **Systray** tab, must also be selected.) Following successful authentication, the password or token is copied to the clipboard.

Action	Description / Notes
Allow Octopus Authenticator	When selected, users working in Kiosk Mode are able to retrieve the AD password / temporary login token after authenticating with the Octopus mobile app,
SSH	
Use SSH with Username and Password	When selected, users will be able to authenticate to a selected PuTTY profile by entering Username + Password.
Use SSH with Passkey/ Windows Hello	When selected, users will be able to authenticate to a selected PuTTY profile using the Windows Hello sign-in configured for the workstation. For details about setting up Windows Hello integration, refer to Configuring Windows Hello Support.
Launch SSH with FIDO2	When selected, users will be able to authenticate to a selected PuTTY profile. To use this feature, the following conditions need to be met: • **FIDO2** and/or **FIDO2 (BIO)** is selected as an authenticator in the **Parameters** tab. • The user is enrolled in the system with the FIDO authenticator. • PuTTY is installed on the Windows workstation.

Configuring Systray VPN Access Options

The **SysTray (VPN)** tab contains settings related to connecting to the Check Point, Cisco and F5 VPNs.



The settings are:

Setting	Description / Notes
Do Not use User with Cisco VPN	When selected, the Cisco username needs to be provided manually.
Use XML for Cisco Servers	When selected, servers from XML files (instead of from registry) are used.
Use Cisco Secure Client (V5)	Select this checkbox to use Cisco Secure Client 5. When the checkbox is not selected, the previous version (V4) will be used.
Always send OTP with Cisco VPN with OTP	When selected, the OTP code is sent to the VPN server (in addition to the username and password) when users log in using an online MFA flow.
Launch Check Point VPN with SDO Authenticator	When selected, users are able to connect to the Check Point VPN directly from the desktop after performing passwordless authentication on the Octopus Authenticator mobile app. In the field to the right, enter the site/profile name of the Check Point VPN, as set on the Check Point client. **Important:** If users work with Check Point Harmony, or if your VPN is installed in different locations, enter a comma after the name, followed by the full path of the VPN client. For example: *office,C:\Program Files (x86)\CheckPoint\Endpoint Security\Endpoint Connect*

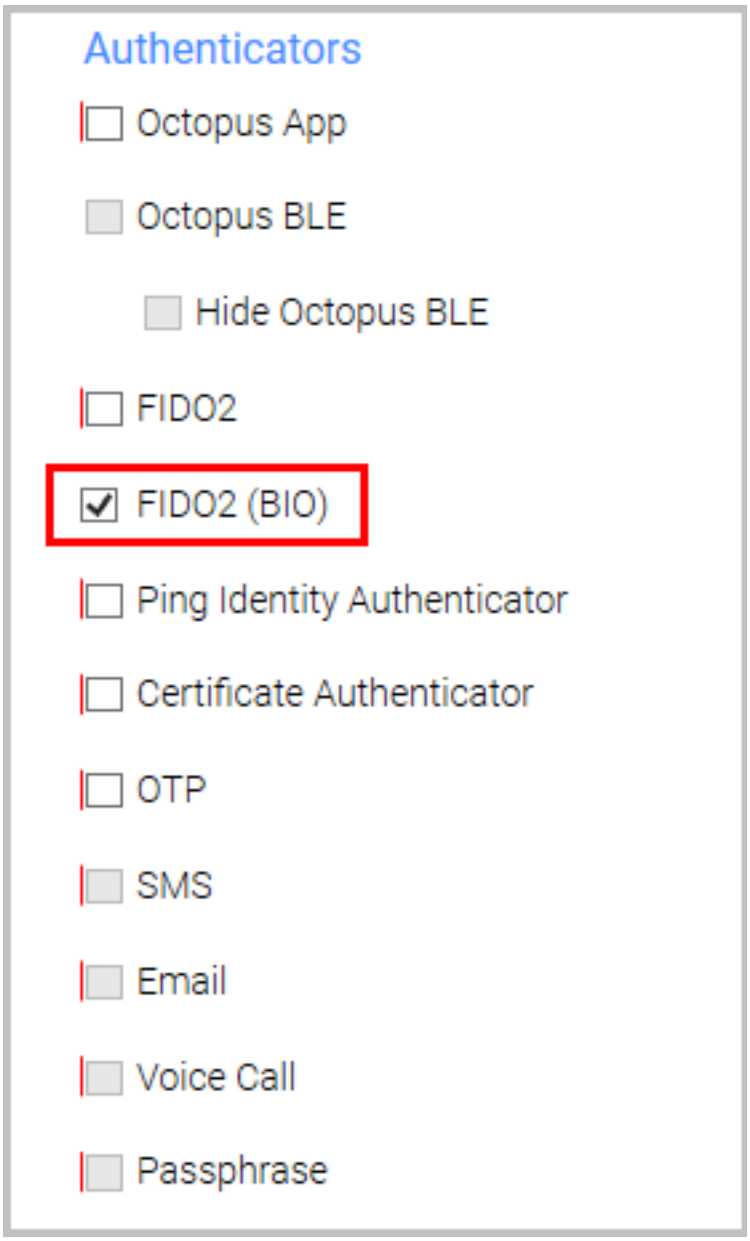
Setting	Description / Notes
Launch Cisco VPN with SDO Authenticator	When selected, users are able to connect to the Cisco VPN directly from the desktop after performing passwordless authentication on the Octopus Authenticator mobile app. In the field to the right, enter the site/profile name of the Cisco VPN, as set on the Cisco client.
Launch F5 VPN with SDO Authenticator	When selected, users are able to connect to the F5 VPN directly from the desktop after performing passwordless authentication on the Octopus Authenticator mobile app. In the field to the right, enter the site/profile name of the F5 VPN, as set on the F5 client.
Launch Check Point VPN Using FIDO2	When selected, users are able to connect to the Check Point VPN directly from the desktop after performing passwordless authentication using a FIDO key. In the field to the right, enter the site/profile name of the Check Point VPN, as set on the Check Point client.
Launch Check Point VPN Using PassKey/ Windows Hello	When selected, users are able to connect to the Check Point VPN directly from the desktop using the Windows Hello sign-in configured for the workstation. In the field to the right, enter the site/profile name of the Check Point VPN, as set on the Check Point client.
Launch Cisco VPN Using FIDO2	When selected, users are able to connect to the Cisco VPN directly from the desktop after performing passwordless authentication using a FIDO key. In the field to the right, enter the site/profile name of the Cisco VPN, as set on the Cisco client.
Launch Check Point VPN with Certificate	When selected, users are able to connect to the Check Point VPN directly from the desktop after performing authentication using a smart card signed by the organization's root CA. In the field to the right, enter the site/profile name of the Check Point VPN, as set on the Check Point client.
Launch Cisco VPN with Certificate	When selected, users are able to connect to the Cisco VPN directly from the desktop after performing authentication using a smart card signed by the organization's root CA. In the field to the right, enter the site/profile name of the Cisco VPN, as set on the Cisco client.
Launch Cisco VPN with PassKey/ Windows Hello	When selected, users are able to connect to the Cisco VPN directly from the desktop using the Windows Hello sign-in configured for the workstation. In the field to the right, enter the site/profile name of the Cisco VPN, as set on the Cisco client.

Setting	Description / Notes
Launch Cisco VPN with OTP Using SDO Authenticator/ Admin Bypass Token	When selected, users are able to connect to the Cisco VPN directly from the desktop after performing OTP authentication on the Octopus Authenticator mobile app. Admin users in Bypass mode need to enter the temporary token to launch the Portal. In the field to the right, enter the site/profile name of the Cisco VPN, as set on the Cisco client.
Launch Cisco VPN with OTP Using FIDO2	When selected, users are able to connect to the Cisco VPN directly from the desktop after performing OTP authentication using a FIDO key. In the field to the right, enter the site/profile name of the Cisco VPN, as set on the Cisco client.

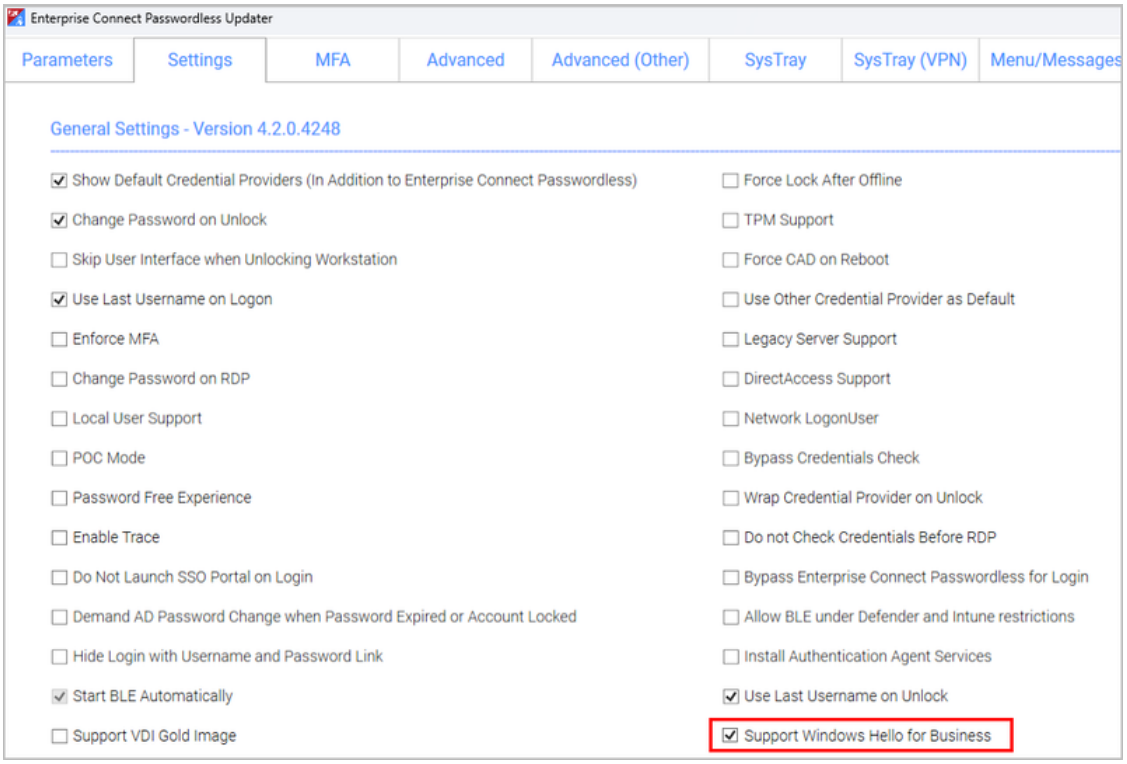
Configuring Windows Hello Support for Systray Actions

Enterprise Connect Passwordless for Windows provides the option for performing some Systray actions using the Windows Hello sign-in configured for the workstation. To enable support for this option, make sure that the following conditions are met:

- In the **Parameters** tab of the MSIUpdater, the **FIDO2 (BIO)** authenticator is selected.



- In the **Settings** tab of the MSIUpdater, the **Support Windows Hello for Business** checkbox is selected.

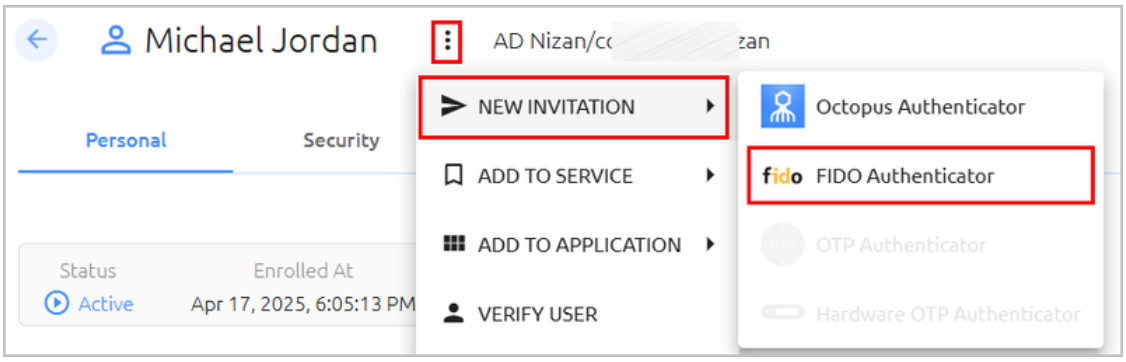


- In the **SysTray** and **SysTray (VPN)** tabs of the MSIUpdater, the relevant systray actions are selected (e.g., **Retrieve Password with Passkey/Windows Hello**).
- Users have configured Windows Hello as a Sign-in option for their workstations.
- Users have enrolled in the platform using FIDO device registration.

Windows Hello Enrollment

The authentication process for Windows Hello is based on the workflow for FIDO authentication. Therefore, users should be sent **FIDO Authenticator** enrollment invitations, and they perform FIDO Authenticator registration (as described below).

> **Important**
>
> Users do NOT need to possess a FIDO key to successfully perform Systray actions using Windows Hello.

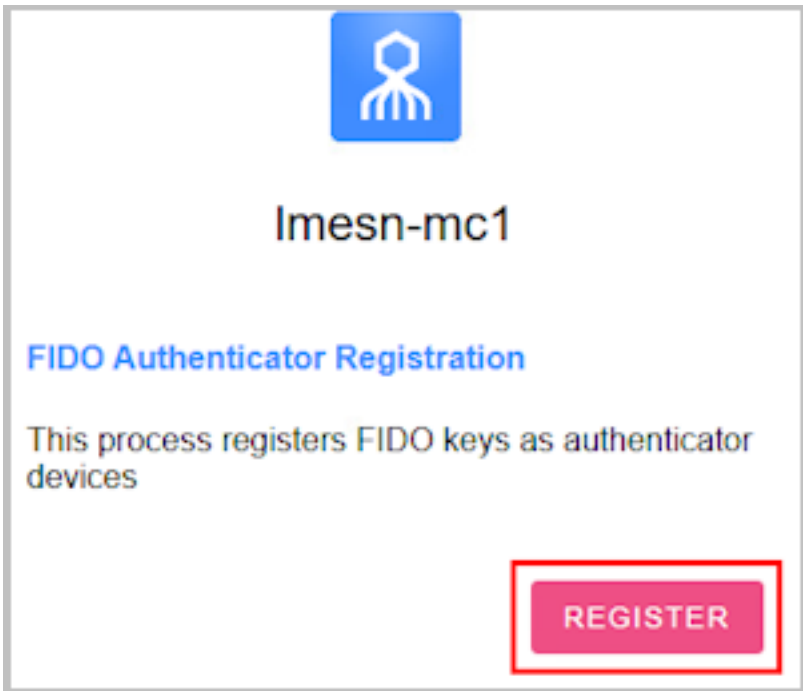


The enrollment flow is as follows:

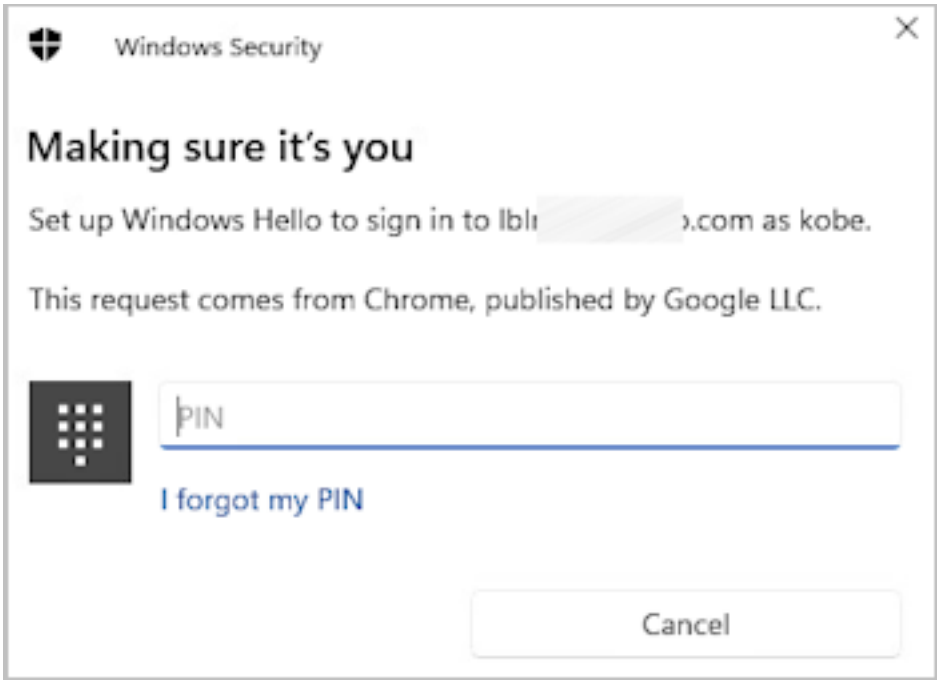
1. The user opens the invitation email sent and clicks the **Click to Enroll** link.

   The user is then redirected to the User Portal, in registration mode.

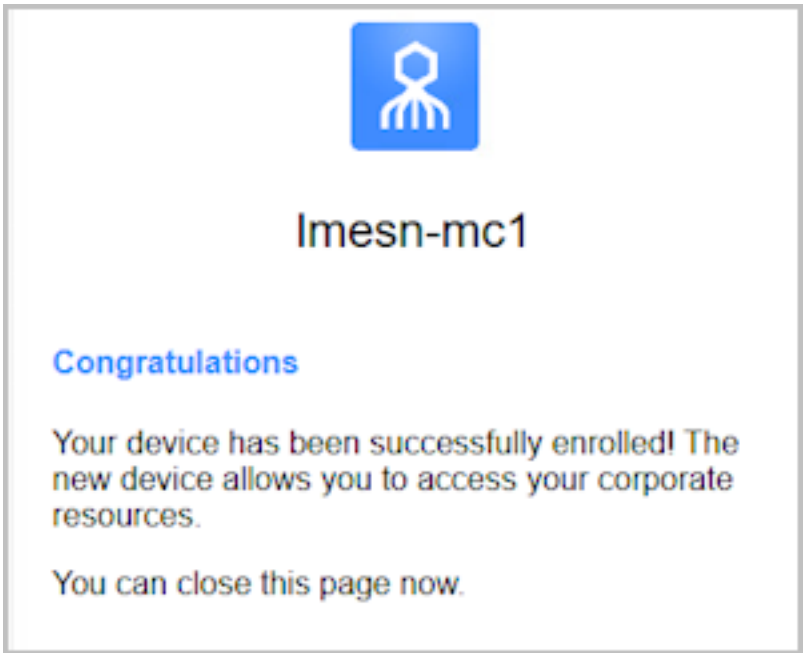
2. The user clicks **Register**.



3. The user is prompted to authenticate using the Windows Hello Sign-in option configured for the workstation. For example:



4. Upon successful authentication, a confirmation message is displayed.

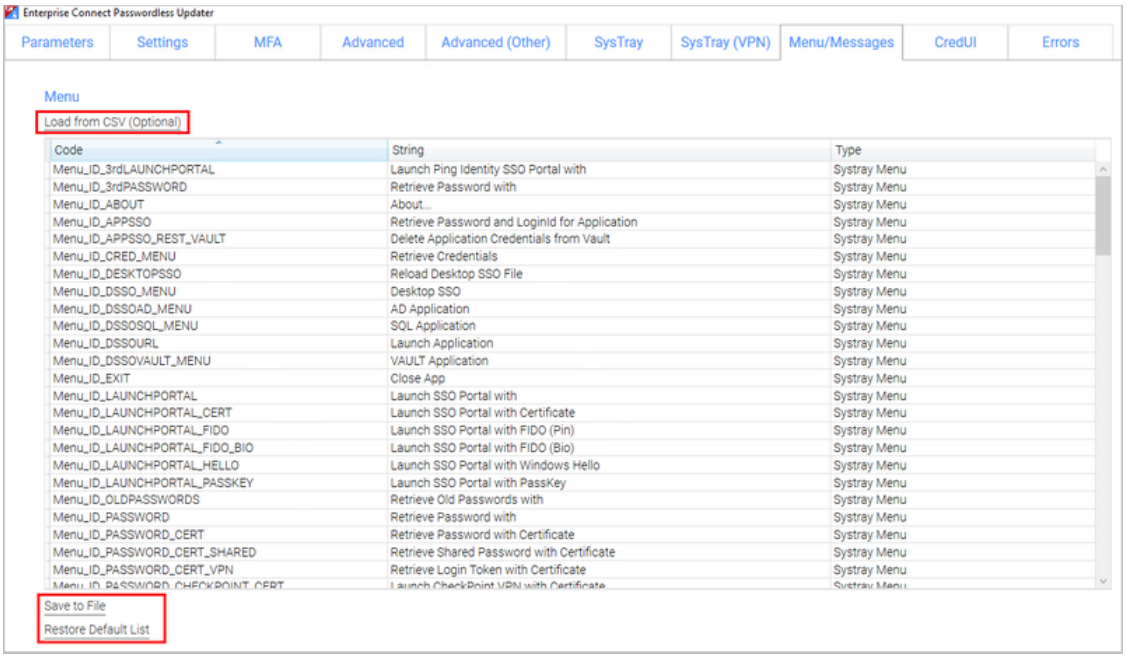


Customizing Systray Messages

In the **Menu/Messages** tab, you can review and modify the default strings for actions and messages that will be displayed to users in the systray. The strings can be customized as required, or entered in a language other than English. (The codes are not editable.)

For convenience, the following options are available:

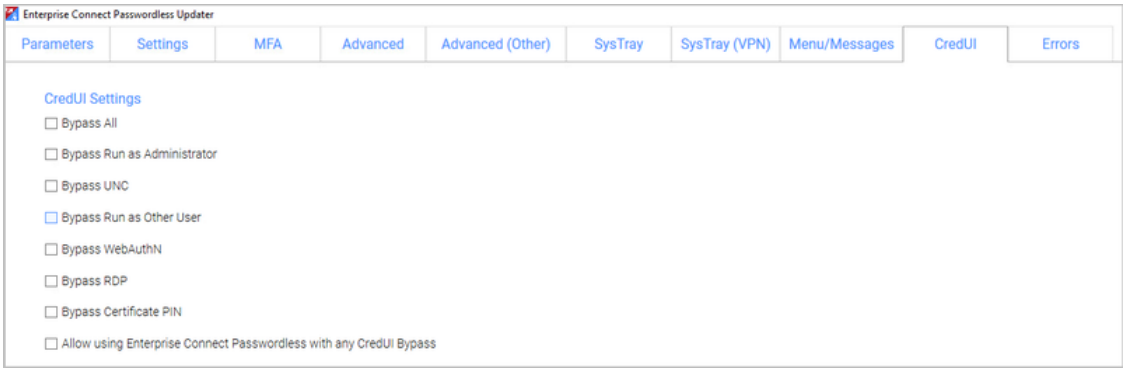
- **Save to File:** Downloads the Strings list to a CSV file, for backup and editing purposes.
- **Load from CSV:** Populates the Strings list with data from an uploaded CSV file.
- **Restore Default List:** Resets the Strings list with the original default texts.



Selecting Bypass Scenarios

The **CredUI** tab allows you to select scenarios in which the Enterprise Connect Passwordless authentication mechanism is hidden, and users perform the login by entering Username + Password. Selecting **Bypass All** (at the top of the tab) activates bypass for all the scenarios.

If you select
Allow using Enterprise Connect Passwordless with any CredUI bypass (at the bottom of the tab), the Enterprise Connect Passwordless authentication mechanism is presented together with additional login options.

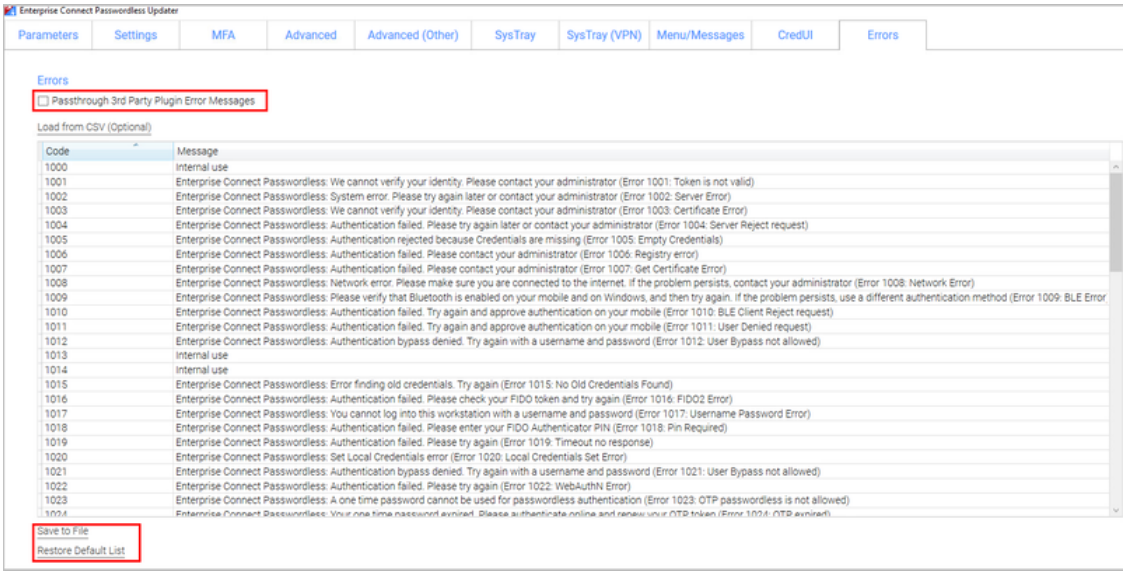


Customizing Error Messages

In the **Errors** tab, you can review the default messages that will be displayed to users when errors occur and customize the message text where relevant. (The error codes are not editable.)

For convenience, the following options are available:

- **Passthrough 3rd Party Plugin Error Messages:** When this checkbox is selected, error messages returned from a 3rd party authenticator to the server are sent to the Windows agent and displayed to the user. (The content of these messages can be configured and customized during authenticator plugin development.)
- **Save to File:** Downloads the Errors list to a CSV file, for backup and editing purposes.
- **Load from CSV:** Populates the Errors list with data from an uploaded CSV file.
- **Restore Default List:** Resets the Errors list with the original default message texts.



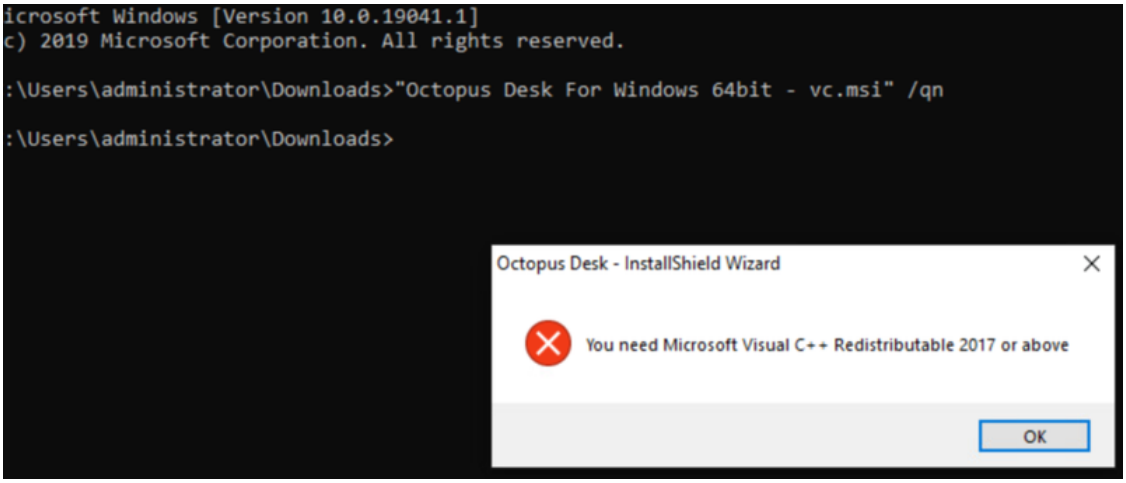
MSI Deployment of Enterprise Connect Passwordless for Windows

The following sections explain how to deploy and upgrade using the MSI tool.

Performing Silent Installation

Silent installation allows administrators to manually install Enterprise Connect Passwordless or push the installation to all client machines from a central tool (e.g., GPO).

Before performing installation with software distribution tools, make sure the Visual C++ 2017 (or later) Redistributable (x64)/(x86) - 14.30.30704.0 is installed. If this package is not installed, the installation will abort and the following error message will be displayed:



Note: Administrator permissions are required to run the Enterprise Connect Passwordless for Windows MSI.

To perform silent installation:

1. Open the command prompt as Admin, and run *Enterprise Connect Passwordless For Windows 64bit.msi*
2. Run *Enterprise Connect Passwordless For Windows 64bit-xx.msi /qn*:

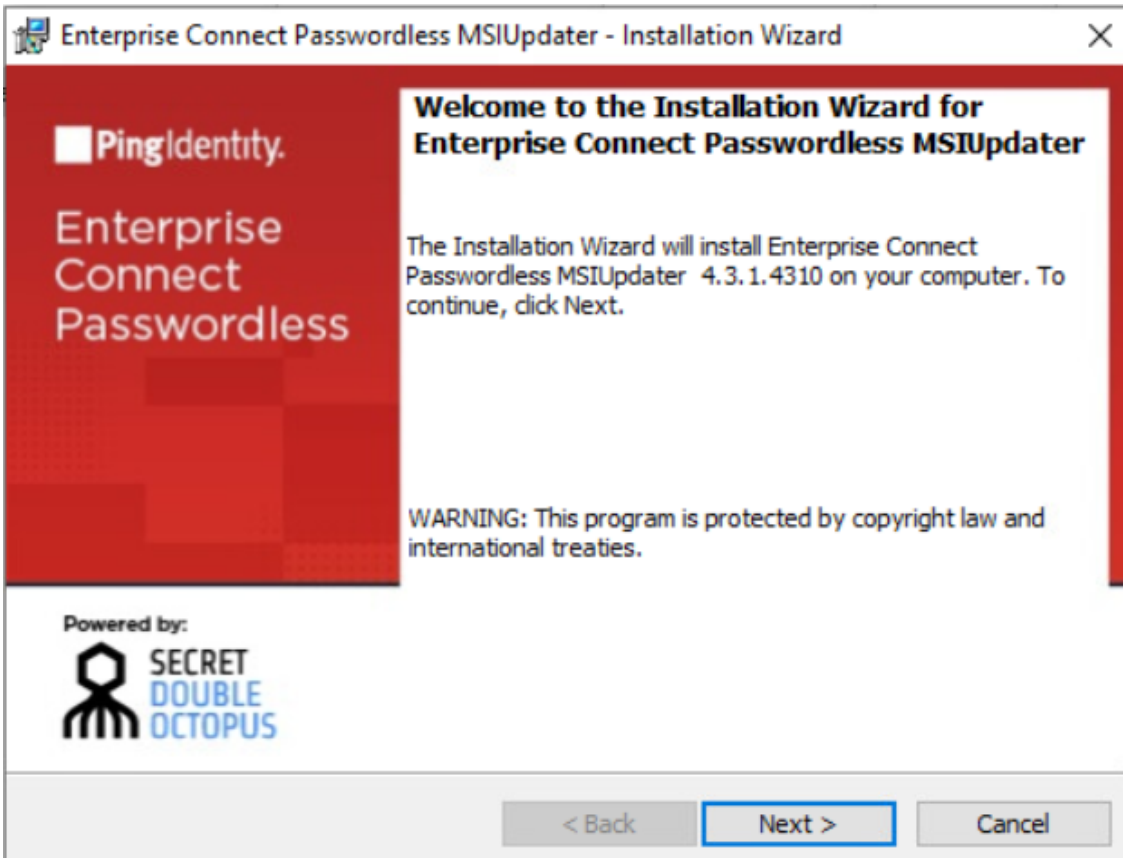
   C:\> Enterprise Connect Passwordless For Windows 64bit – xx_xxx_xx.msi /qn
3. If you want the credential provider to be disabled on some machines after installation (allowing for gradual deployment), refer to Enabling / Disabling the CP Post-installation.

Performing Deployment Using the Installation Wizard

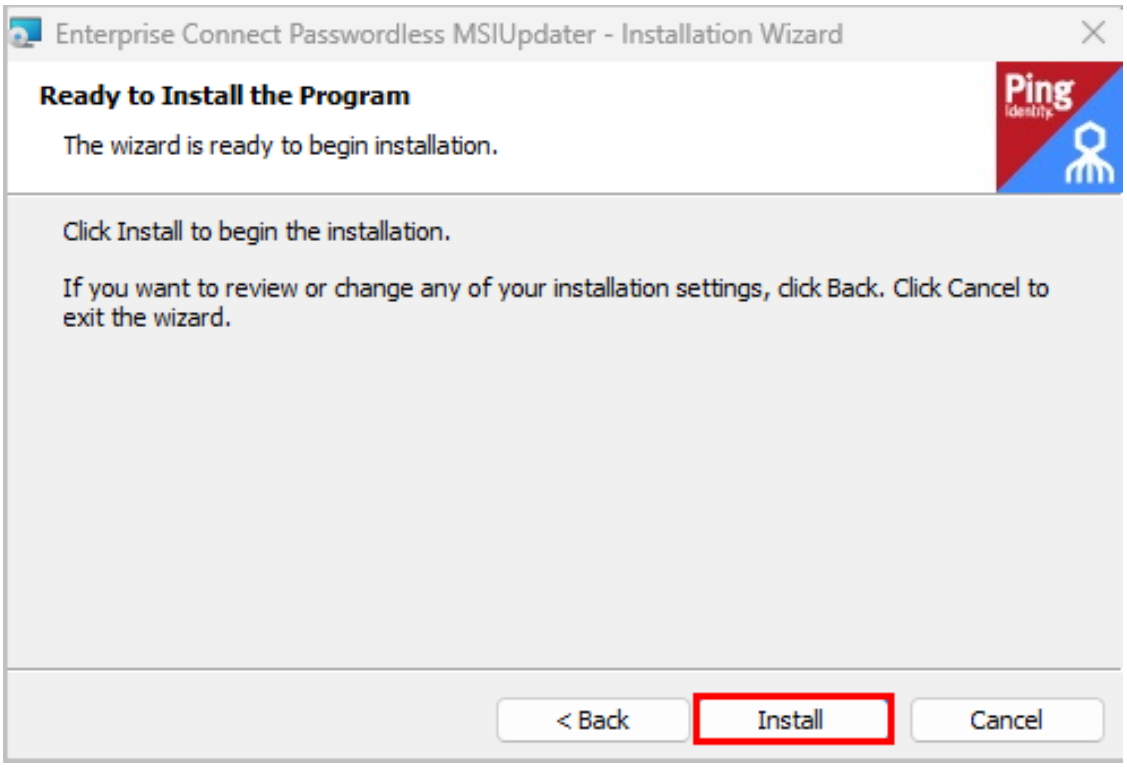
This method deploys the MSI package using the Enterprise Connect Passwordless installation wizard. All required components (including the Visual C++ Redistributable)are automatically installed as part of the deployment.

To deploy Enterprise Connect Passwordless using the installation wizard:

1. To launch the wizard, run the updated Enterprise Connect Passwordless for Windows MSI file.
2. On the Welcome page, click **Next**.

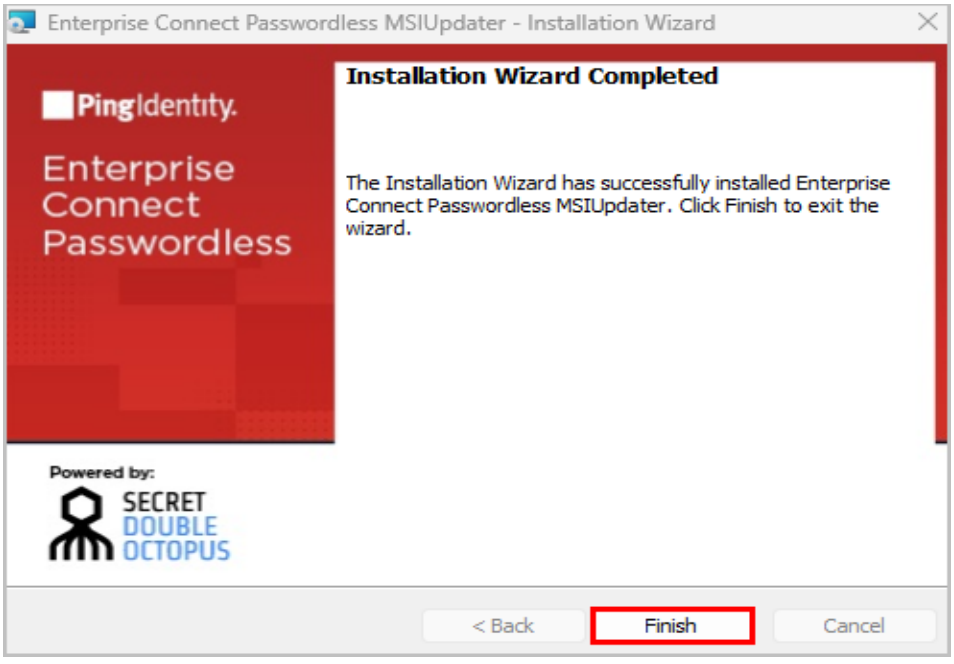


3. To begin the installation, click **Install**.



A status bar is displayed during the installation process.

4. To exit the wizard, click **Finish**.



Performing Installation Through Distribution Tools

Follow the steps below to push the installation through your endpoint management or software distribution tool.

Note: Administrator permissions are required to run the Enterprise Connect Passwordless for Windows MSI.

To push installation through distribution tools:

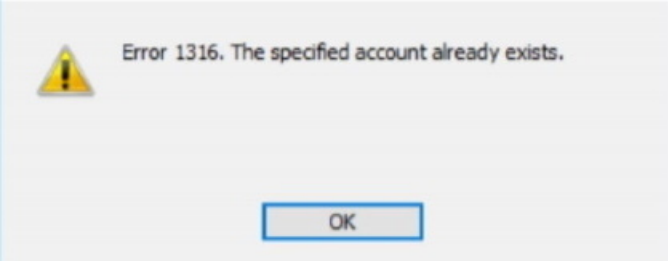
1. Open and run your distribution software.
2. Install Visual C++ 2017 (or later) Redistributable (x64)/(x86) - 14.30.30704.0
3. Open the command prompt as Admin, and run *Enterprise Connect Passwordless For Windows 64bit.msi*
4. Run *Enterprise Connect Passwordless For Windows 64bitxx.msi /qn*:

   C:\> Enterprise Connect Passwordless For Windows 64bit – xx_xxx_xx.msi /qn

Performing MSI Upgrade

IMPORTANT: To successfully perform MSI upgrade, the MSI file must have the same filename as the one used for original installation. The MSI updater creates an MSI file with the update date in the filename. **This file needs to be renamed** to match the name of the original installation file.

If you try to upgrade using an MSI file that is named differently from the original installation file, **Error 1316: The specified account already exists** will be generated. This message is a notification that you are trying to install an MSI file with a different name from the one that is already installed.



If you are not sure of the name of the original installation file, follow these steps:

1. Navigate to **C:\Windows\Installer**
2. Open the following file: **SourceHash{F88FAA40-72B9-4CE0-88DA-6592EF361C94}**
3. Search for the name of the file that was used for installation. You will find it at the end of the SourceHash file.

In addition, before performing the upgrade, verify that you have not changed the setting for **TPM Support** (in the **Settings** tab of the MSIUpdater). If the TPM setting for the upgrade is different from that set in the original installation, the upgrade will fail due to a public key mismatch error.

To upgrade the MSI, run the following command:

C:\> msiexec /I " Enterprise Connect Passwordless For Windows 64bit.msi" REINSTALL=ALL REINSTALLMODE=vomus IS_MINOR_UPGRADE=1 /norestart /qn

For more information and a list of additional optional installation parameters, click here.

Enabling the Password Free Experience

The Password Free Experience enables customers to start deploying the Windows agent while maintaining control over the password, so they can continue to use it for other applications. In the Password Free flow, users will be required to enter the password for the first login. After one successful login, all other authentication will be Passwordless (the user simply selects the authenticator, and does not need to provide a password for each login).

When the Password Free Experience is enabled, Enterprise Connect Passwordless does not manage the password, and users need to replace the password according to organizational policy. Once users change the password, they will again be required to enter it for the first login only.

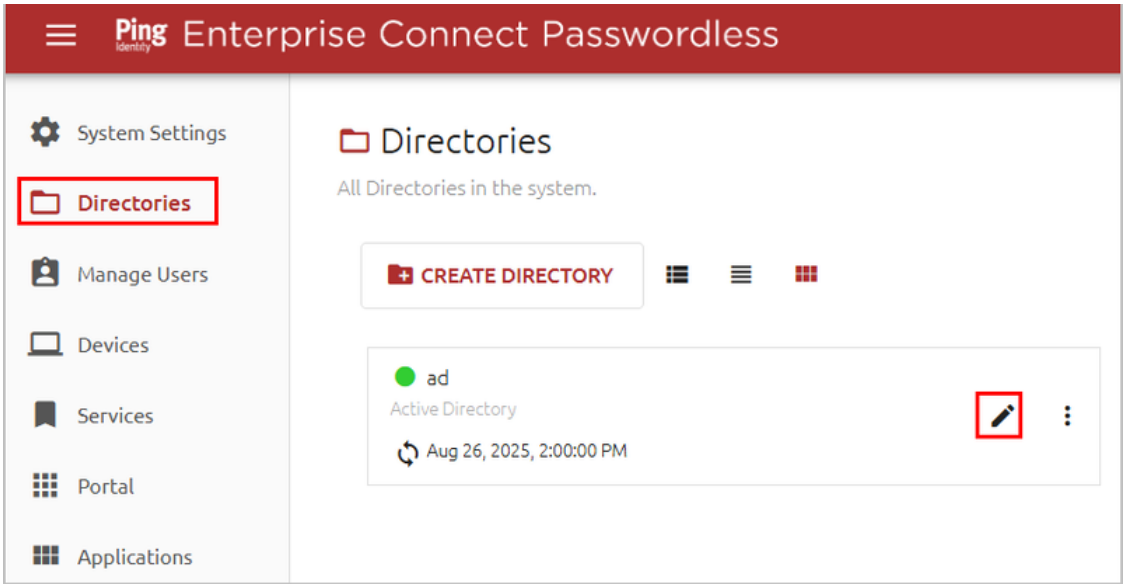
To enable the Password Free Experience, some configuration needs to be done in the Management Console and in the MSIUpdater.

Management Console Configuration

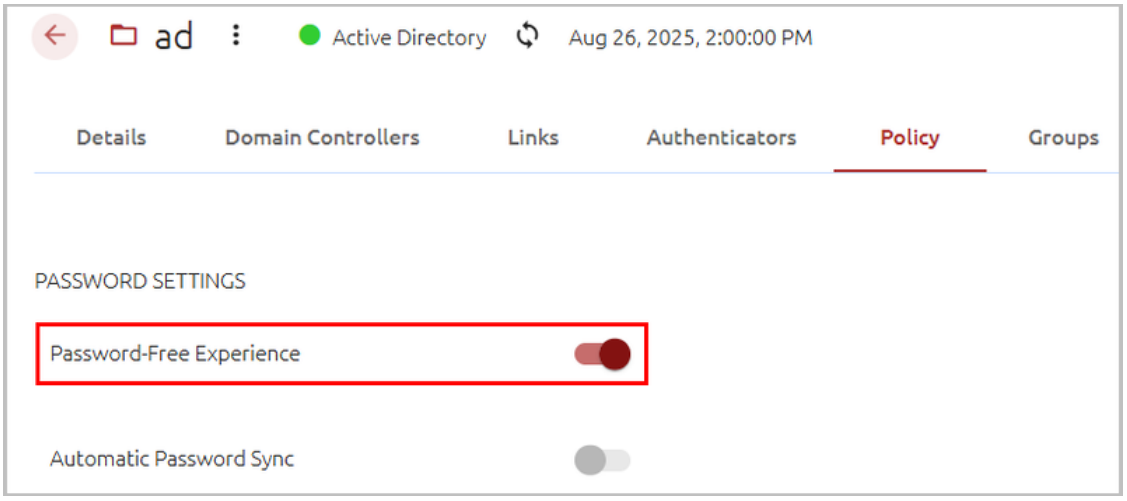
To support the Password Free Experience, the **Password Settings** of the directory need to be configured correctly so the system does NOT rotate the AD password. The configuration required varies depending on whether Compatibility Mode is ON or OFF (as explained in the procedure below). For more information about Compatibility Mode, please refer to the Management Console Admin Guide.

To configure Password Settings:

1. In the Management Console, select the **Directories** menu. Then, open the settings of the relevant directory by clicking .

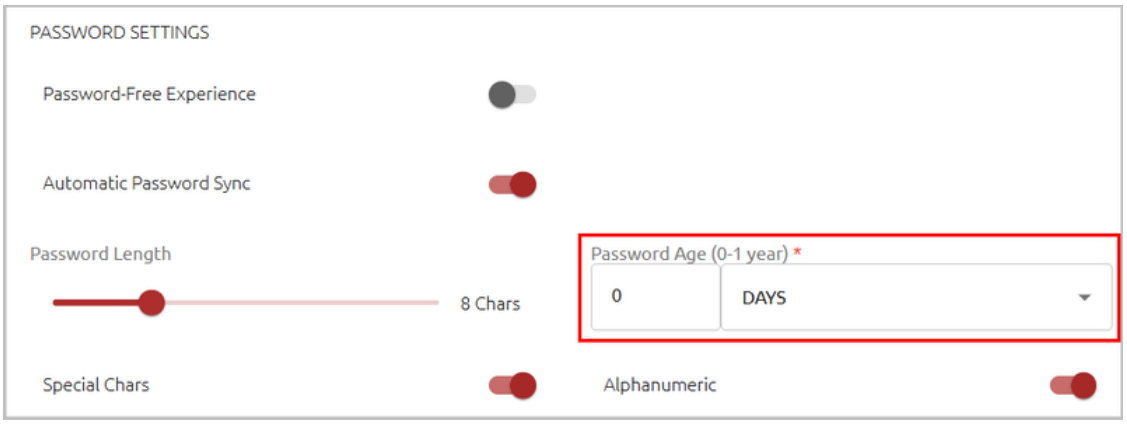


2. Select the **Policy** tab.
3. If Compatibility Mode is OFF, make sure that the **Password-Free Experience** toggle is enabled.



Then, go to Step 5 (below).

4. If Compatibility Mode is ON, set the **Password Age** to **0**.



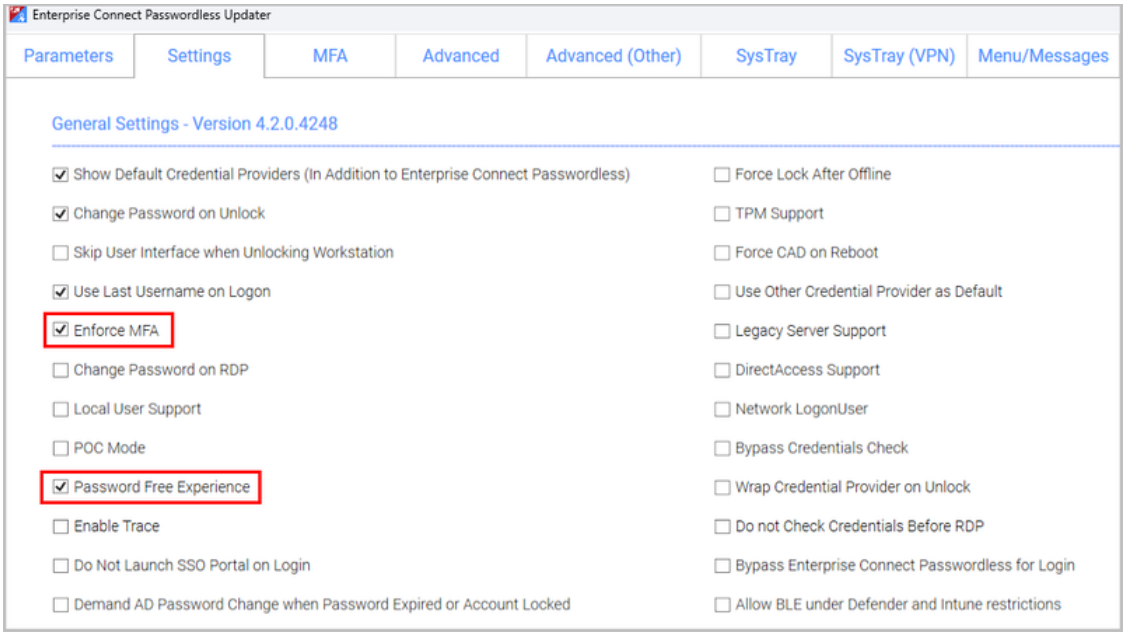
When the value is **0**, the system never rotates the password, and the password is managed directly on the directory or the AD.

5. Click **Save** and publish your changes.

Windows MSIUpdater Configuration

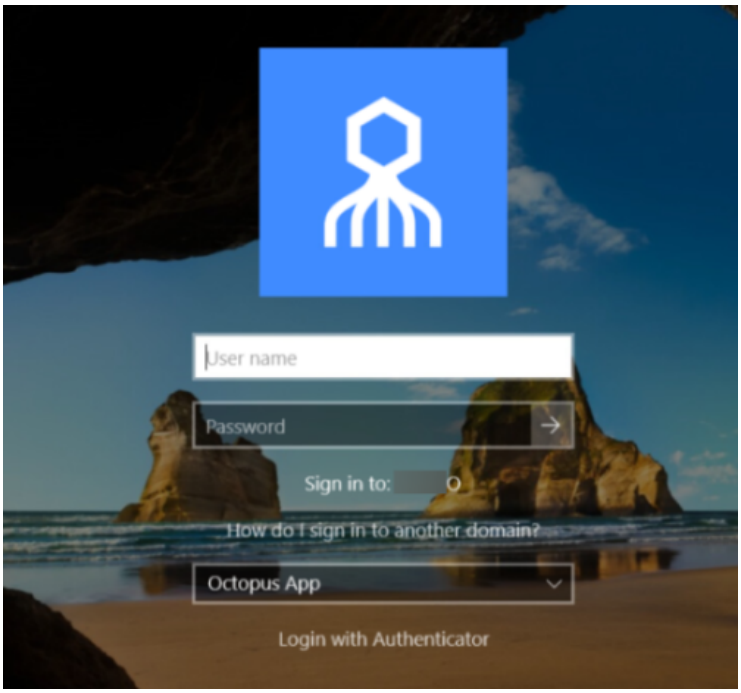
To enable support for the Password Free Experience in Enterprise Connect Passwordless for Windows, verify that BOTH of the following checkboxes are selected in the **Settings** tab of the MSIUpdater:

- Enforce MFA
- Password Free Experience

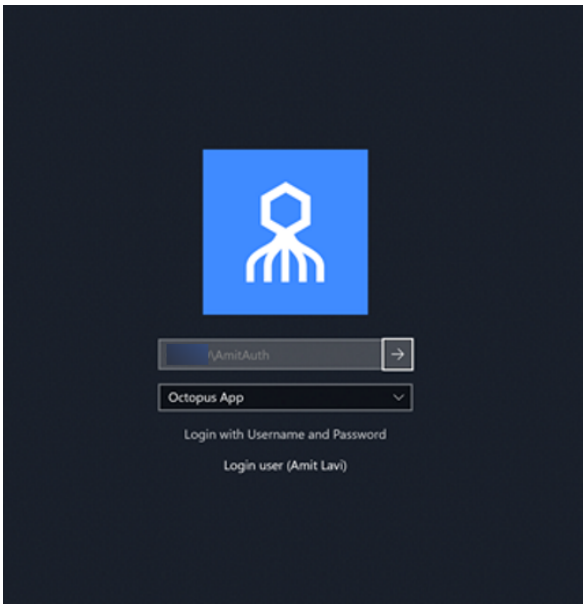


Password Free Experience: User Authentication

When the Password Free Experience feature is enabled, users need to enter Username + Password for the first login. Users may also select the authentication method (if relevant).



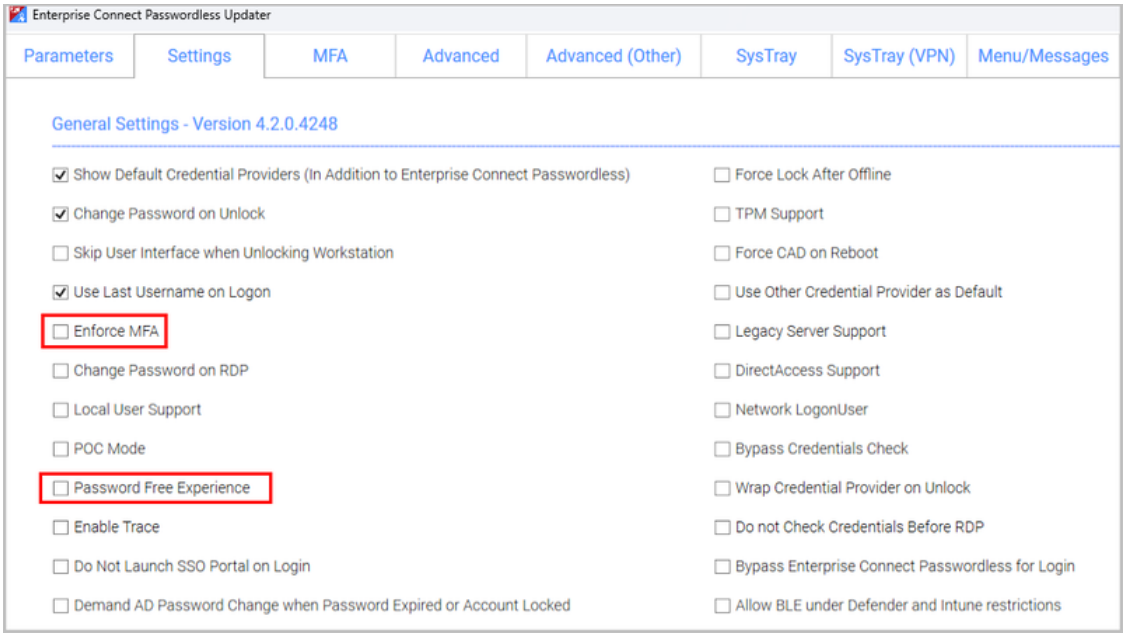
After the first successful login, users can still select the authentication method, but there is no need to enter a password for login or unlock.



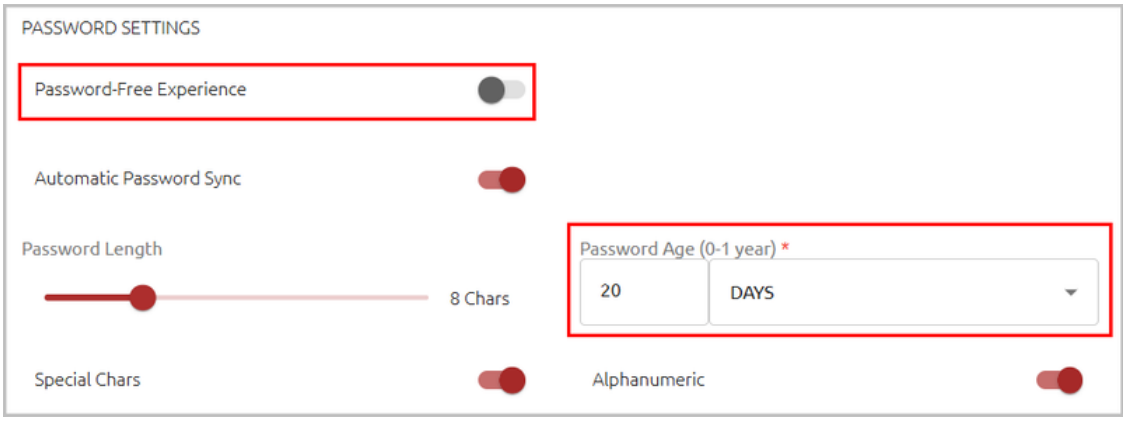
Transitioning to Passwordless Authentication

When your organization is ready to go from the Password Free Experience to passwordless authentication, follow these guidelines to ensure a smooth transition:

- **MSI configuration:** Create a new MSI configuration for deployment. In the **Settings** tab, make sure that the **Enforce MFA** and the **Password Free Experience** checkboxes are NOT selected.



- **Directory configuration:** In the Management Console, open the settings of the relevant directory, select the **Policy** tab, and configure the following settings:
  - **Password Free Experience:** Verify that the toggle is NOT enabled.
  - **Password Age:** Specify the period of time before the password expires. The maximum supported value is one year.



For more information about the password settings, refer to the Enterprise Connect Passwordless Management Console Admin Guide.

Enabling FIDO User Bypass

FIDO User Bypass allows users set to Bypass Mode in the Management Console to authenticate with Username + Password only. This feature enables uninterrupted remote desktop access to users who are unable to perform MFA (e.g., lost, forgotten or broken FIDO tokens).

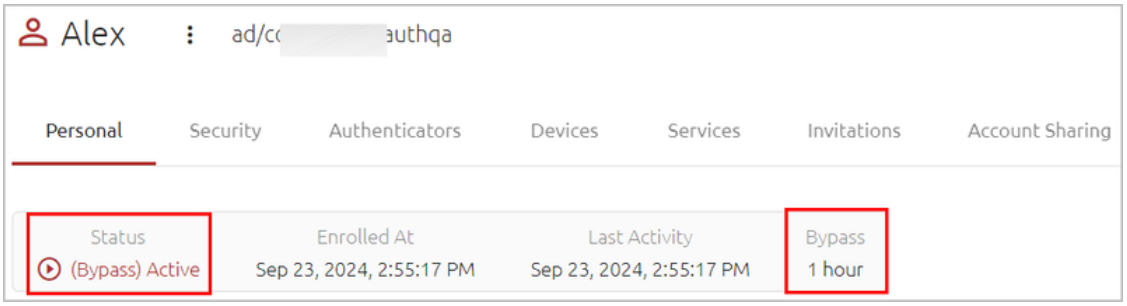
The following sections describe the relevant Management Console configurations, the required MSIUpdater settings, and the user authentication experience in runtime.

Bypassing Users in the Management Console

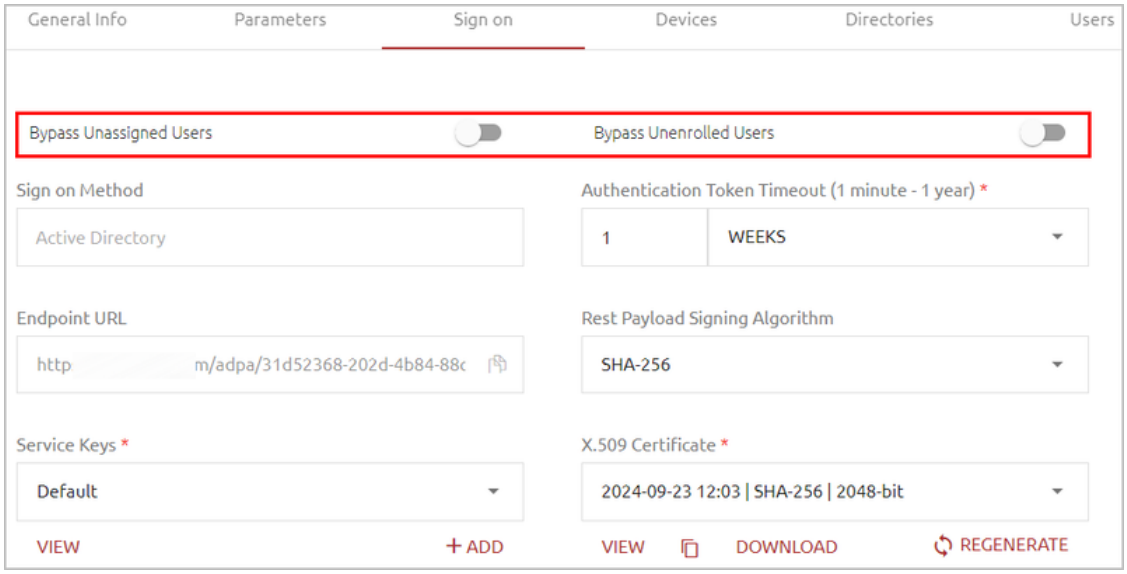
Users can be bypassed at the individual user level or at the service level. For complete details about the Bypass options, refer to the Management Console Admin Guide.

- **To bypass individual users:** Open the **Manage Users** menu, navigate to the relevant user and click the Edit icon to open the user's settings. Then, open the **Security** tab, scroll to the **Authenticators** section, and select **Bypass User > Bypass**.

  The Bypass state is indicated in the user's information bar, and the time remaining until the bypass expires is displayed. For example:



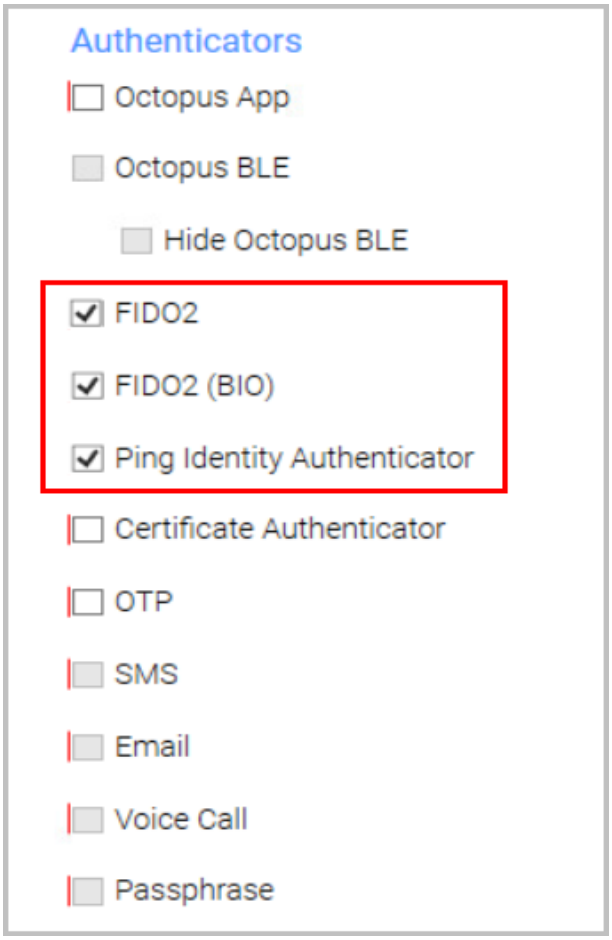
- The following Bypass options are available at the service level, in the **Sign on** tab of the service's settings:
  - **Bypass Unassigned Users:** Allows users who are not assigned to the service to login with username and password.
  - **Bypass Unenrolled Users:** Allows users who are assigned to the system but have not yet enrolled a mobile device or workstation to login with username and password.



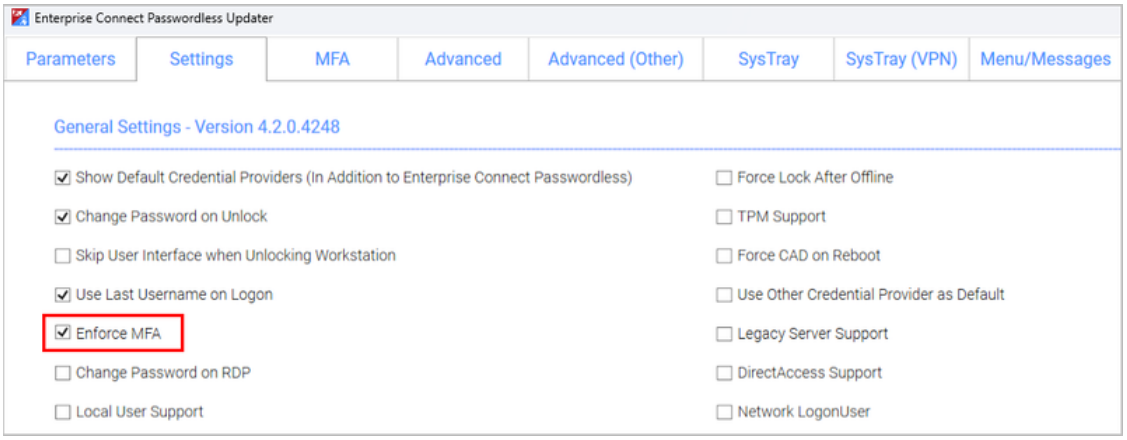
Configuring the MSIUpdater

To enable support for FIDO User Bypass, the following settings need to be configured in the Windows MSIUpdater:

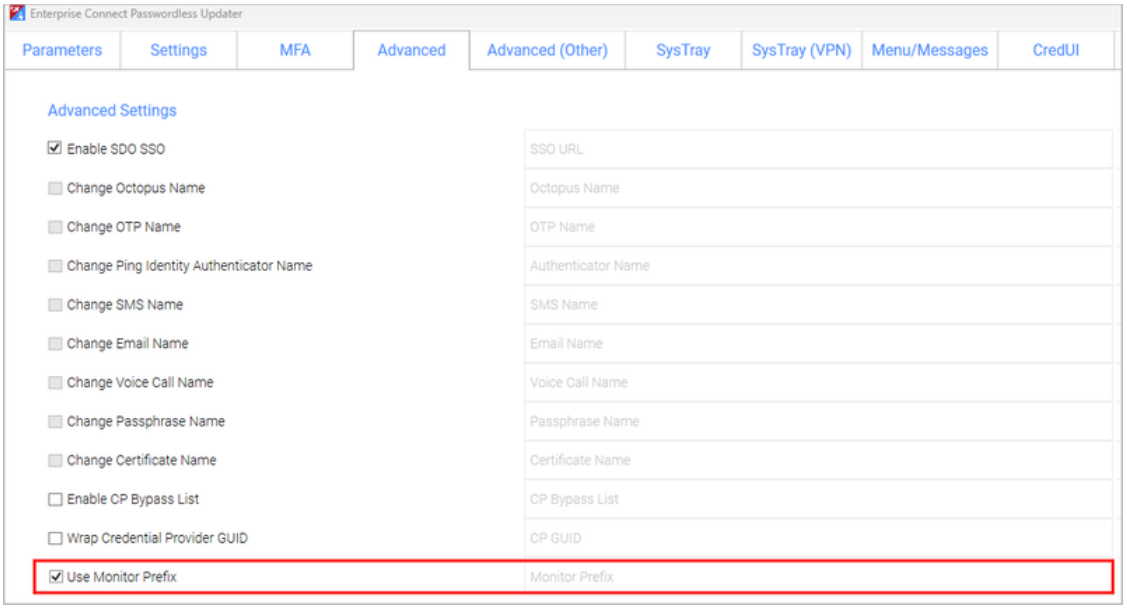
- In the **Authenticators** sections of the **Parameters** tab, select both **FIDO2 / FIDO2 (BIO)** and **Ping Identity Authenticator**.



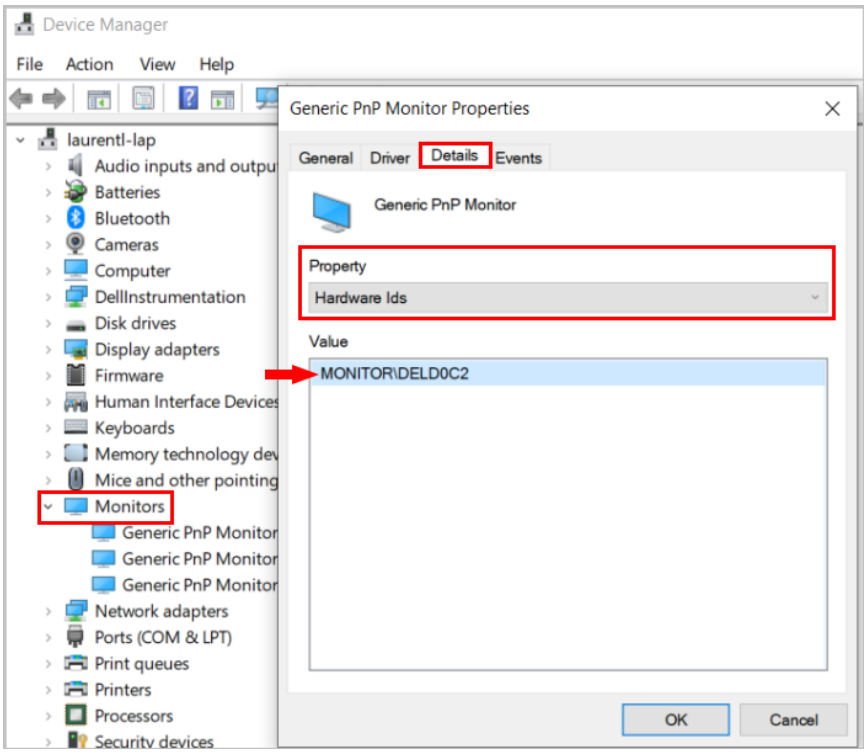
- In the **Settings** tab, select **Enforce MFA**.



- In the **Advanced** tab, select the **Monitor Prefix** checkbox, and then enter the appropriate prefix in the field to the right. In runtime, when there is a prefix match, users are presented with the Enterprise Connect Passwordless login option only. If there is no match, users are presented with the FIDO2 (BIO) and / or FIDO Bypass login options.

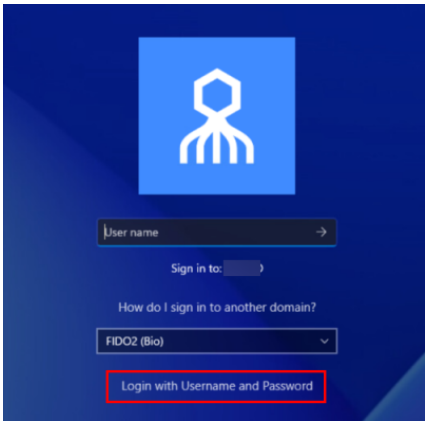


You can find the prefix in the Windows Device Manager. Under **Monitors**, open the properties of the monitor. Then, in the **Details** tab, select the *Hardware Ids* property.

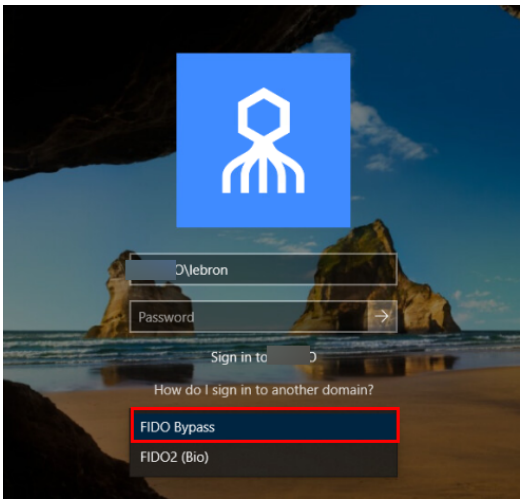


User Authentication Experience

When FIDO User Bypass is enabled, users in Bypass Mode need to click **Login with Username and Password**.



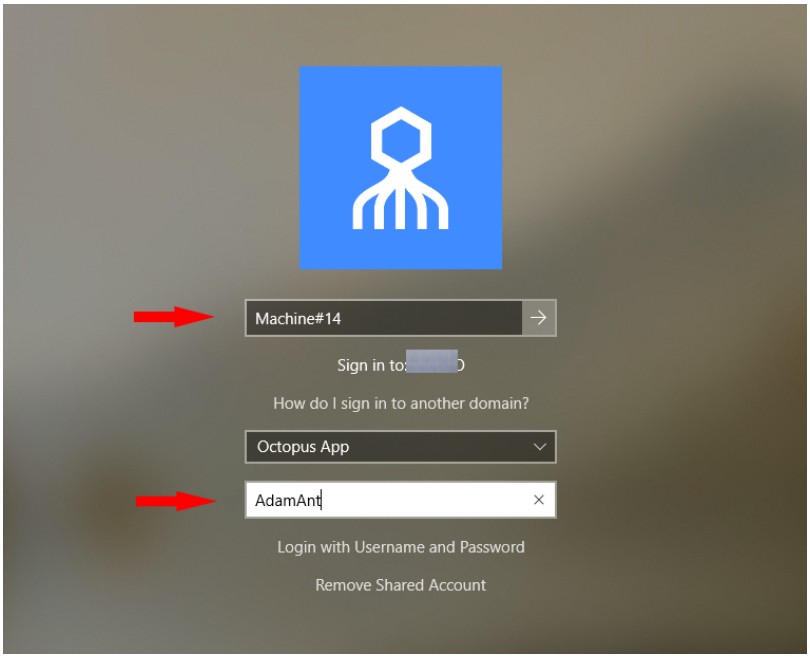
After selecting the **FIDO Bypass** login option, they enter a username and password to authenticate to Windows.



Enabling Shared Account Login

The Shared Account feature enables designated users to log into a generic account on a shared workstation using their personal credentials and devices. Account sharing is particularly useful for specific groups of personnel (such as IT, DevOps, manufacturing floor workers, etc.) who use a shared workstation.

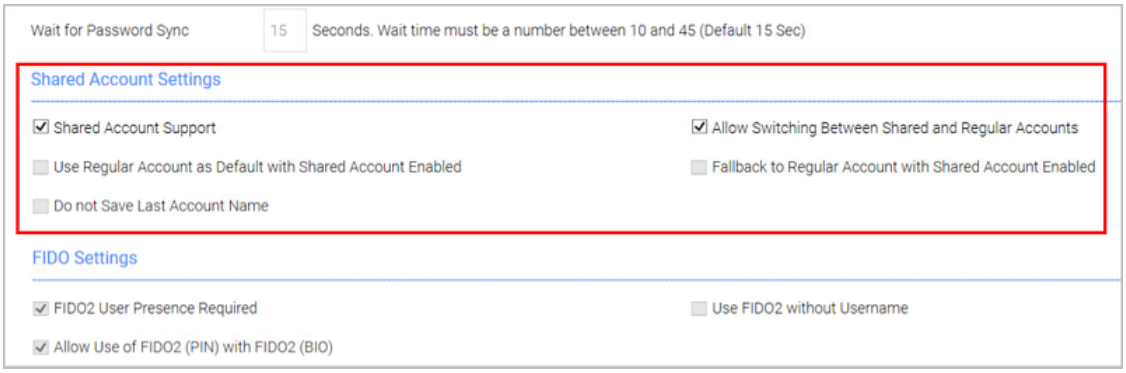
When account sharing is activated, users who are authorized to access the account enter two usernames on the Login screen: the name by which the shared account is known (e.g., Machine#14), and their own username. They then complete the login process by authenticating with their personal mobile device, FIDO key, etc.



To enable support of shared accounts, some configuration needs to be done in the Windows MSIUpdater and in the Enterprise Connect Management Console.

Windows MSIUpdater Configuration

To enable shared account login, in the **Settings** tab of the MSIUpdater, scroll to **Shared Account Settings** and select the **Shared Account Support** checkbox.



To enable users to choose either a shared account login flow or a standard login flow (to a non-shared account), select the
Allow Switching Between Shared and Regular Account checkbox. When this setting is enabled, a link will appear on the Windows Login screen
(**Remove Shared Account** / **Use Shared Account**) allowing users to switch between the two options.

By default, when switching is allowed, the Windows Login screen presents the shared account login flow. To override this behavior, select the
Use Regular Account as Default in Shared Account Enabled checkbox. When the

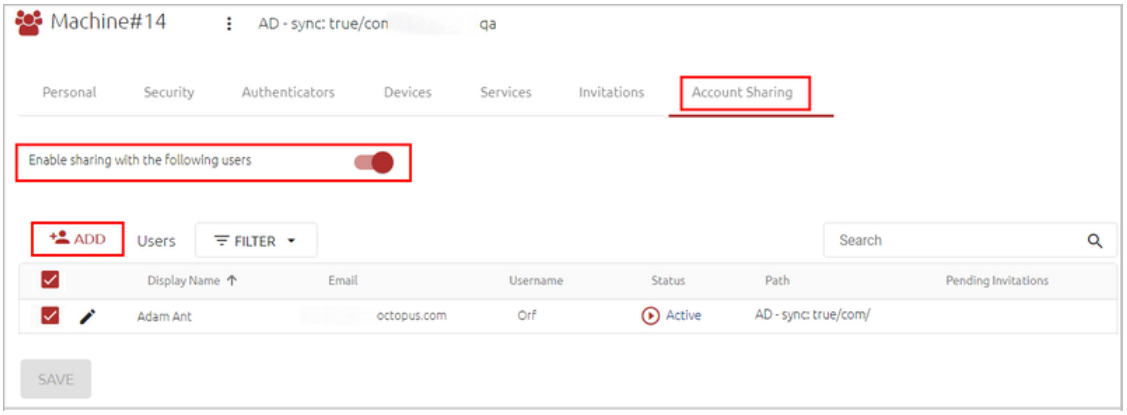
Fallback to Regular Account with Shared Account Enabled checkbox is also selected, the Windows Login display always returns to the standard (regular account) login flow, even when the last login / unlock was to a shared account.

Management Console Configuration

Shared user accounts are designated and managed from the user details of the relevant account.

To activate account sharing:

1. From the **Manage Users** menu of the Management Console, navigate to the relevant user and click ✎ to open the user details.
2. From the **Account Sharing** tab, select the **Enable sharing** toggle button.



3. To allow users to log into the shared account, click **Add** and select the relevant user(s) from the dialog that opens.

Once users are added, you can temporarily block their access to the account when required, by clearing the checkbox in the row of the relevant user(s).

You can also temporarily disable account sharing when necessary by deselecting the **Enable sharing** toggle. The list of approved users will remain intact while sharing is disabled, so you can quickly and easily reactivate account sharing with those users.

For more details about shared accounts, refer to the Enterprise Connect Passwordless Management Console Admin Guide.

Windows Authentication Methods

Once installation is completed, users will be able to authenticate to Windows machines using Enterprise Connect Passwordless Authentication, FIDO key authentication or OTP.

- For passwordless authentication, users should enter a username and then press **<Enter>**.
- For authentication using MFA, users should enter a username + password and then press **<Enter>**.

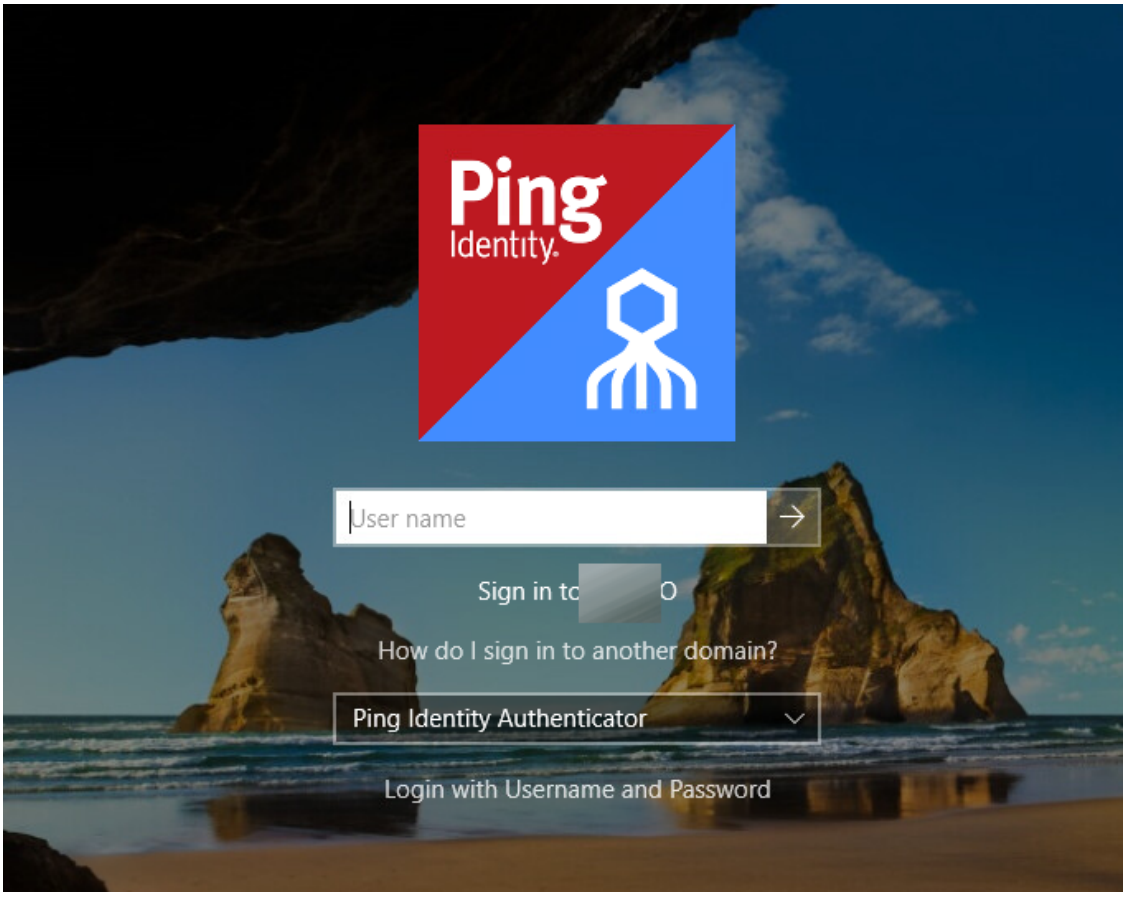
Users can choose from a wide variety of login methods, both online and offline (in the event that a enterprise network is not available). **Online** login methods are listed and described in the following table.

Authentication Method	User Experience (On mobile)	User Experience (Not on mobile)
PingID/ForgeRock mobile app	• Passwordless: Username + PingID/ForgeRock (Push) • MFA: Username + Password + PingID/ ForgeRock (Push)	N/A
FIDO	N/A	• Passwordless: Username + PIN + FIDO Authenticator (touch) • MFA: Username + Password + FIDO Authenticator (touch)
Username + Password	For Bypass users only	For Bypass users only
Username + Temporary token	For Bypass users only	For Bypass users only
ForgeRock online OTP	**MFA**: Username + Password + OTP	N/A
Username + Password + SMS	**MFA**: Username + Password + SMS OTP	
Username + Password + Email	N/A	MFA: Username + Password + Email OTP

When a enterprise network is unavailable, or mobile is not available, users can login using any of the following **offline / off network** methods:

Authentication Method	User Experience (On Mobile)	User Experience (Not On Mobile)
Username + Password	For Bypass users only	For Bypass users only

Authentication Method	User Experience (On Mobile)	User Experience (Not On Mobile)
FIDO	N/A	• Passwordless: Username + PIN + FIDO Authenticator (Touch) • MFA: Username + Password + FIDO Authenticator (Touch)
PingID/ForgeRock offline OTP	**MFA**: Username + Password + OTP	N/A

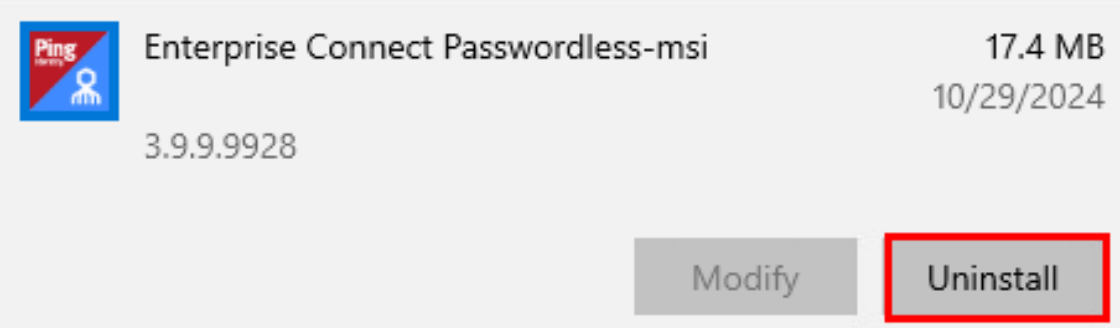


Uninstalling Enterprise Connect Passwordless for Windows

You may uninstall Enterprise Connect Passwordless via the system Settings or via the command line.

Uninstalling via System Settings

Using Admin permissions, navigate to **Settings > Apps.** Select Enterprise Connect Passwordless from the list of installed programs and uninstall it.



Uninstalling via the Command Line

Run the following command to uninstall Enterprise Connect Passwordless for Windows:

C:\> msiexec /x {F88FAA40-72B9-4CE0-88DA-6592EF361C94}

Appendix A: Remote Desktop Windows Login

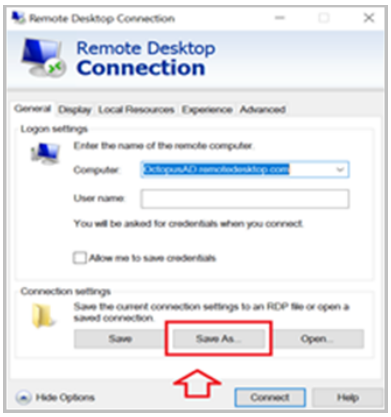
To enable remote desktop login, the following additional configurations are required.

Editing the Remote Desktop Script

The following procedure explains how to make required edits to the RDP script.

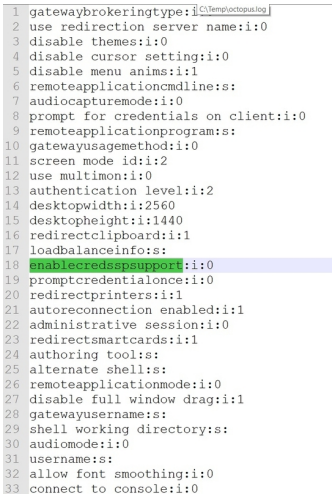
To edit the RDP script:

1. Launch a Remote Desktop Connection.
2. Select the remote computer and click **Show Options**.
3. Under **Connection Settings**, click **Save As** and save the RDP script.



4. Add the following line to the script:

enablecredssp support:i:0



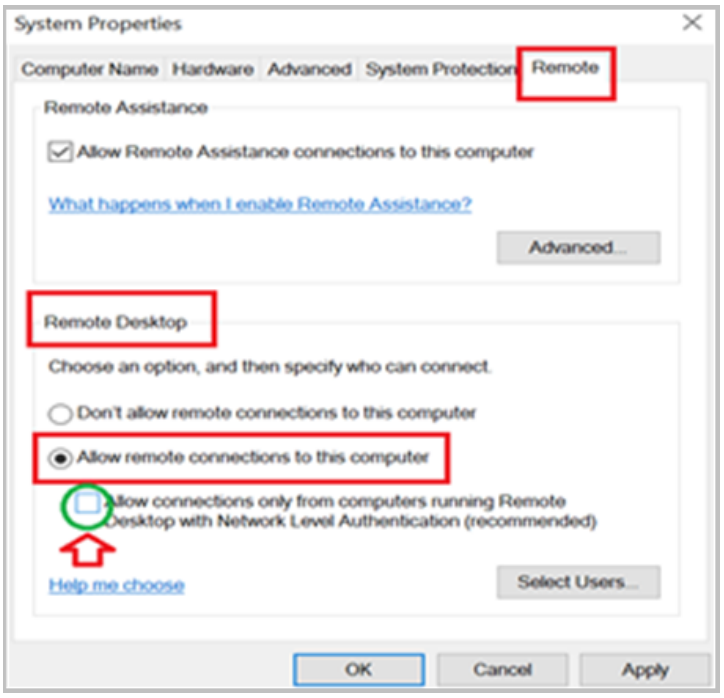
5. Save the script.

Configuring Windows PC System Properties Settings

The procedure below explains how configure system protection settings for the remote machine.

To configure system protection settings:

1. Log into the designated remote desktop Windows machine.
2. Open the System Properties Settings application and select the **Remote** tab.
3. Under **Remote Desktop**:
    - Select the **Allow remote connections to this computer** radio button
    - Verify that the **Allow connections only from computers running Remote Desktop wit h Network Level Authentication** checkbox is NOT selected.



4. Click **Apply**.

Appendix B: Importing the Self-signed Certificate

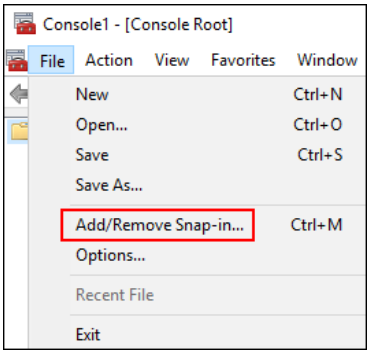
The self-signed certificated can be found on the Authentication Server in the following location: **/etc/pki/nginx/selfsigned.crt** This certificate should be copied to the Windows environment to allow the self-signed certificate to work with Enterprise Connect Passwordless for Windows.

The self-signed certificate should be imported to the root certificate folder on the Windows machine that is using Enterprise Connect Passwordless.

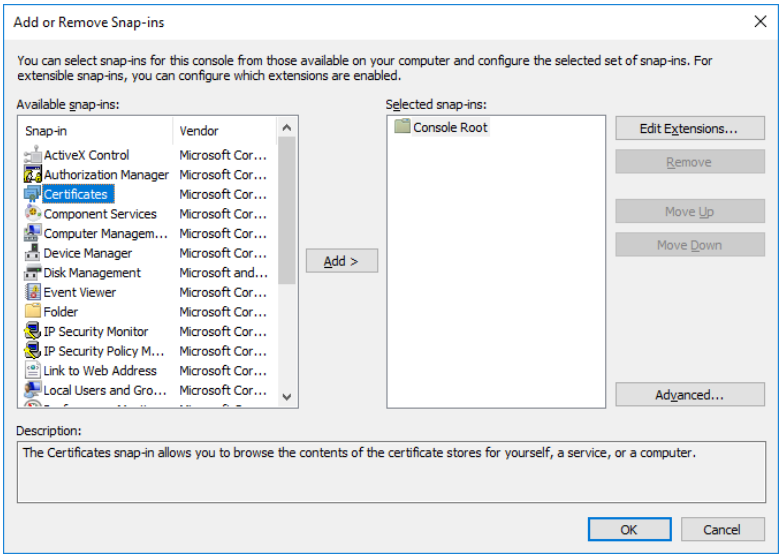
Note: This action should be done for POC purposes and not for the production environment.

To import the self-signed certificate:

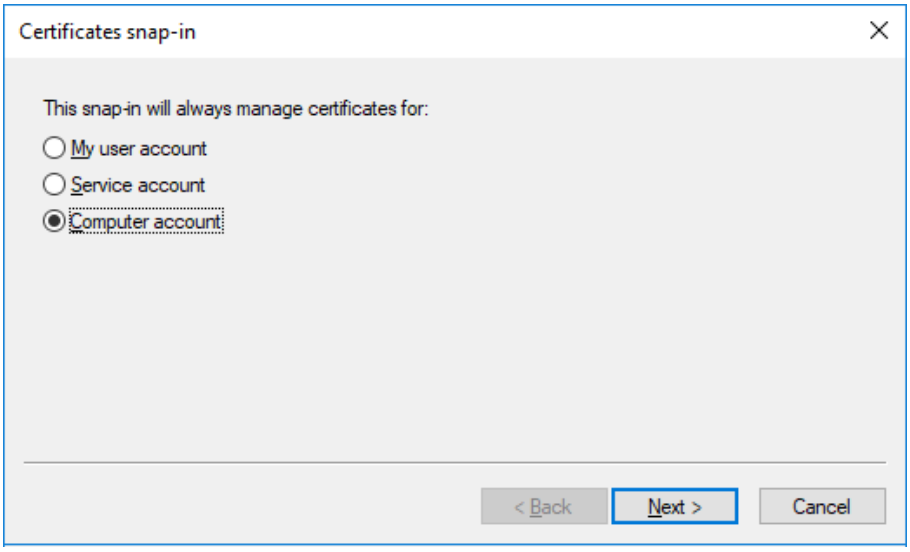
1. Open the Microsoft Management Console (mmc.exe).
2. From the **File** menu, select **Add/Remove Snap-in**.



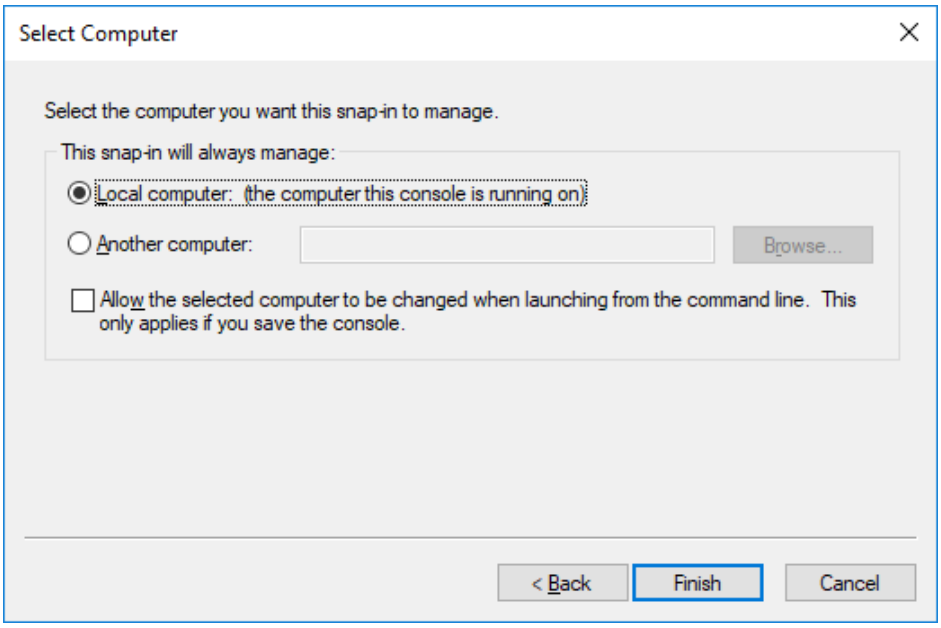
Then, double-click **Certificates**.



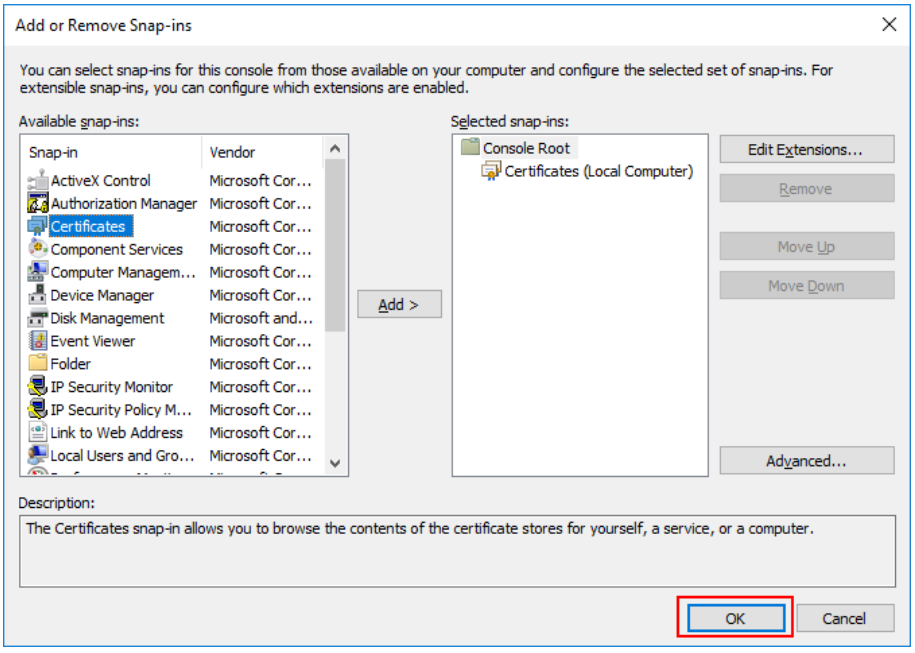
3. From the Certificates snap-in wizard, select the **Computer account** radio button. Then, click **Next**.



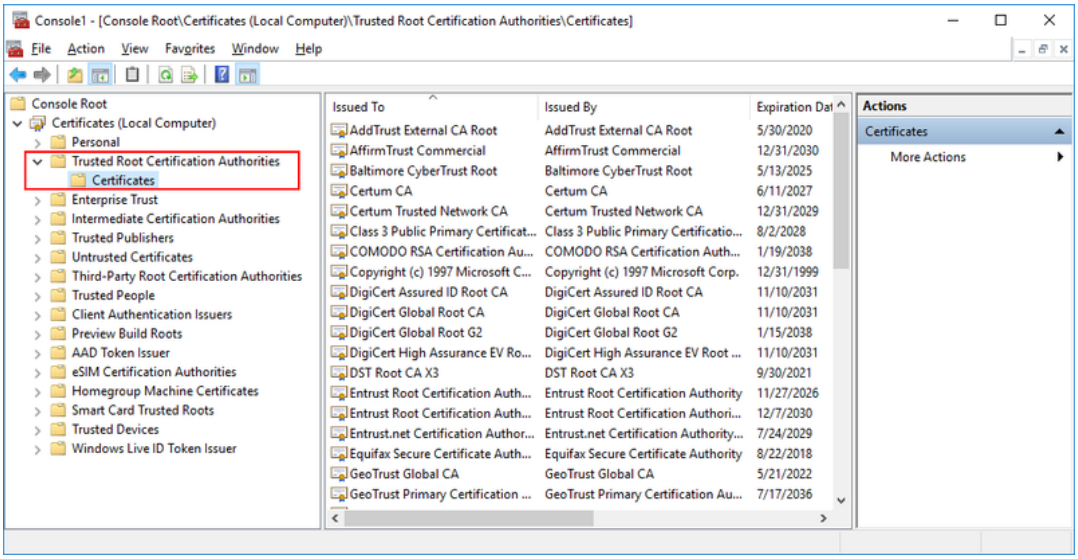
4. Select the **Local computer** radio button. Then, click **Finish**.



5. At the bottom of the **Add or Remove Snap-ins** dialog, click **OK** to close the dialog.



6. From the Certificates tree, select
Trusted Root Certification Authorities > Certificates.

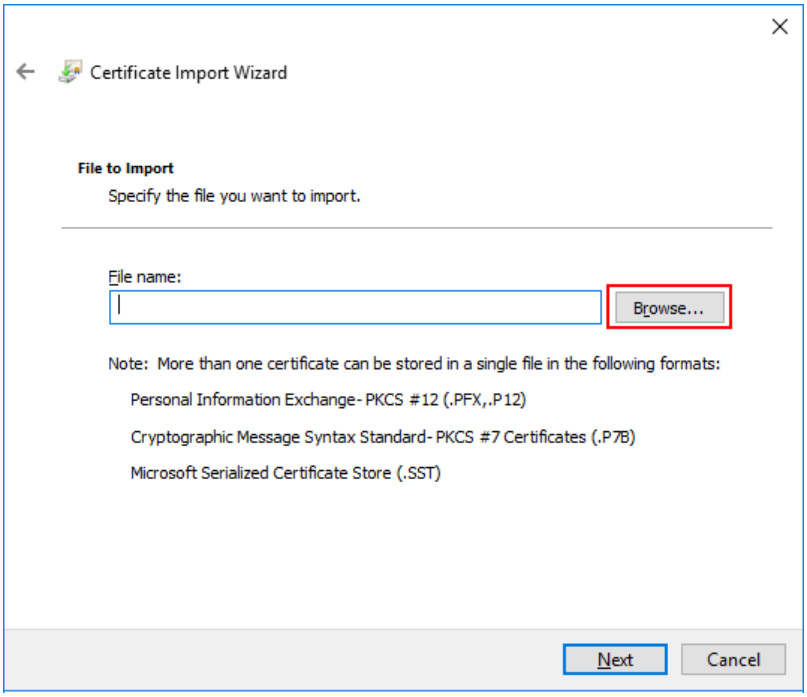


7. Right-click on **Certificates**, and select **All Tasks > Import**.

   The Certificate Import Wizard opens.

8. On the first page of the wizard, click **Next**.

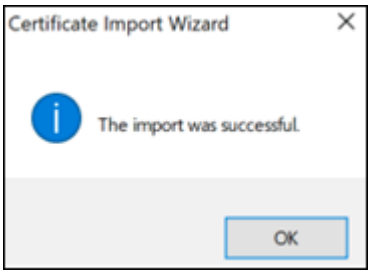
9. Click **Browse** and select the self-signed certificated (copied from the Linux server).



   Then, click **Next**.

10. Select the **Place all certificated in the following store** radio button. Then, click **Next**.
11. After reviewing the certificate details, click **Finish**.

    A confirmation message is displayed.



12. In the **Certificates** node, verify that the new certificate appears in the list of certificates.

Appendix C: Enabling / Disabling the Enterprise Connect Passwordless Authentication CP Post-installation

Enterprise Connect Passwordless for Windows supports the ability to control availability of the Enterprise Connect Passwordless credential provider (CP) on target machines after installation. This feature allows for bulk installation, followed by gradual deployment on group / user workstations.

Workstations on which the Enterprise Connect Passwordless CP is manually disabled post-installation will not support Enterprise Connect Passwordless Authentication as a means of logging into Windows. The installation of Enterprise Connect Passwordless will be transparent to users, who will not see the Enterprise Connect Passwordless CP on the Login screen and will continue to login as they did prior to installation.

To disable Enterprise Connect Passwordless Authentication CP post-installation, use the following syntax:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenti
cation
\Credential Provider Filters\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SDOCredentialProvider"
"Disabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenti
cation
\Credential Providers\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
```

```
@="SDOCredentialProvider"
"Disabled"=dword:00000001
```

To enable Enterprise Connect Passwordless Authentication CP, use the following syntax:

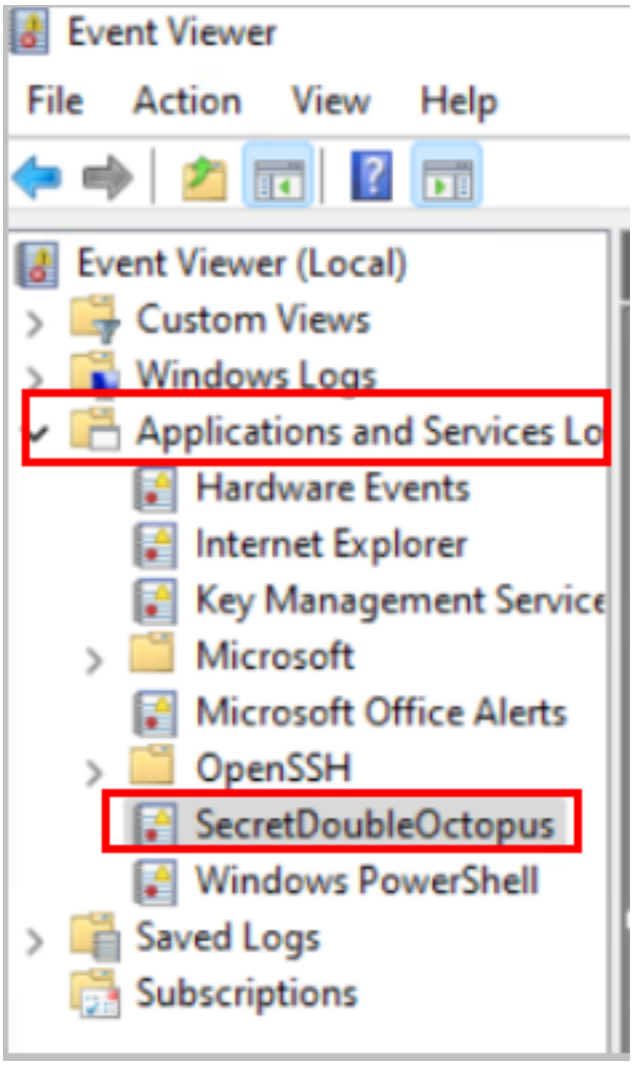
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenti
cation
\Credential Provider Filters\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SDOCredentialProvider"
"Disabled"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenti
cation
\Credential Providers\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SDOCredentialProvider"
"Disabled"=dword:00000000
```

Appendix D: Troubleshooting

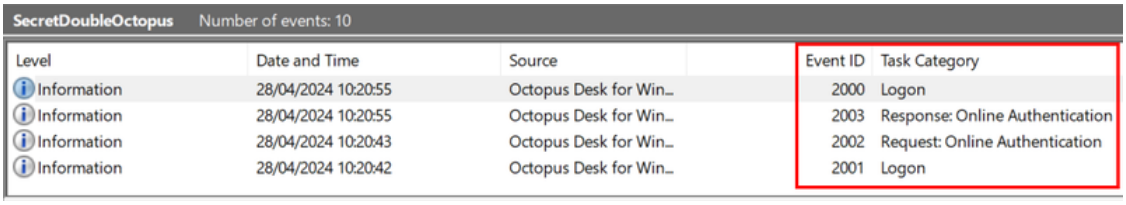
This section provides guidance for understanding the audit records and for handling issues that you may encounter when working with Enterprise Connect Passwordless for Windows.

Viewing Windows Agent Events

You can view the Windows Agent logs at any time (there is no need to stop the service). To view events, open the Windows Event Viewer and navigate to **Applications and Service Logs > SecretDoubleOctopus**.



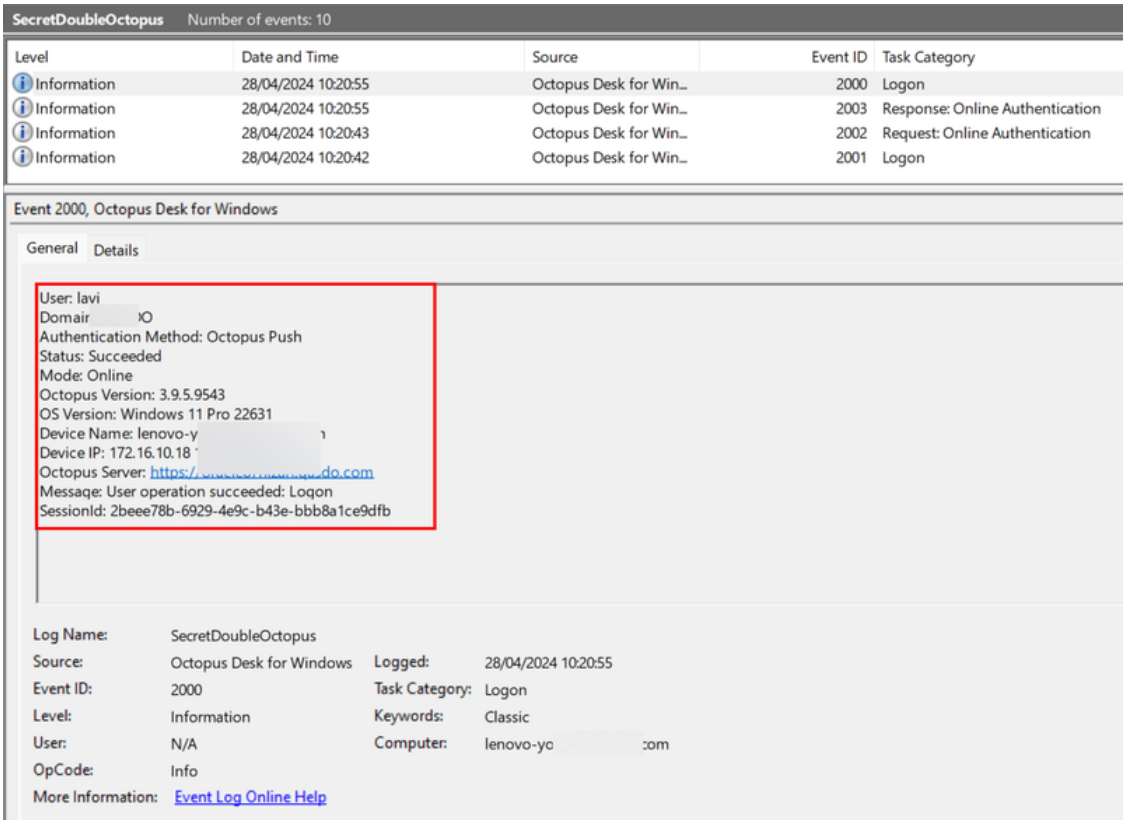
The upper portion of the Event Viewer shows a summary of the events associated with each authentication session. The ID (code) and category of each event are clearly displayed, enabling you to quickly and easily follow the authentication flow.



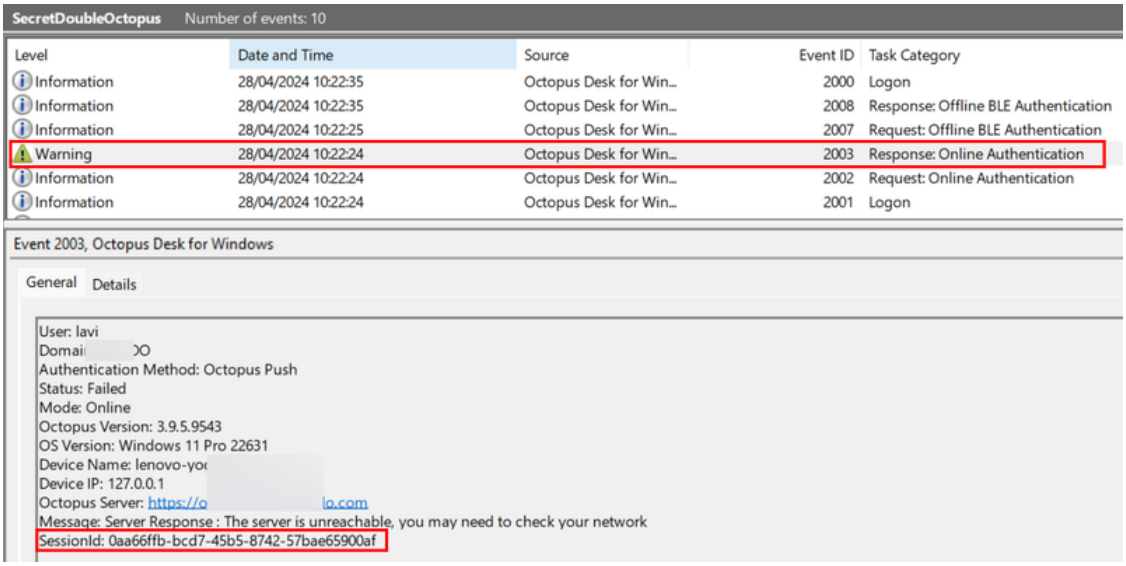
SecretDoubleOctopus Number of events: 10

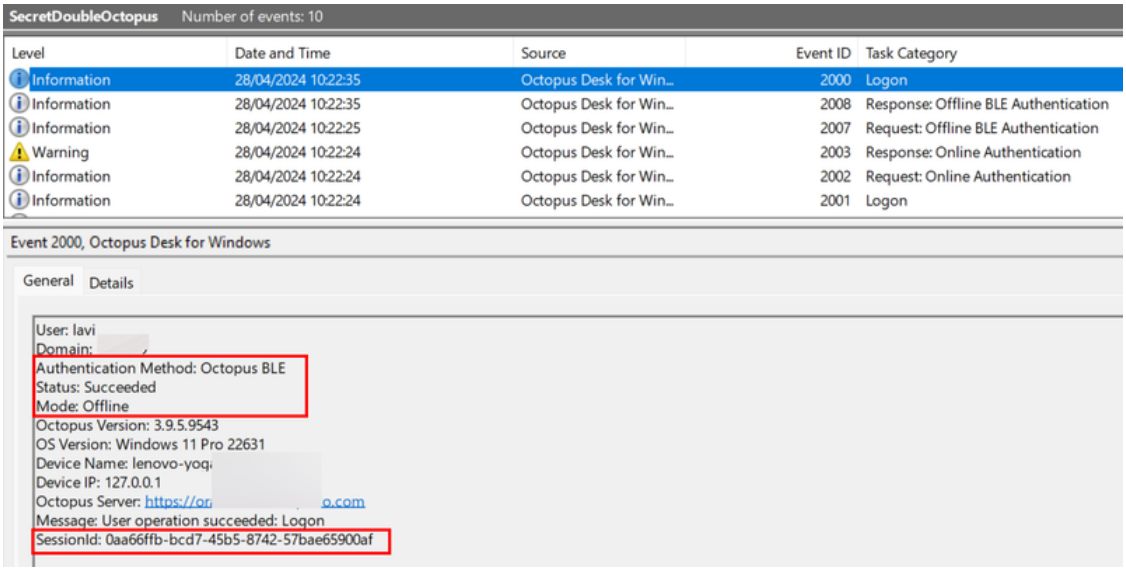
Level	Date and Time	Source	Event ID	Task Category
Information	28/04/2024 10:20:55	Octopus Desk for Win...	2000	Logon
Information	28/04/2024 10:20:55	Octopus Desk for Win...	2003	Response: Online Authentication
Information	28/04/2024 10:20:43	Octopus Desk for Win...	2002	Request: Online Authentication
Information	28/04/2024 10:20:42	Octopus Desk for Win...	2001	Logon

Clicking a row allows you to view additional details about the selected event, including status, device info, and Session ID.



The following figures show an example of unsuccessful online authentication (due to a network issue) followed by successful offline BLE authentication. Note the identical Session ID for the online and offline flows.





List of Event Codes

The following table lists the event codes, descriptions and corresponding messages (if relevant). For additional resources and advanced troubleshooting guidelines, please visit the Secret Double Octopus Support Center.

> **Note**
>
> If you require more advanced troubleshooting and/or debugging, you may need to download the full Windows Agent logs. Keep in mind that the process will require stopping the service.

Event Code	Event Description	Message to User
1000	Internal use	N/A
1001	Token is not valid	We cannot verify your identity. Please contact your administrator.
1002	Server Error	System error. Please try again later or contact your administrator.
1003	Certificate Error	We cannot verify your identity. Please contact your administrator.
1004	Server Reject request	Authentication failed. Please try again later or contact your administrator.
1005	Empty Credentials	Authentication rejected because Credentials are missing.
1006	Registry error	Authentication failed. Please contact your administrator.

Event Code	Event Description	Message to User
1007	Get Certificate Error	Authentication failed. Please contact your administrator.
1008	Network Error	Network error. Please make sure you are connected to the internet. If the problem persists, contact your administrator.
1009	BLE Error	Please verify that Bluetooth is enabled on your mobile and on Windows, and then try again. If the problem persists, use a different authentication method.
1010	BLE Client Reject request	Authentication failed. Try again and approve authentication on your mobile.
1011	User Denied request	Authentication failed. Try again and approve authentication on your mobile.
1012	User Bypass not allowed	Authentication bypass denied. Try again with a username and password.
1013	Internal use	N/A
1014	Internal use	N/A
1015	No Old Credentials Found	Error finding old credentials. Try again.
1016	FIDO2 Error	Authentication failed. Please check your FIDO token and try again.
1017	Username Password Error	You cannot log into this workstation with a username and password.
1018	Pin Required	Authentication failed. Please enter your FIDO Authenticator PIN.
1019	Timeout no response	Authentication failed. Please try again.
1020	Local Credentials Set Error	Set Local Credentials error.
1021	User Bypass not allowed	Authentication bypass denied. Try again with a username and password.
1022	WebAuthN Error	Authentication failed. Please try again.
1023	OTP passwordless is not allowed	A one time password cannot be used for passwordless authentication.

Event Code	Event Description	Message to User
1024	OTP expired	Your one time password expired. Please authenticate online and renew your OTP token.
1025	Internal use	N/A
1026	Timeout no response	Authentication failed. Please try again.
1027	MFA Bypass not allowed	MFA Bypass not allowed. Please try again.
1028	NOMEMORY	Your computer needs more memory to run. Contact your administrator.
1029	Credentials Decrypt Error	Can't decrypt credentials.
1030	OTHER	Oops, something went wrong. Please contact your administrator.
1031	Lock for 1 minute	Your computer is locked for 1 minute. Please try again later.
1032	Lock for 30 minutes	Your computer is locked for 30 minutes. Please try again later.
1033	Lock for 1 hour	Your computer is locked for 1 hour. Please try again later.
1034	Locked	Your computer is locked. Please try again later.
1035	Reset Credentials is not set	Reset Credentials is not set. Please contact your administrator.
1036	Credentials are out of sync	Your credentials are out of sync. Please contact your administrator.
1037	Windows Error	Please try again or contact your administrator.
1038	ForgeRock Error	Please try again or contact your administrator.
1040	Server Reject request	Authentication failed. Please try again or contact your administrator.
1041	No Challenge from Server	Authentication failed. Please try again or contact your administrator.
1042	Internal use	N/A
1043	No OTP from Server	Can't retrieve OTP from Server. Please try again later or contact your administrator.

Event Code	Event Description	Message to User
1044	Reserved / Internal	N/A
1045	Certificate Error	Certificate Error. Please try again or contact your administrator.
1046	Sign-in method isn't allowed	Sign-in method isn't allowed. Please try again or contact your administrator.
1047	Offline Login Error	Offline Login Fail. Please try again or contact your administrator.
1048	Your account is restricted	Your account is restricted. Please contact your administrator.
1049	Bypass token not supported	Bypass token not supported. Please contact your administrator.
1050	Wrong user format	Azure Login Wrong User Format. Please use UPN.
1052	Fingerprint error	Can't read fingerprint. Please try again.
1053	Enhanced Assurance Server error	Server returned wrong info for Enhanced Assurance. Please contact your administrator.
1054	Enhanced Assurance Server error	Mobile returned wrong info for Enhanced Assurance / Not found. Please contact your administrator.
2000	User action successful	
2001	User action initiated	
2002	Initiating Authentication Server call	
2003	Authentication Server call result	
2004	Notification from Authentication Server	
	"Password changed by Server"	
2005	Request to FIDO Server	
2006	Response from FIDO Server	

Event Code	Event Description	Message to User
2007	Request to mobile app over BLE	
2008	Response from mobile app over BLE	
2009	Offline certificate authentication	
2010	User clicked on popup dialog	
2011	Offline OTP authentication	

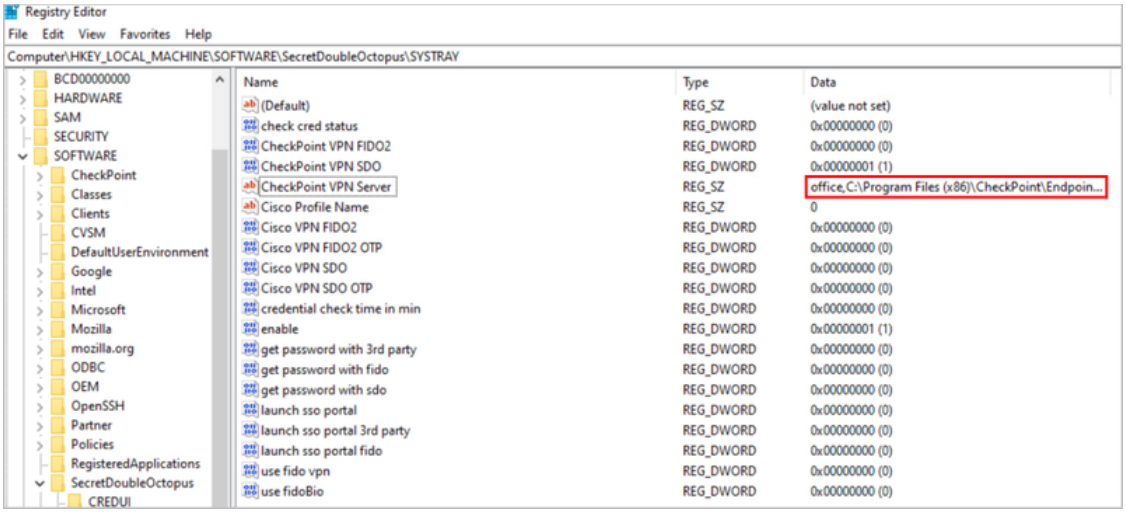
Launching the Check Point VPN from the Systray

Check Point Harmony users may encounter difficulty when attempting to open the VPN from the Windows systray. This issue can also occur when your VPN is installed in multiple locations.

To resolve this issue, check the configurations described below.

MSIUpdater Configuration

In the **Systray** tab of the MSIUpdater, verify that the site / profile name of the VPN is followed by a comma and the full path of the VPN client. The correct format can be viewed in the Registry Editor. For example:



Endpoint Security Configuration

In the properties of your VPN Server, make sure that the **Enable Always-Connect** checkbox is NOT selected.