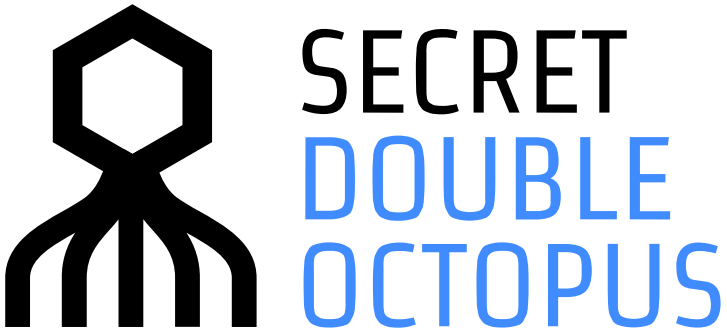
JUNE 7, 2021



Octopus Desk for Windows Installation Guide Version 3.4

FOR OCTOPUS AUTHENTICATION SERVER V4.8 AND ABOVE

CONTENTS

Preface

This document provides step by step installation instructions for Octopus Desk for Windows.

Product Overview

Secret Double Octopus replaces passwords altogether with a high assurance, password-free authentication paradigm. Using the Secret Double Octopus 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.

Prerequisites

Before beginning installation, verify that:

- Octopus Authentication Server **v4.8 (or higher)** is installed and operating with a valid enterprise certificate
  Note: If your version is below 4.8, please continue to work with Octopus Authentication for Windows version 3.3. (Octopus Desk for Windows v3.4 does not support Server versions below 4.8.)
- **For Active Directory**:
  - Corporate Active Directory 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., OKTA, ORACLE)

- Enrolled users are assigned to use one or more authentication methods -- Octopus Authenticator, FIDO Authenticator, 3rd party authenticator (Okta, ForgeRock or OTP)
- Workstations support TPM version 2.0
- The Octopus Desk for Windows MSI and MSIUpdater packages have been obtained from the Secret Double Octopus team
- For installation via software distribution tools, **Visual C++ 2015-2019 Redistributable (x64)/(x86) - 14.28.29325** is required.

IMPORTANT: To successfully perform MSI upgrade, the MSI file must have the same filename as that of the original installation. The MSI updater creates an MSI file with the update date in the filename. We recommend renaming this file to match the name of the original installation file.

NOTE: Octopus Desk for Windows is delivered in **MSI format only**. The standalone installation (.exe) is no longer available as part of the release.

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

Octopus Desk for Windows supports the following Windows versions: Windows 8, 10 and Windows Servers 2012, 2016 and 2019.
For information about required updates for Windows 8.1, refer to Appendix C: Windows 8.1 Registry Update.

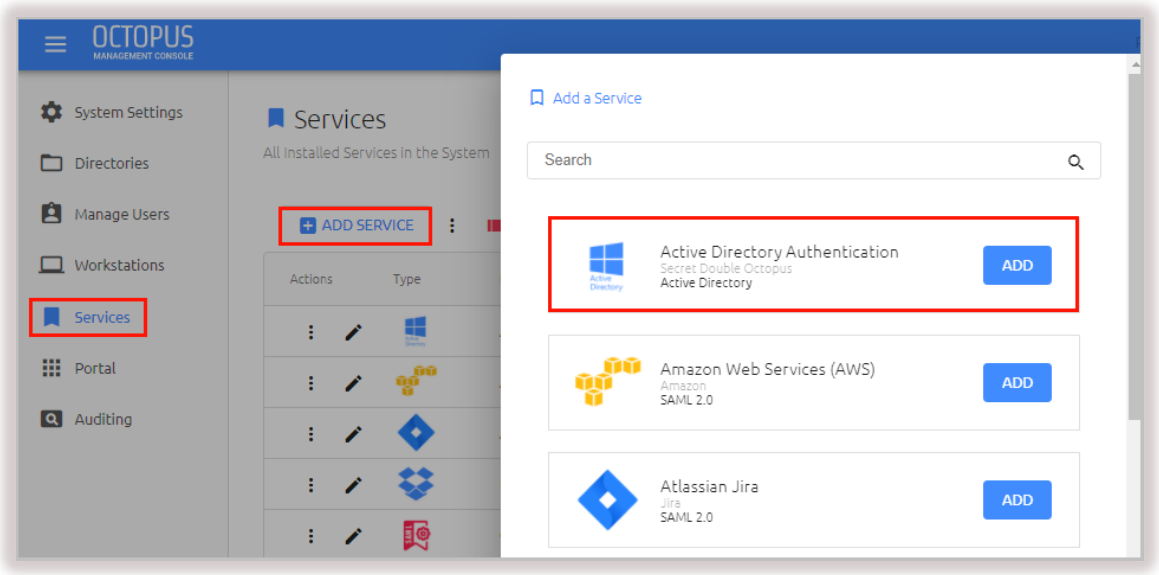
Creating the Active Directory Authentication Service

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

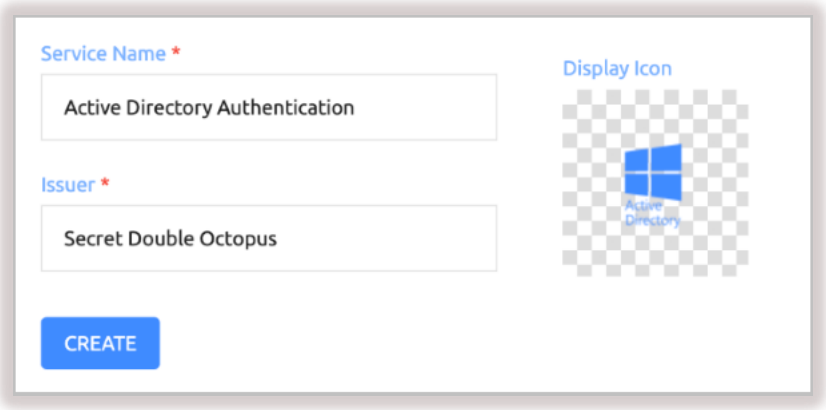
IMPORTANT: Before starting this procedure, verify that you have integrated your Corporate Active Directory (or third-party directory, e.g., Okta) with the Octopus Management Console. Refer to the Octopus Management Console Admin Guide (version 4.8 and above) for detailed instructions on integrating Active Directory and other directory types.

To create the Active Directory Authentication service:

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

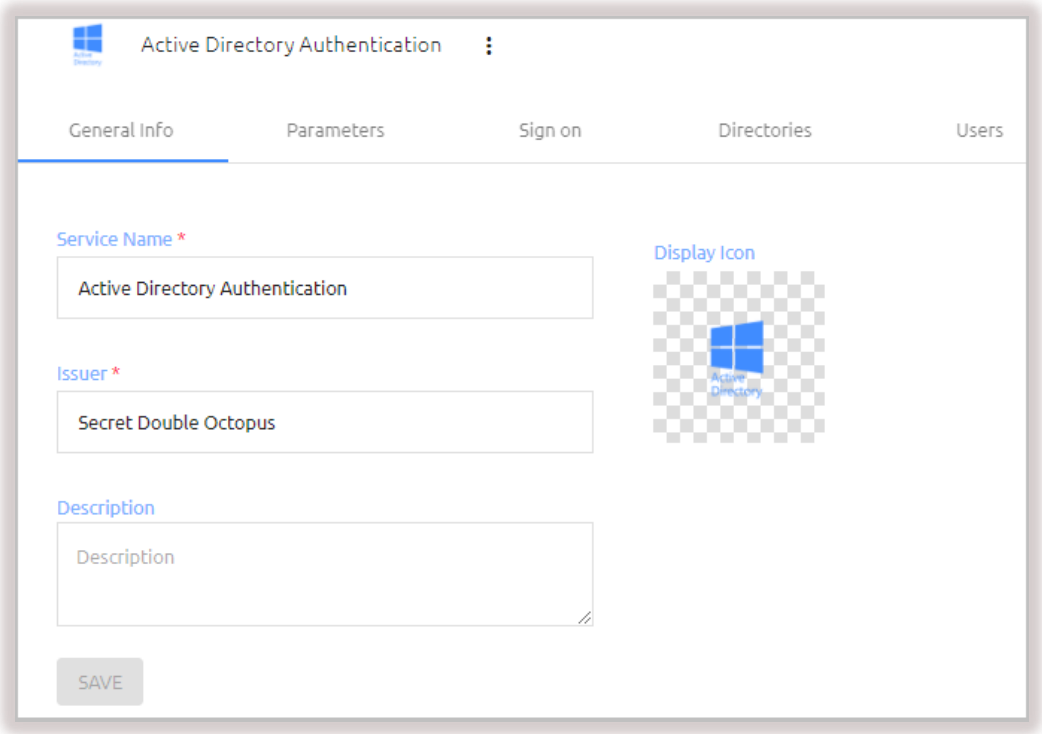


Then, in the dialog that opens, click **Create**.

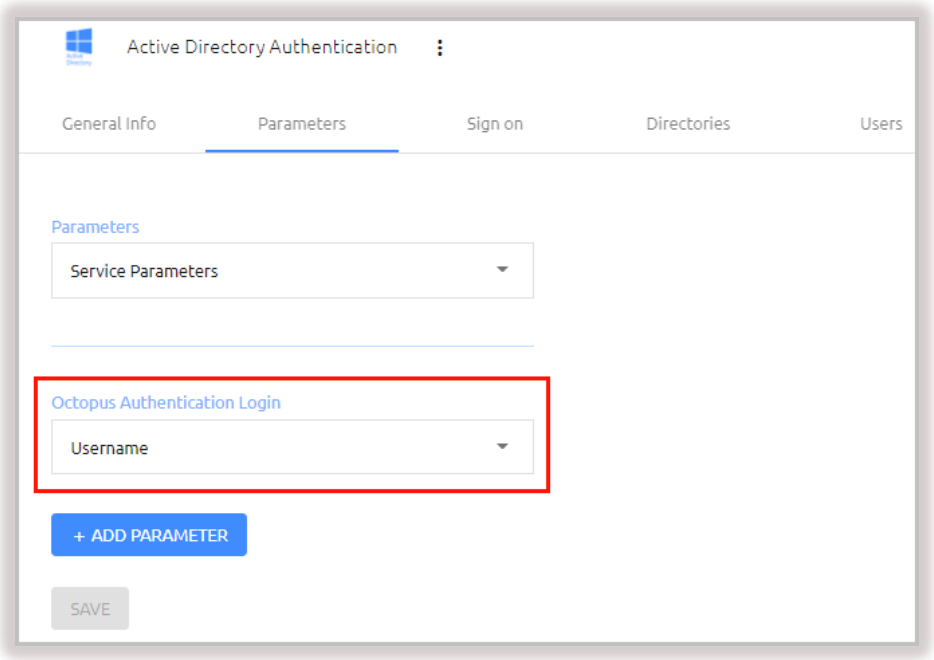


3. Review the settings in the **General Info** tab. If you make any changes, click **Save**.

Setting	Value / Notes
Service Name / Issuer	Change the default values if desired.
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 icon of your choice. JPG and PNG formats are supported.



4. Open the **Parameters** tab. From the **Octopus Authentication Login** dropdown list, select the credential type that will be sent by the user for the authentication (usually **Username**).

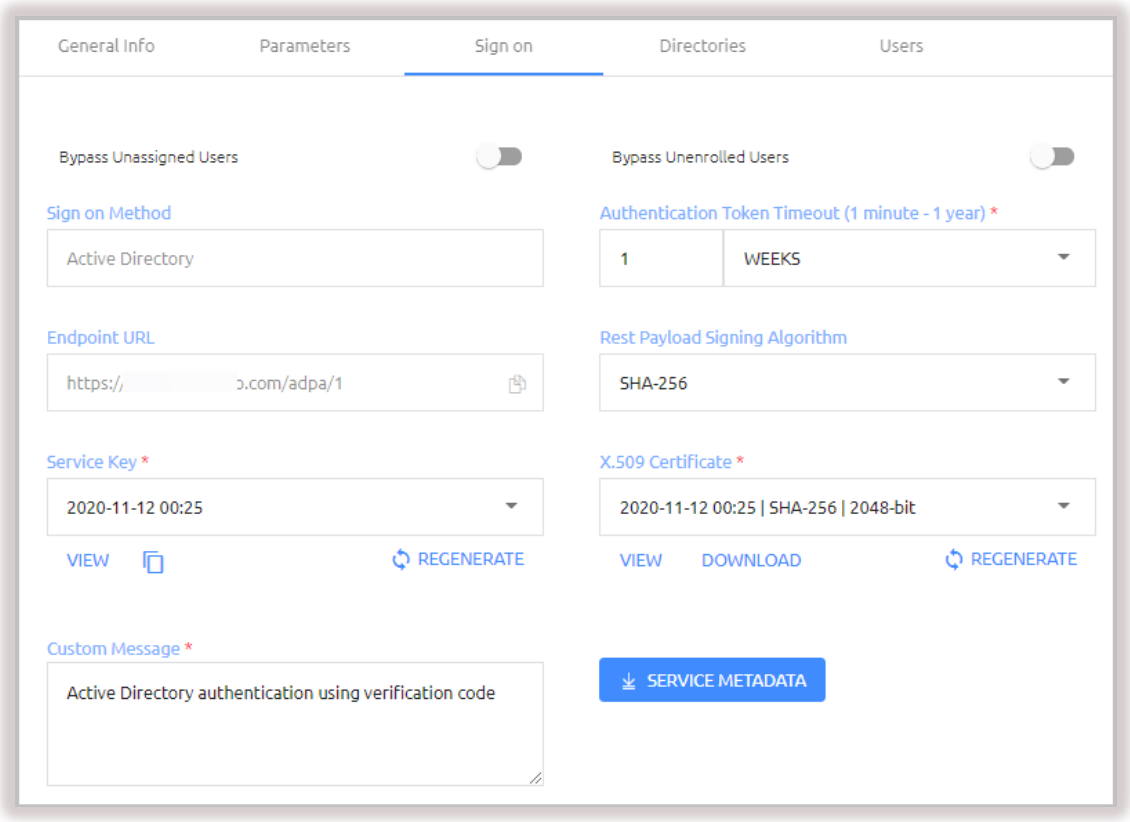


Then, click **Save**.

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

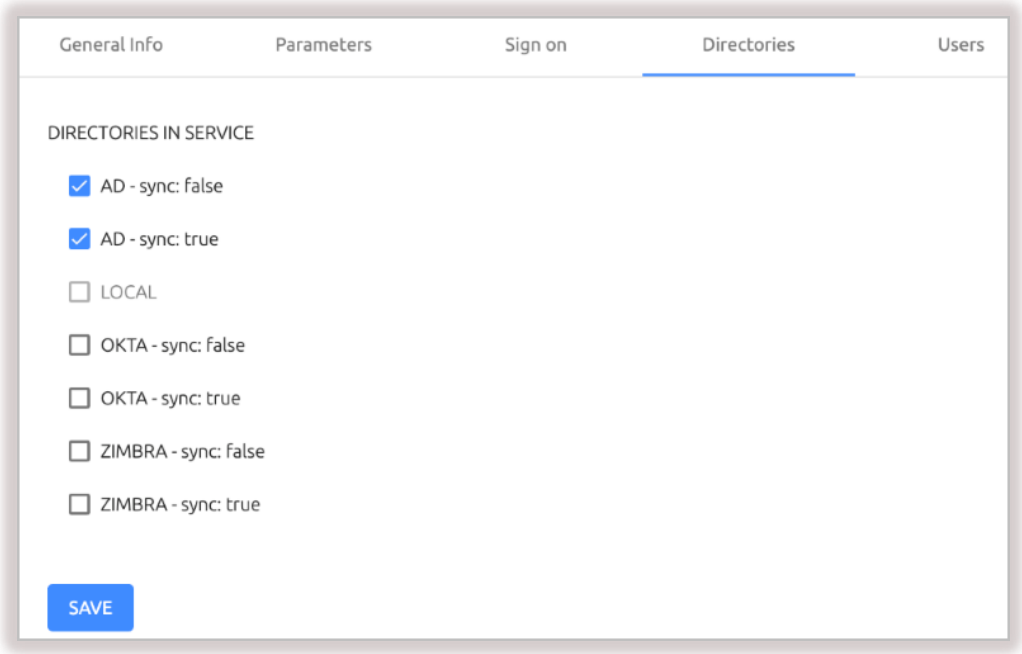
Setting	Value / Notes
Bypass Unassigned Users	When enabled, users who are not assigned to the service will be allowed to login with username and password (without MFA). By default, this option is disabled. The option is usually used on a temporary basis only, during gradual rollouts of Octopus Authenticator.
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 Octopus Authentication Server (not editable). Click the Copy icon to copy the value.
Service Key	Key used by the service to authenticate with Octopus Authenticator. Click **View** to display the content of the key in a popup window. The Copy icon in the popup lets you easily copy the content. To replace the key**,** click **Regenerate.**

Custom Message	Message shown to the user on successful authentication. Use the *%p* tag to display the password in the message.
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**.
X.509 Certificate	The public certificate used to authenticate with Octopus Authenticator. • Click **View** to display the content of the certificate in a popup. • 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.

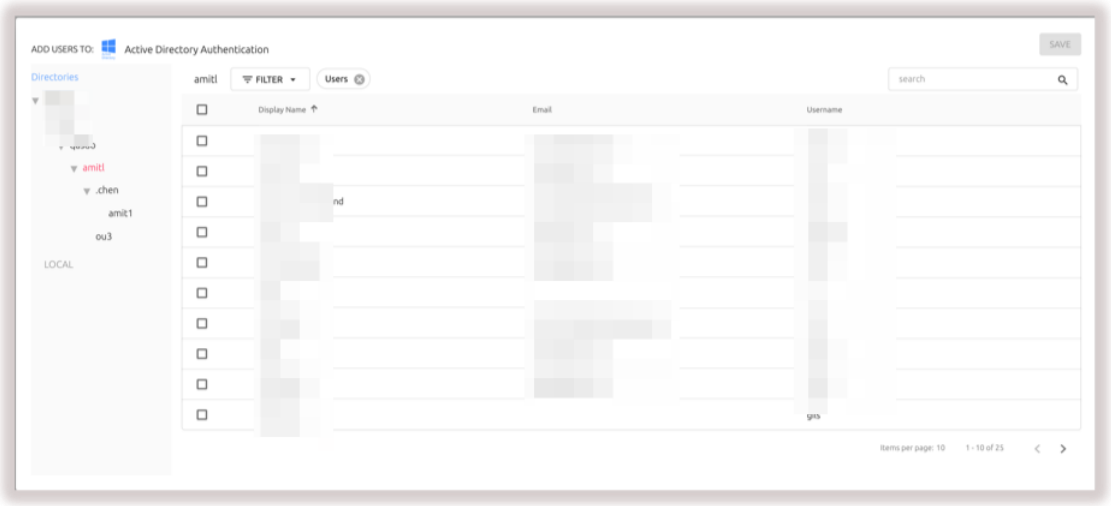


6. At the bottom of the **Sign on** tab, click **Save** (if the button is enabled).

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.



10. 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.
11. At the bottom of the **Users** tab, click **Save**. Then, 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 Octopus Desk 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 Octopus Authenticator

Installing the MSIUpdater Client

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

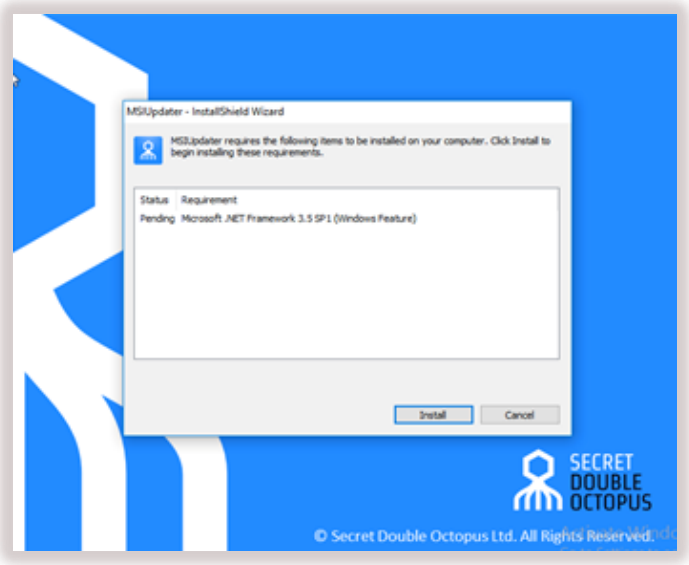
MSIUpdater can run on any Windows client running the following versions: Windows 10, Windows Server 2016 or 2019.

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

To install the MSIUpdater client:

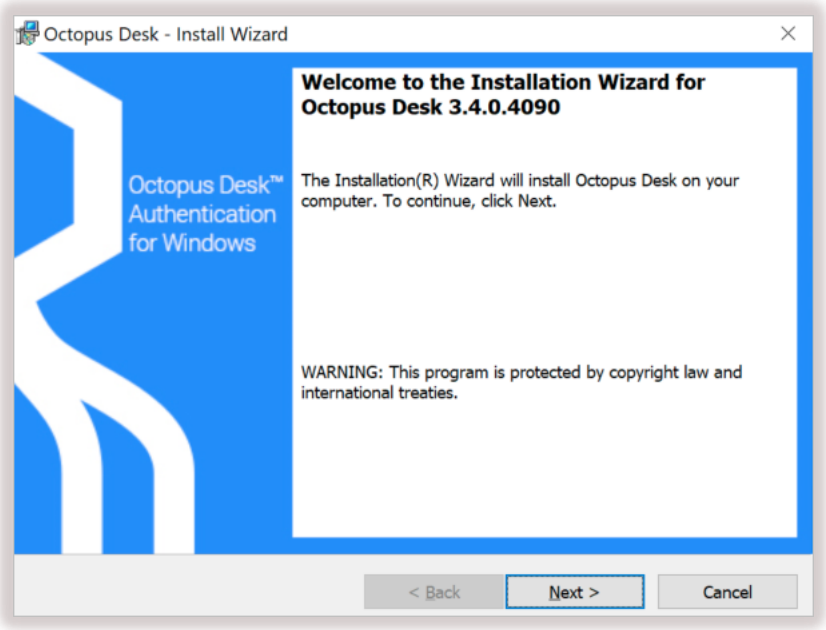
1. Run **MSIUpdater.exe**

   If the Microsoft .NET Framework is not installed, an installer opens.

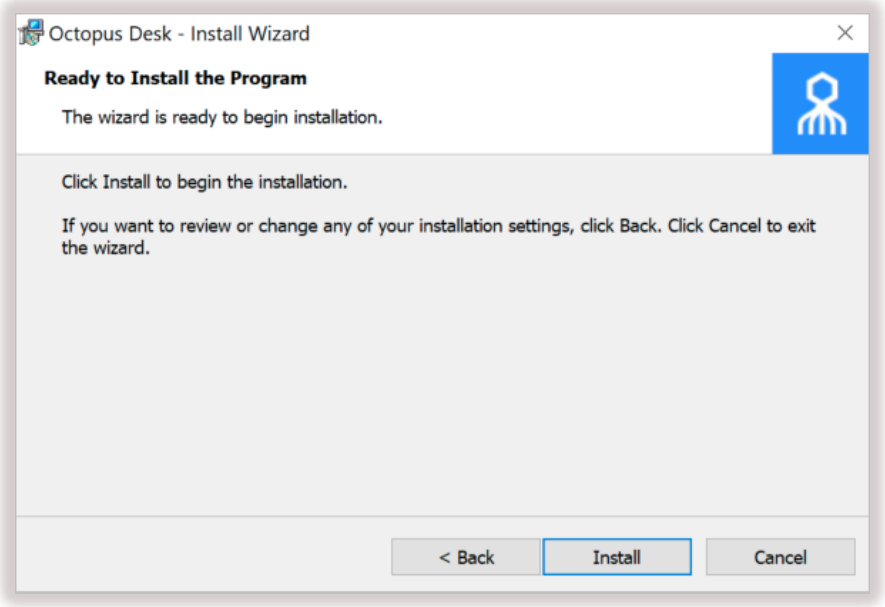


2. To launch the wizard, click **Install**.

3. On the **Welcome** page, click **Next**.

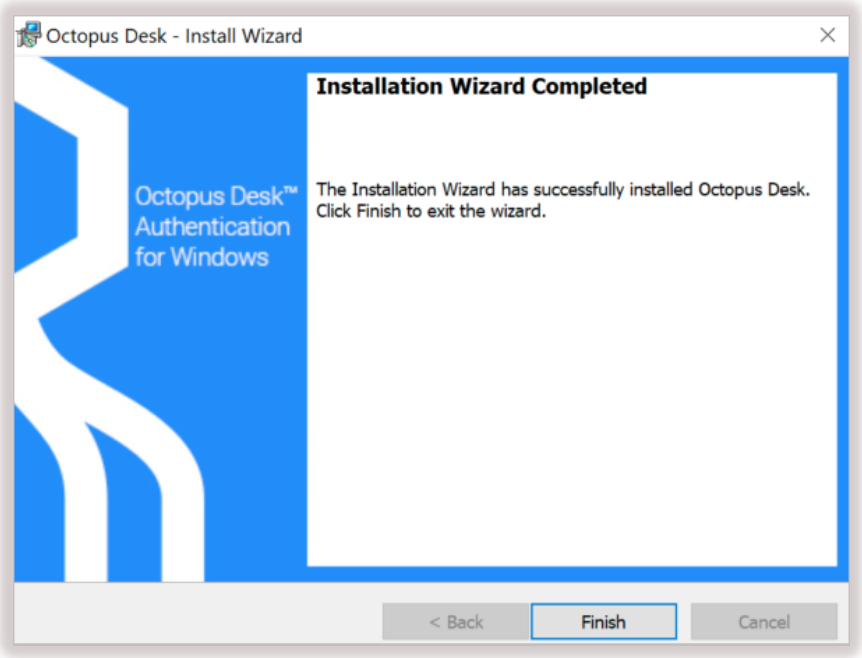


4. On the page that opens, accept the license agreement, and then click **Next**.
5. To start installation, click **Install**.



A confirmation is displayed when installation is complete.

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



When you quit the wizard, the MSIUpdater Client will auto launch, allowing you to configure the Octopus Desk for Windows.msi with the corporate Octopus Active Directory Authentication Sign-on details. For more information, refer to Configuring the MSIUpdater Client (below).

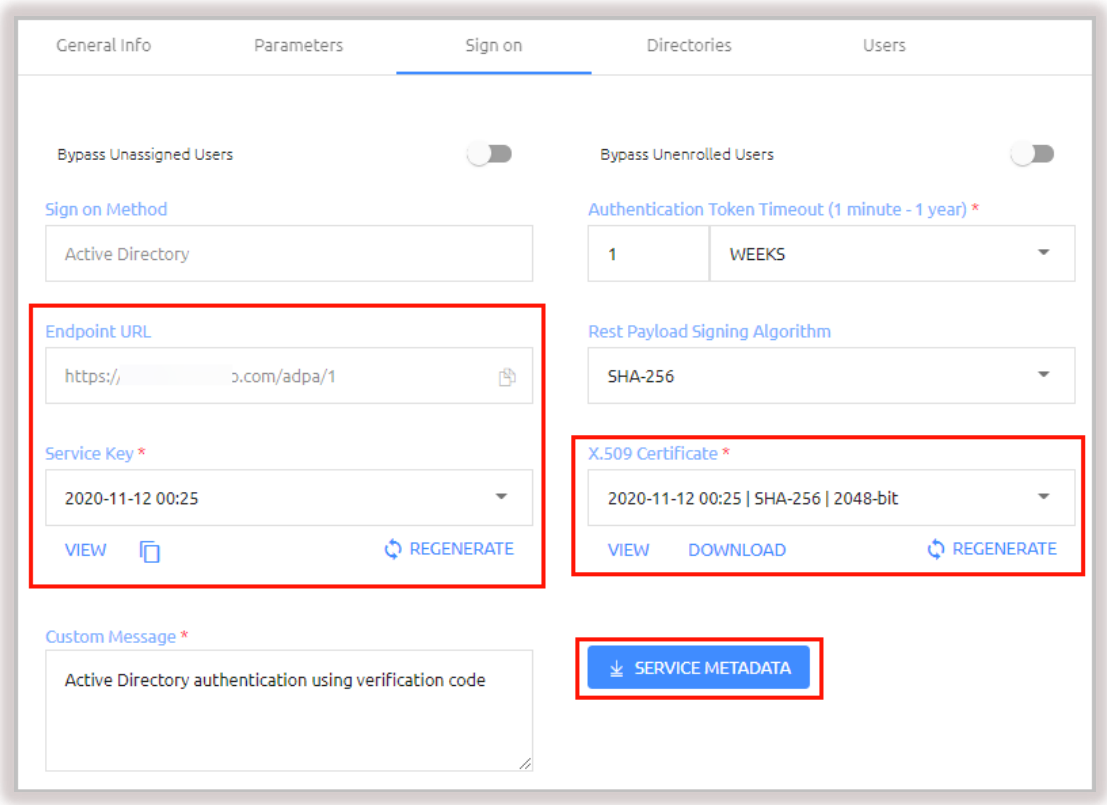
Configuring the MSIUpdater Client

The MSIUpdater, which launches automatically after you quit the MSIUpdater installer, updates the Octopus Desk for Windows (64-bit or 32-bit) MSI file with the corporate Octopus Active Directory Authentication Sign-On details and allows you to configure various settings related to authentication and the Windows login experience.

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 Octopus Management Console.

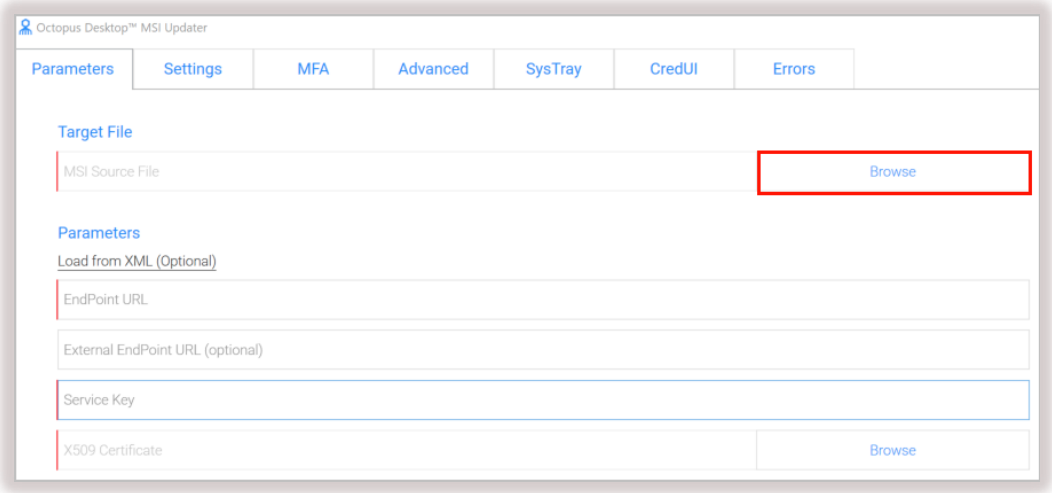
- **Endpoint URL:** Click the Copy icon to copy the URL.
- **Service Key:** Click the Copy icon to copy the URL.
- **X.509 Certificate:** Click **Download** to download the **cert.pem** file.

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



To configure the MSIUpdater client:

1. At the top of the **Parameters** tab, click **Browse** and upload the Octopus Desk for Windows MSI (64-bit or 32-bit) file to be updated.



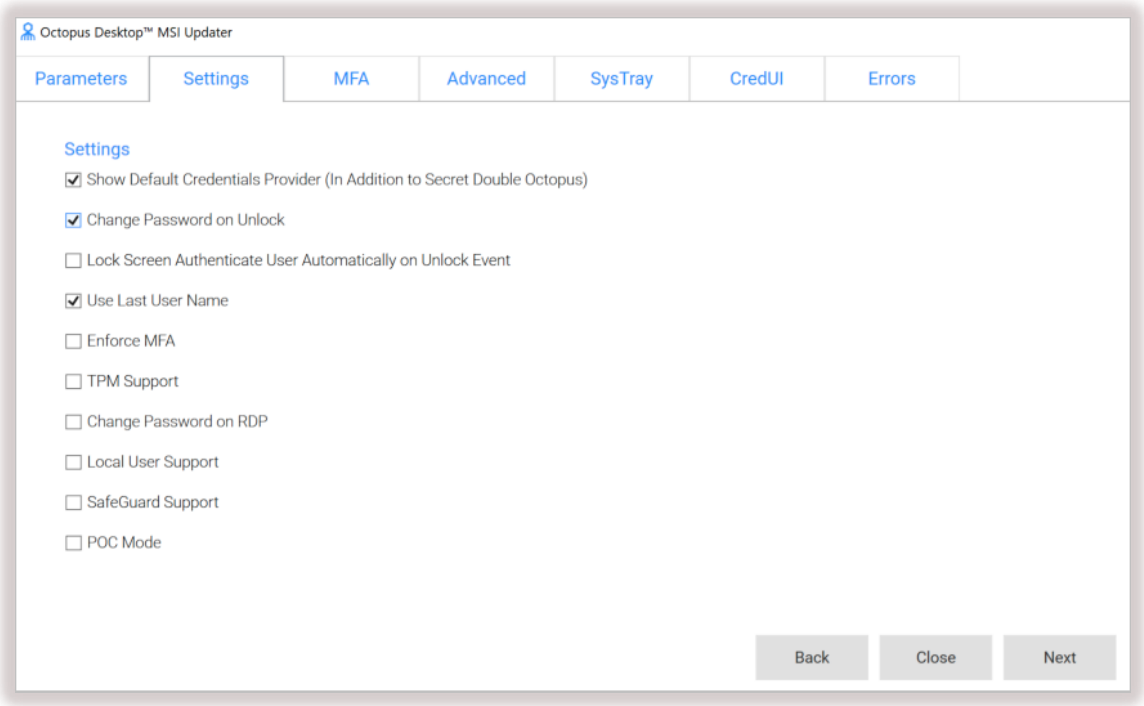
2. Add the service parameters using one of the following methods:
   - **Configure parameters manually:** Paste the **Endpoint URL** and **Service Key** values into the appropriate fields. Optionally (if required), enter an external endpoint URL in the **External Endpoint URL** field. This setting allows the Windows agent to access different URLs according to connection type (within the organization or outside of it). Finally, click **Browse** and upload the X.509 certificate file.
   - **Upload the parameters:** Click **Load from XML** to upload the **metadata.xml** file from the Active Directory Authentication service.

3. Select one or more of the following authenticators:

Authenticator	Description
Octopus App	Octopus Authenticator mobile app (iOS/Android)
FIDO2	FIDO authenticator from Yubico or Feitian
3rd Party Authenticator	Select this checkbox to enable login to Windows using third party authentication. (It is not necessary to select specific authenticators.)
OKTA Verify / ForgeRock	These checkboxes are for lower server versions and are not relevant to Octopus Desk for Windows version 3.4.
OTP	Select this checkbox to enable authentication with ForgeRock OTP or Octopus-generated OTP.

4. Click **Next**.

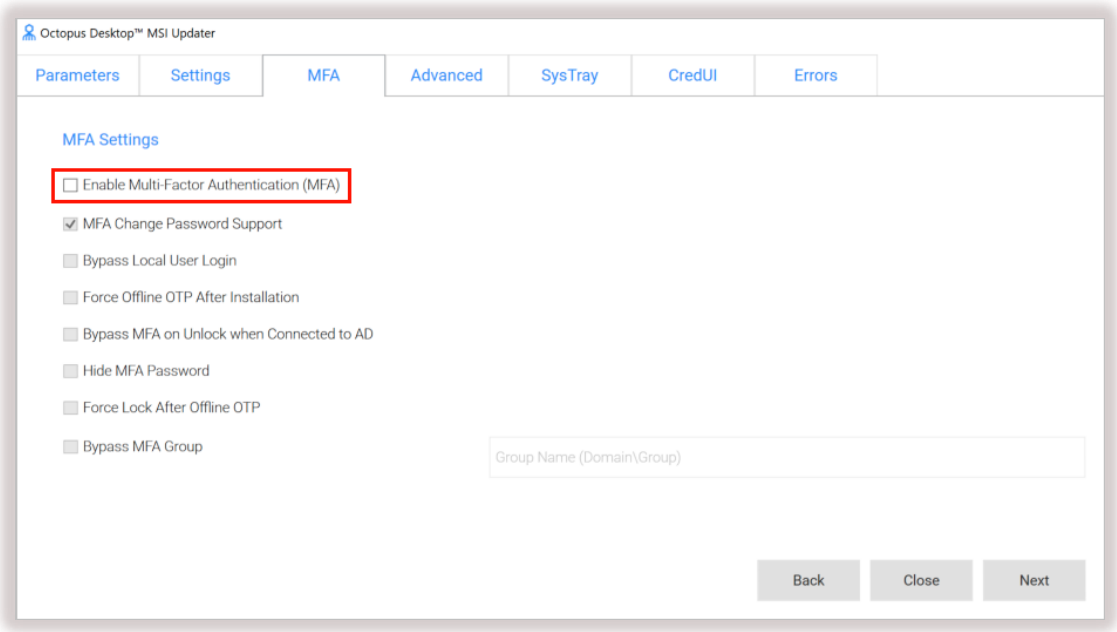
5. In the **Settings** tab, enable the options as required by selecting the relevant checkboxes.



Setting	Description / Notes
Show Default Credential Provider	Determines whether Windows default credential providers (Windows and Active Directory) are displayed when logging into Windows.
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.
Lock Screen Authenticate User Automatically on Unlock Event	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 Octopus, ForgeRock or OKTA Authenticators immediately after pressing **<Ctrl> <Alt> <Del>**.
Use Last User Name	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 relevant for users with Octopus, ForgeRock or OKTA authenticators only (not FIDO).
TPM Support	If TPM 2.0 is enabled, selecting this option allows TPM to store the private key for BLE password encryption.
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, Octopus Desk for Windows will be enabled for Local users and will verify that the Local user matches the mapping with Octopus Authentication Server user. **Note: This setting is relevant for non-domain users only**.
SafeGuard Support	Selecting this option enables Octopus Desk for Windows to login to the SafeGuard client (session).
POC Mode	When selected, Octopus Desk 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 Octopus Authentication Server.

6. Click **Next**.
7. Open the **MFA** tab. If you want to use MFA with Active Directory authentication for logging into Windows, select the **Enable Multi-Factor Authentication (MFA)** checkbox. When MFA is activated, users will need to enter their AD passwords in order to receive a push notification from Octopus, ForgeRock or Okta Authenticators.
   When the checkbox is not selected, Windows login will be Passwordless.
   Note: In order to successfully use a FIDO key with MFA, a PIN must NOT be set on the key. For passwordless FIDO authentication, a PIN needs to be set on the key.



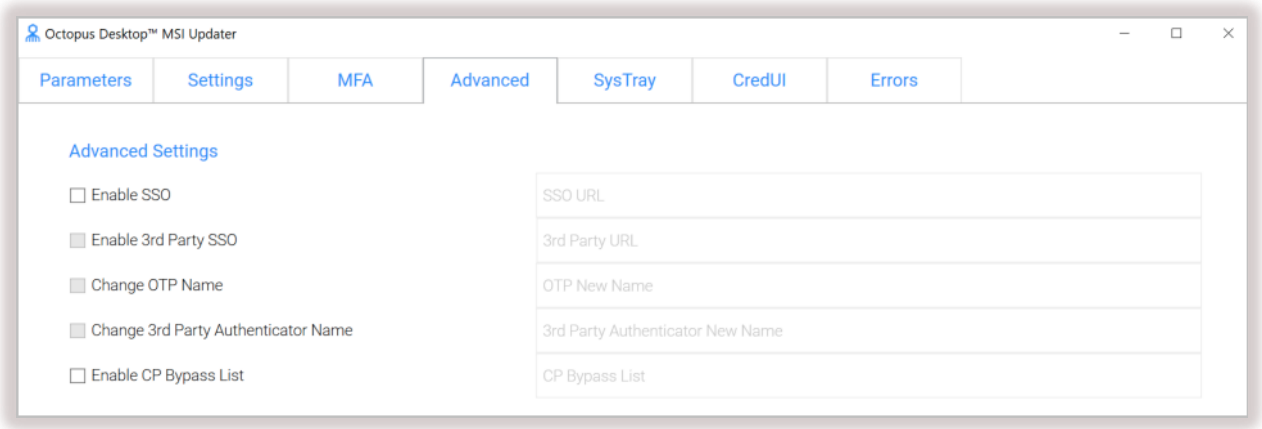
8. When MFA is activated, you may enable the following options as required by selecting the relevant checkboxes:

Setting	Description / Notes
MFA Change Password Support	When selected, users are able to change the password on the Windows workstation without the Octopus credential provider (CP) intercepting the process. When the checkbox is cleared, the Octopus CP controls the password change process.
Bypass Local User Login	When selected, administrators with a Local user account bypass Octopus Authentication and login with username and password.
Force Offline OTP After Installation	When selected, users are prompted to download an offline OTP buffer (by scanning a QR code) when they perform online login, and they are not permitted to login offline without the OTP. When this checkbox is **NOT** selected, users will be able to login offline using Username + Password.
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).
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).
Bypass MFA Group	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.

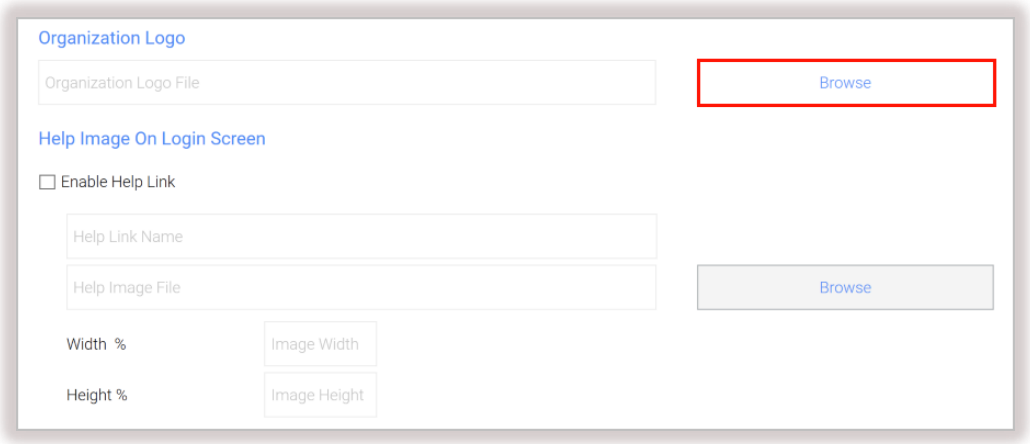
9. Click **Next**.

10. In the **Advanced** tab, configure the following settings, as required:

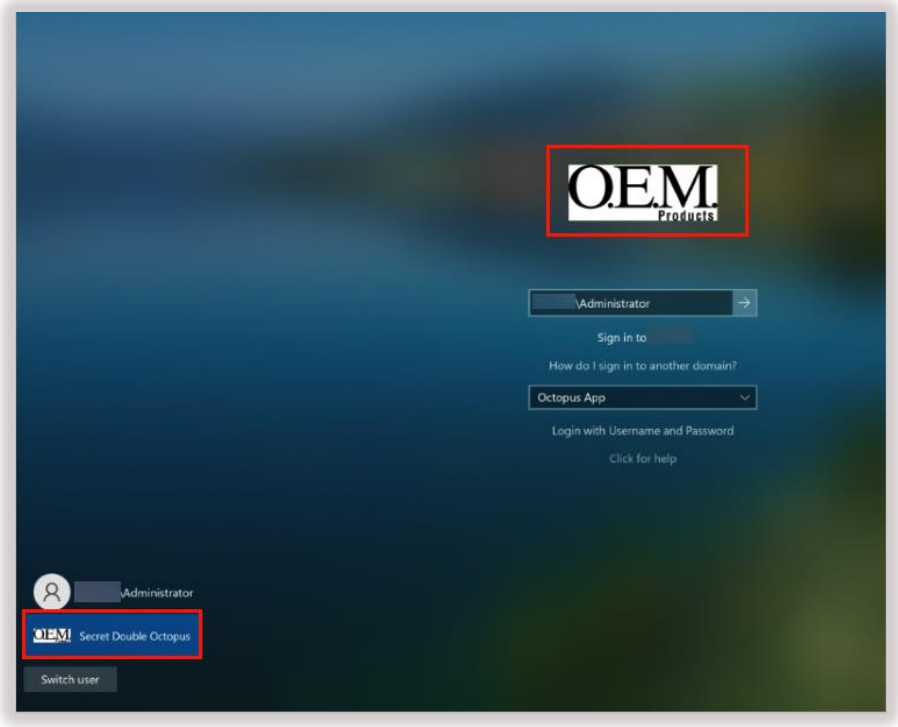
Setting	Description / Notes
Enable SSO Enable 3rd Party SSO	**You may configure ONE of these settings only**. After selecting the checkbox, enter the portal URL / 3rd party portal URL. In runtime, the portal will open in the default browser. Users will be automatically logged in and be able to view all assigned services. The **Enable 3rd Party SSO** setting is available only when the **OKTA Verify** or **ForgeRock** checkbox on the **Parameters** tab is selected.
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 (e.g., *ForgeRock OTP*). This setting is available only when the **OTP** checkbox on the **Parameters** tab is selected.
Change 3rd Party 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 **3rd Party Authenticator** checkbox on the **Parameters** tab is selected.
Enable CP Bypass List	Allows you to specify credential providers (in addition to Octopus Authenticator) 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.



11. To display your company's logo on the Windows Login screen, under **Organization Logo**, click **Browse**. Then, navigate to and select the relevant image file.
IMPORTANT: The image must be 448x448, in 24-bit BMP format.

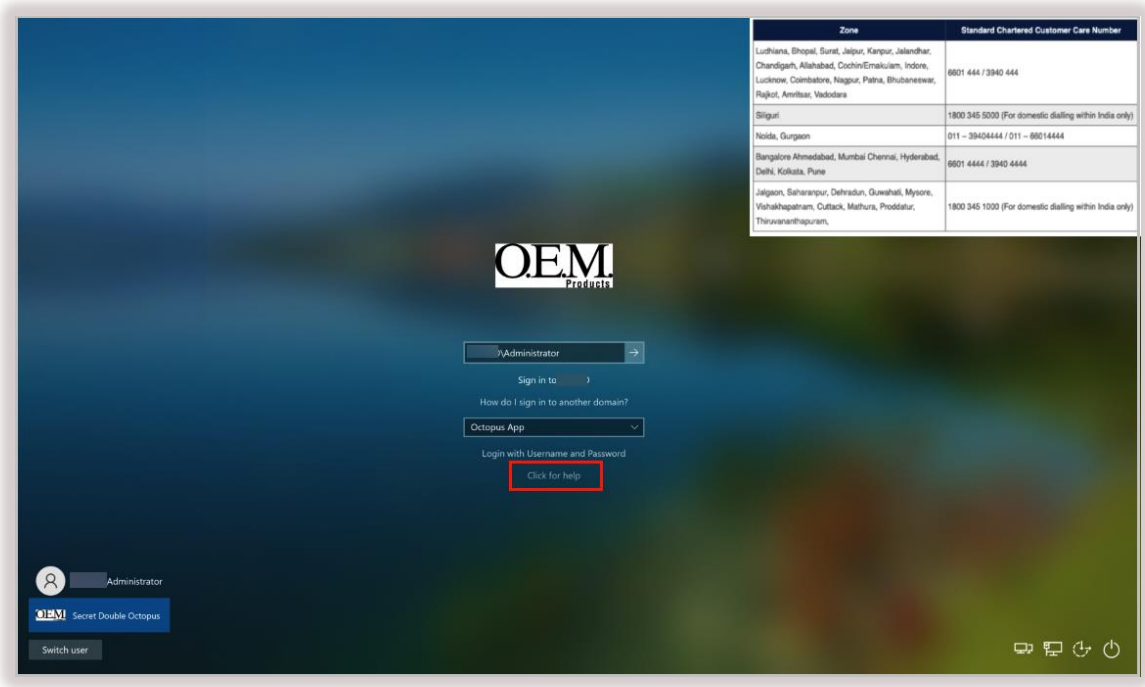


In runtime, your logo will appear on the Login screen instead of the default Secret Double Octopus logo. For example:



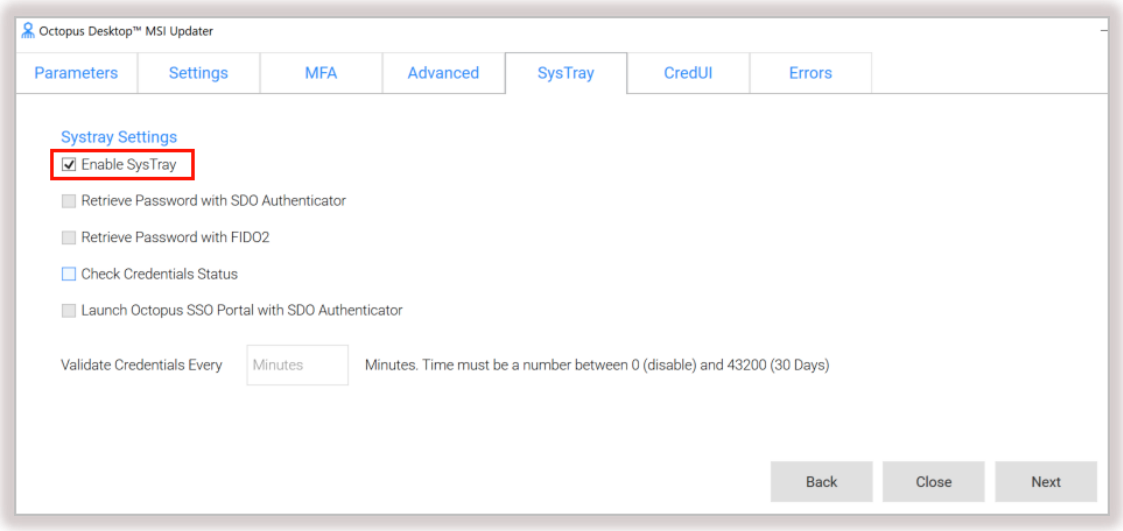
12. To display support resources on the Windows Login screen, select the **Enable Help Link** checkbox. Then click **Browse** and select the file containing the support information. **IMPORTANT: The uploaded image may be any size but must be in 24-bit BMP format.** You can adjust the size of the displayed image by specifying values in the **Width** and **Height** fields.

In runtime, users will be able to click the link to open the Help image. For example:



13. At the bottom of the **Advanced** tab, click **Next**.

14. Open the **SysTray** tab. To activate the system tray actions menu that allows users to perform self-service flows, select the **Enable SysTray** checkbox.



15. If the SysTray is enabled, select the following options as required by selecting the relevant checkboxes:

Action	Description / Notes
Retrieve Password with SDO Authenticator	When selected, users are able to view and copy the AD password after performing passwordless authentication on the Octopus Authenticator mobile app.
Retrieve Password with FIDO2	When selected, users are able to view and copy the AD password after performing passwordless authentication using a FIDO key.
Check Credentials Status	When selected, users are able to view the time remaining until password expiration.
Launch Octopus SSO Portal with SDO Authenticator	When selected, users are able to open the User Portal from the desktop after performing passwordless authentication on the Octopus Authenticator mobile app.

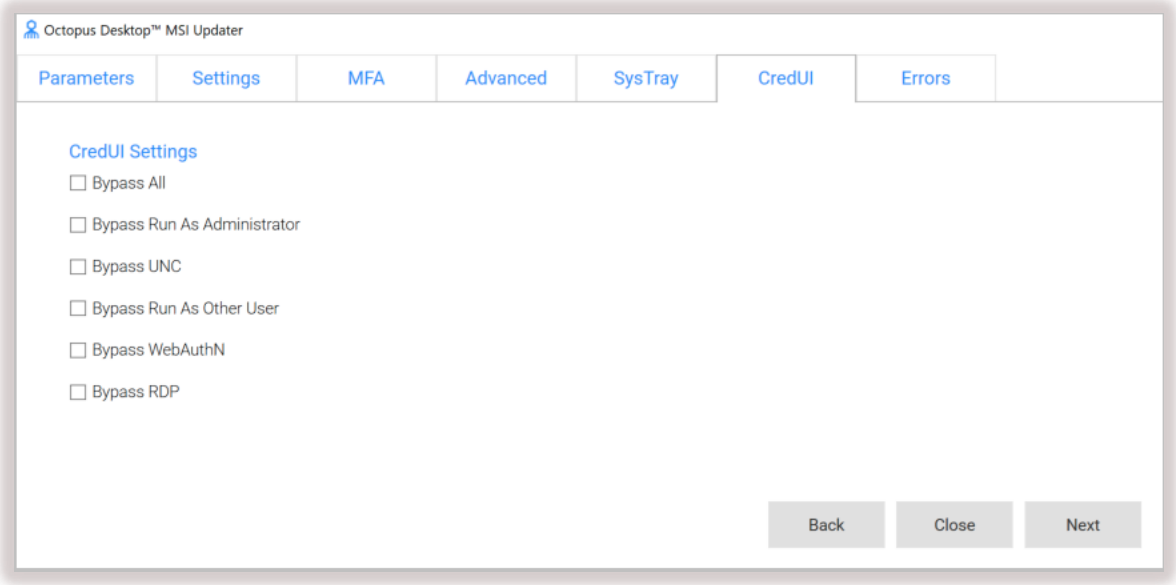
Note: After deployment of Octopus Desk for Windows, users need to logout and login again in order to operate the systray. When users initiate a systray action, the systray is automatically locked for 30 seconds. (Multiple actions are not supported.)

16. At the bottom of the **SysTray** tab, enter 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).

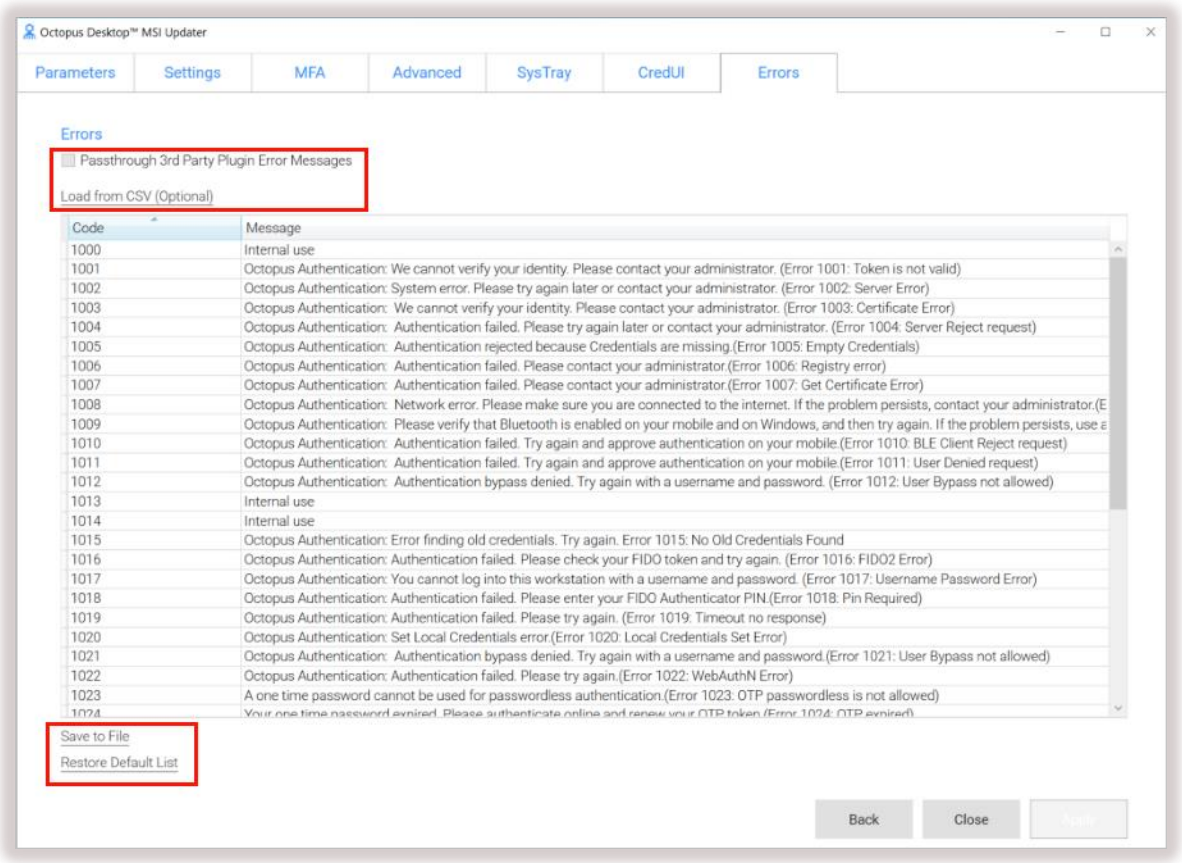
    Note: Once the password expires, users will need to login within the organization network or via the VPN in order to reauthenticate.

17. Click **Next**.

18. In the **CredUI** tab, select the scenarios in which an additional MFA credential (e.g., push, OTP, etc.) will not be required. (When a Bypass is selected, the default Windows Login screen is presented and users authenticate by entering Username + Password.)
    Selecting **Bypass All** activates MFA bypass for all the scenarios.



19. Click **Next**.
20. In the **Errors** tab, 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.



21. At the bottom of the **Errors** tab, click **Apply**.
    A new modified MSI file is created in the same location as the original MSI file. The name of the new file will include Octopus Desk for Windows 32-bit or 64-bit and the timestamp of file creation.

Note: The original MSI file will not be updated and can be reused. **Do not use the original MSI file for installation**.

MSI Deployment of Octopus Authenticator

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

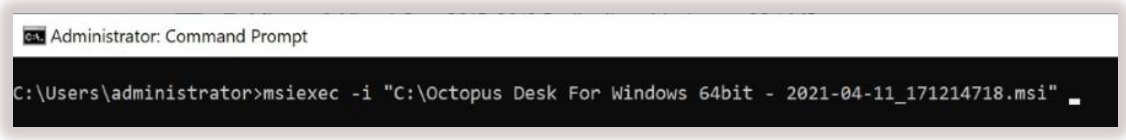
Performing Silent Installation

Silent installation allows administrators to push the installation to all client machines from a central tool (e.g., GPO). All required components are installed as part of the deployment.

Note: Administrator permissions are required to run the Octopus Desk for Windows MSI.

To perform silent installation:

1. **Open the command prompt as Admin**, and run *Octopus Desk For Windows (64bit or 32bit).msi*
2. Run *Octopus Authentication for windowsxx.msi /qn*:
   - Windows 64bit:
     C:\> Octopus Desk For Windows 64bit – xx_xxx_xx.msi /qn
   - Windows 32bit:
     C:\> Octopus Desk For Windows 32bit – xx_xxx_xx.msi /qn



3. If you want the Octopus Authentication credential provider to be disabled on some machines after installation (allowing for gradual deployment), refer to Appendix D: Enabling / Disabling the Octopus Authentication CP Post-installation.

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 Octopus Desk for Windows MSI.

To push installation through distribution tools:

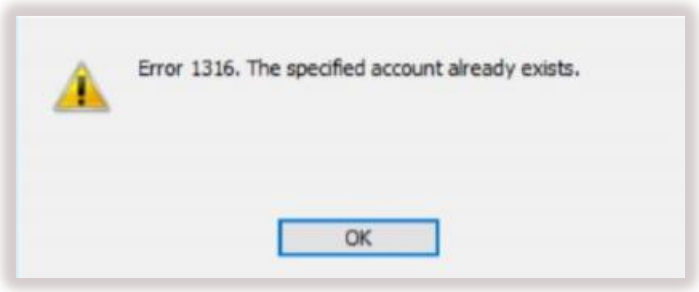
1. Open and run your distribution software.
2. Install Visual C++ 2015-2019 Redistributable (x64)/(x86) - 14.28.29325
3. **Open the command prompt as Admin**, and run *Octopus Desk For Windows (64bit or 32bit).msi*
4. Run *Octopus Authentication for windowsxx.msi /qn*:
   - Windows 64bit:
     C:\> Octopus Desk For Windows 64bit – xx_xxx_xx.msi /qn
   - Windows 32bit:
     C:\> Octopus Desk For Windows 32bit – 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, the following error message will appear:

Error 1316: The specified account already exists – 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.

To upgrade the MSI, run the following command:

- Windows 64bit:
  C:\> msiexec /I " Octopus Desk For Windows 64bit.msi" REINSTALL=ALL REINSTALLMODE=vomus IS_MINOR_UPGRADE=1 /qn
- Windows 32bit:
  C:\> msiexec /I " Octopus Desk For Windows 32bit.msi" REINSTALL=ALL REINSTALLMODE=vomus IS_MINOR_UPGRADE=1 /qn

Windows Authentication Methods

Once installation is completed, users will be able to authenticate to Windows machines using Octopus Authenticator, OKTA Verify, ForgeRock Authenticator, 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>**.

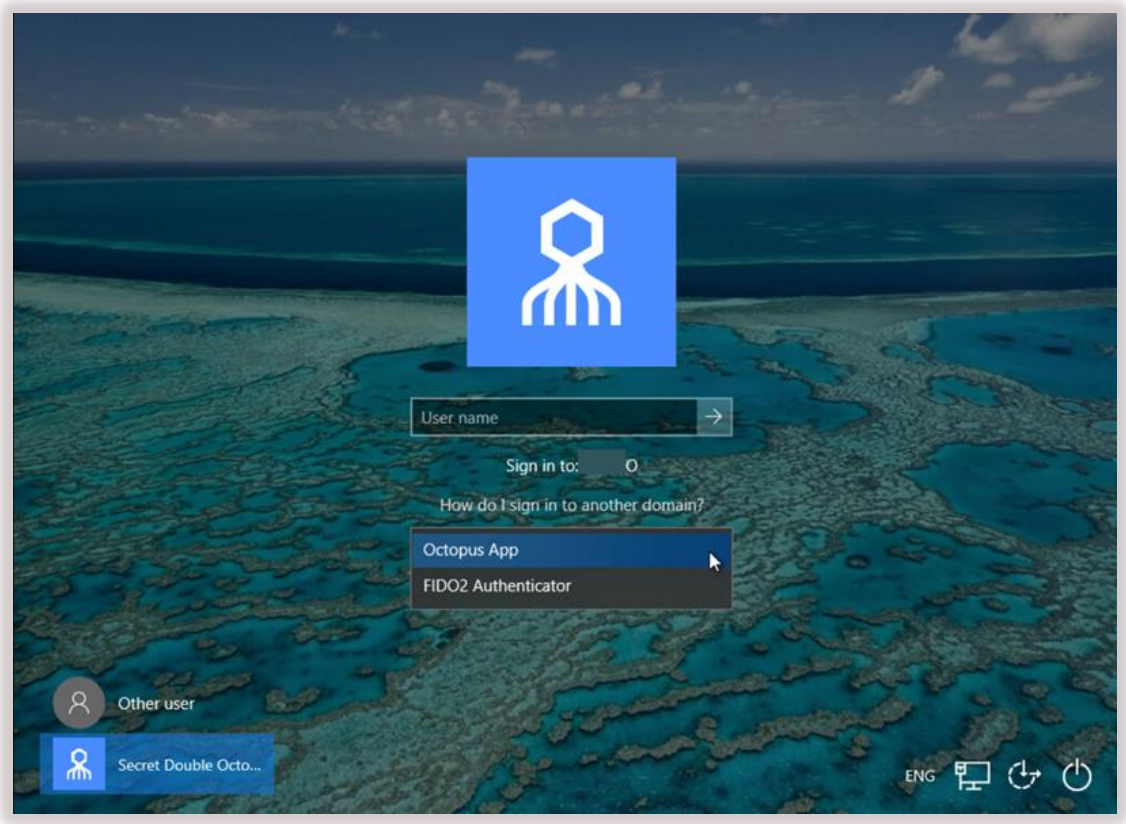
Users can choose from a wide variety of login methods, both online and offline (in the event that a enterprise network is not available). **Online** login methods are listed and described in the following table.

Authentication Method	User Experience (On mobile)	User Experience (Not on mobile)
Octopus App	• **Passwordless:** Username + Octopus • **MFA:** Username + Password + Octopus	N/A
OKTA Verify	• **Passwordless:** Username + OKTA (Push) • **MFA:** Username + Password + OKTA (Push)	N/A
ForgeRock App	• **Passwordless:** Username + ForgeRock (Push) • **MFA:** Username + Password + 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
Octopus online OTP	**MFA**: Username + Password + OTP	N/A
ForgeRock online OTP	**MFA**: Username + Password + OTP	N/A
Octopus app via Bluetooth	• **Passwordless:** Username + Octopus BLE • **MFA:** Username + Password + Octopus BLE	N/A

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
FIDO	N/A	• **Passwordless:** Username + PIN + FIDO Authenticator (Touch) • **MFA:** Username + Password + FIDO Authenticator (Touch)
Octopus offline OTP	**MFA**: Username + Password + OTP	N/A
ForgeRock offline OTP	**MFA**: Username + Password + OTP	N/A
Octopus app via Bluetooth	• **Passwordless:** Username + Octopus BLE • **MFA:** Username + Password + Octopus BLE	N/A

Note: Bluetooth can be used in Windows 10 systems only.

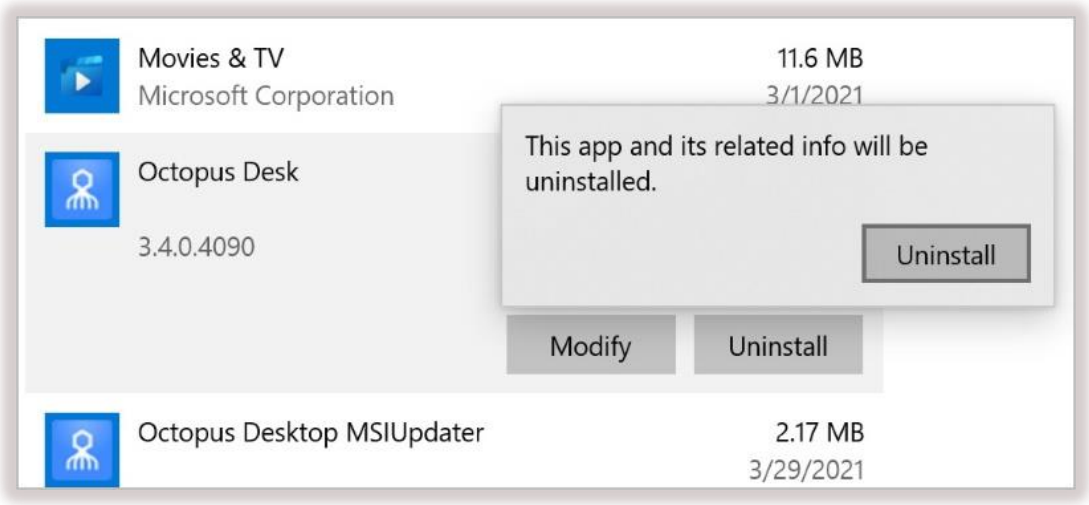


Uninstalling Octopus Desk for Windows

You may uninstall Octopus Desk for Windows via the system Settings or via the command line.

Uninstalling via System Settings

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



Uninstalling via the Command Line

Run the following command to uninstall Octopus Desk for Windows:

```
C:\> msiecex /x {a95d85be-778f-4ed1-9ded-9f62ecc8a744}
```

Appendix A: Remote Desktop Windows Login

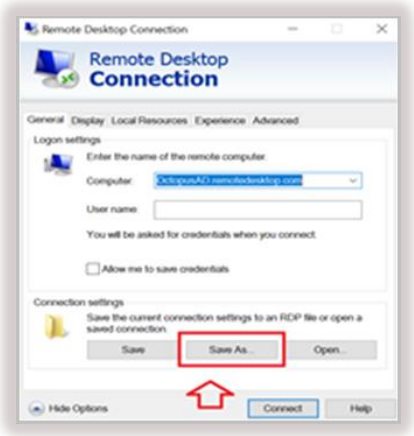
To enable remote desktop login, the following additional configurations are required.

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:
   enablecredsspsupport:i:0

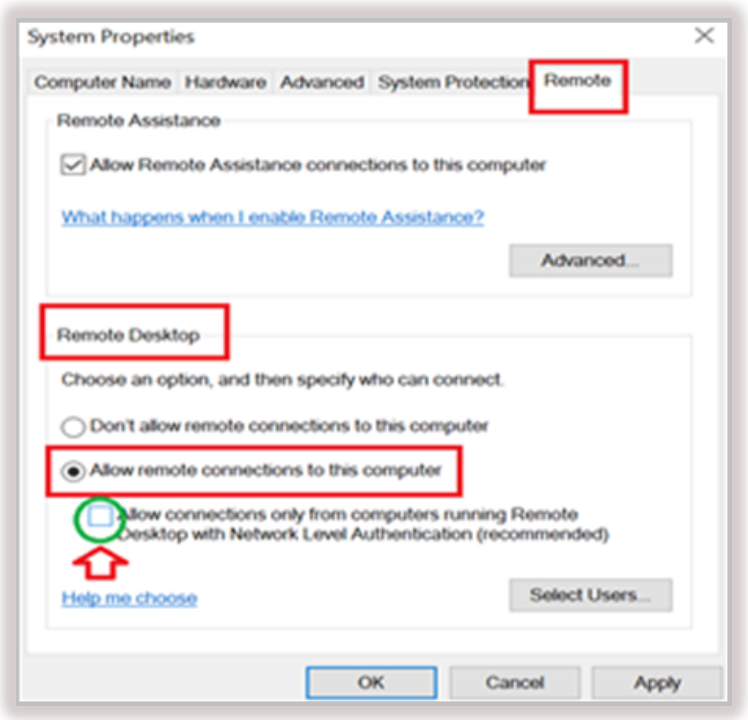
5. Save the script.

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 with Network Level Authentication** checkbox is NOT selected.



4. Click **Apply**.

Appendix B: Importing the Self-signed Certificate

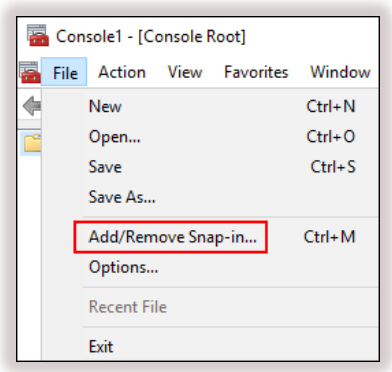
The self-signed certificated can be found on the Octopus Authentication Server in the following location**: /etc/pki/nginx/selfsigned.crt**
This certificate should be copied to the Windows environment to allow the self-signed certificate to work with Octopus Desk for Windows.

The self-signed certificate should be imported to the root certificate folder on the Windows machine that is using Octopus Desk.

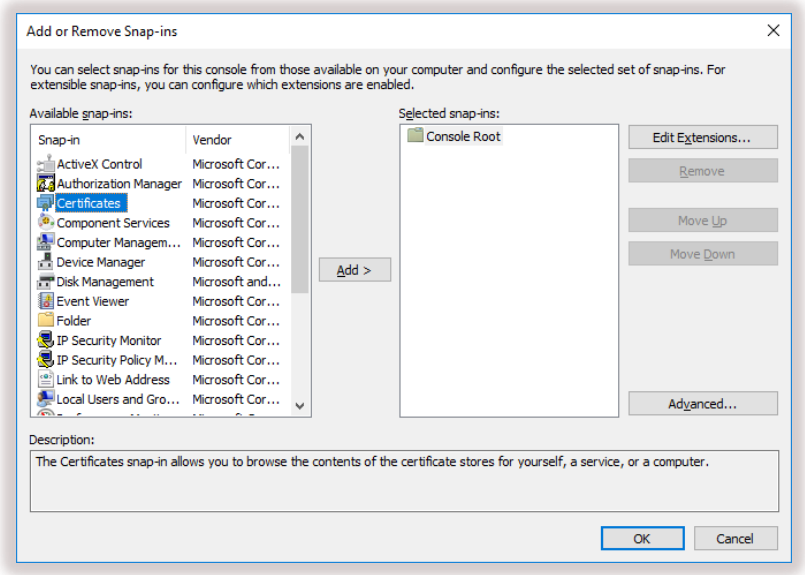
Note: This action should be done for POC purposes and not for the production environment.

To import the self-signed certificate:

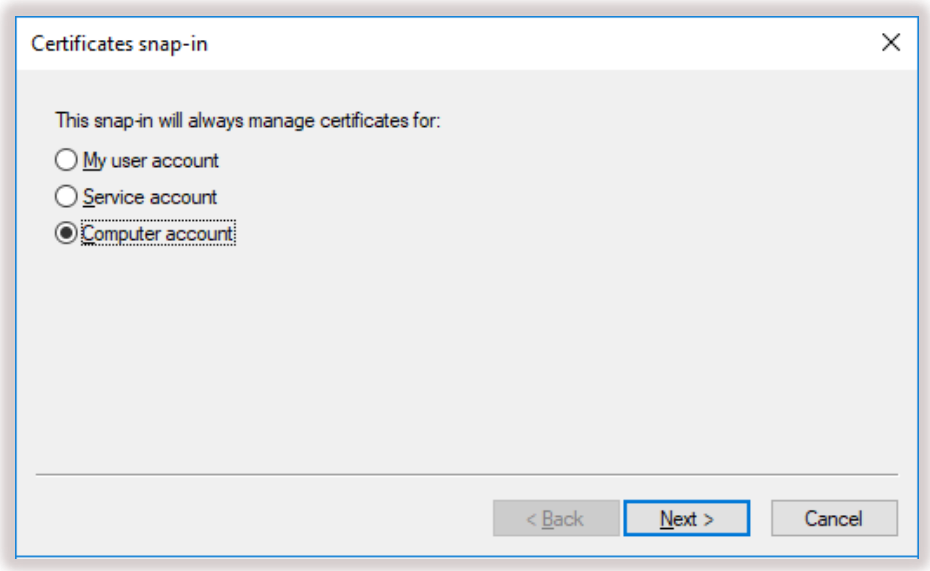
1. Open the Microsoft Management Console (mmc.exe).
2. From the **File** menu, select **Add/Remove Snap-in**.



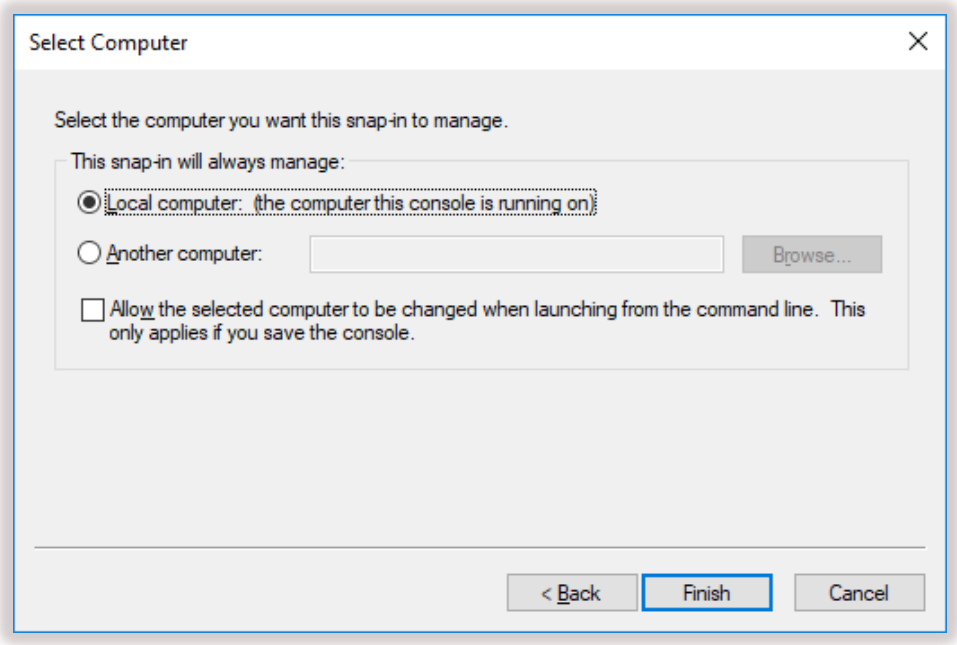
Then, double-click **Certificates**.



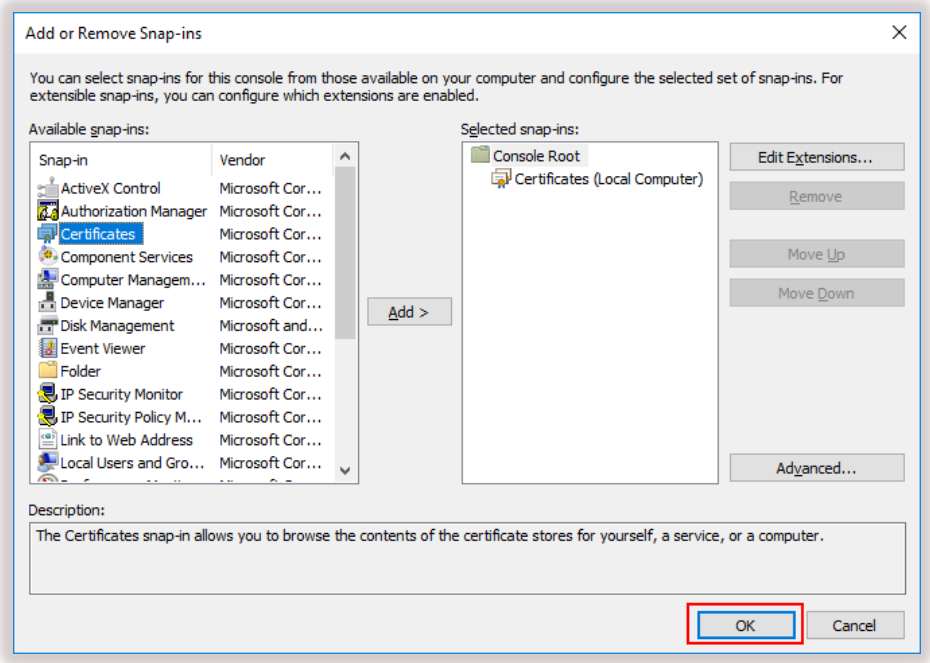
3. From the Certificates snap-in wizard, select the **Computer account** radio button. Then, click **Next**.



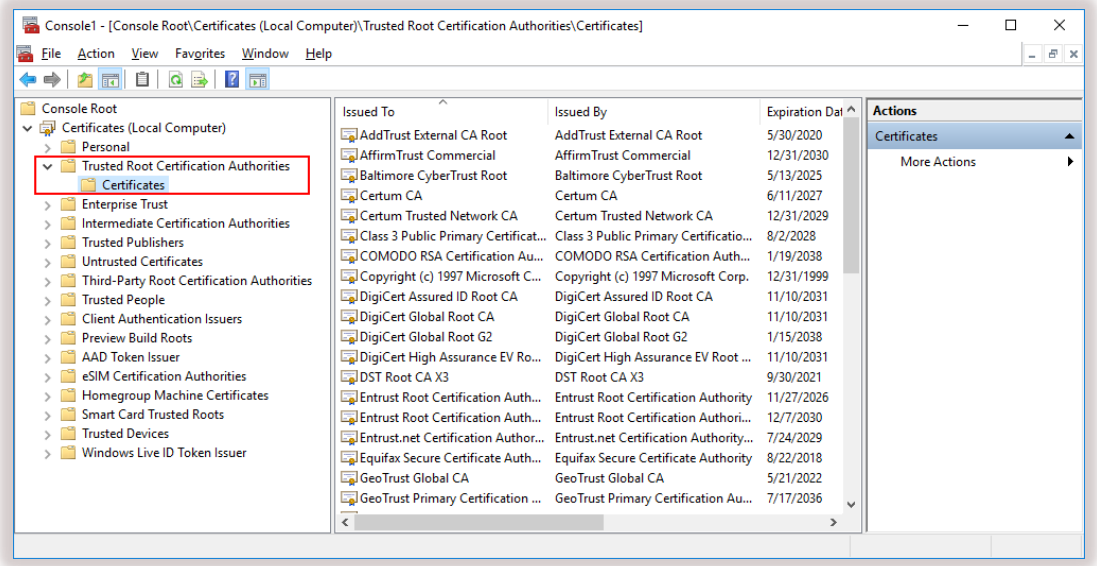
4. Select the **Local computer** radio button. Then, click **Finish**.



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



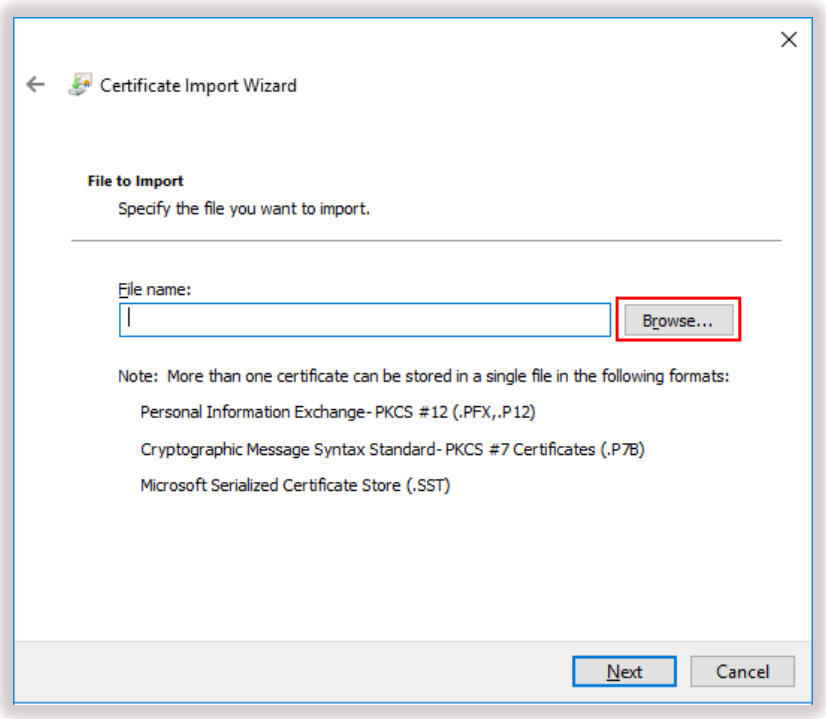
6. From the Certificates tree, select **Trusted Root Certification Authorities > Certificates**.



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

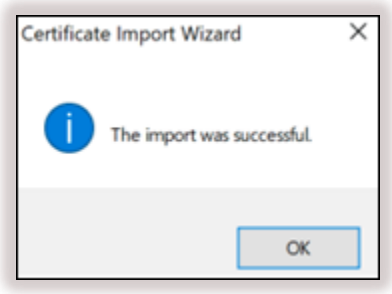
   The Certificate Import Wizard opens.
8. On the first page of the wizard, click **Next**.

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.



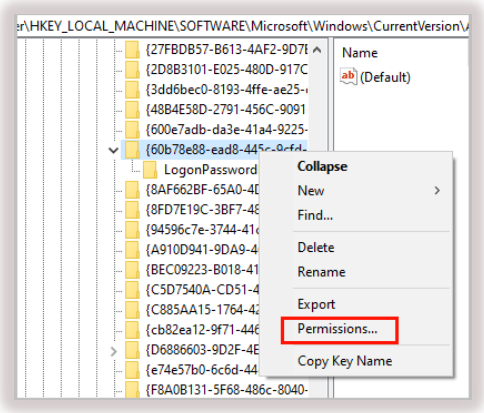
12. In the **Certificates** node, verify that the new certificate appears in the list of certificates.

Appendix C: Windows 8.1 Registry Update

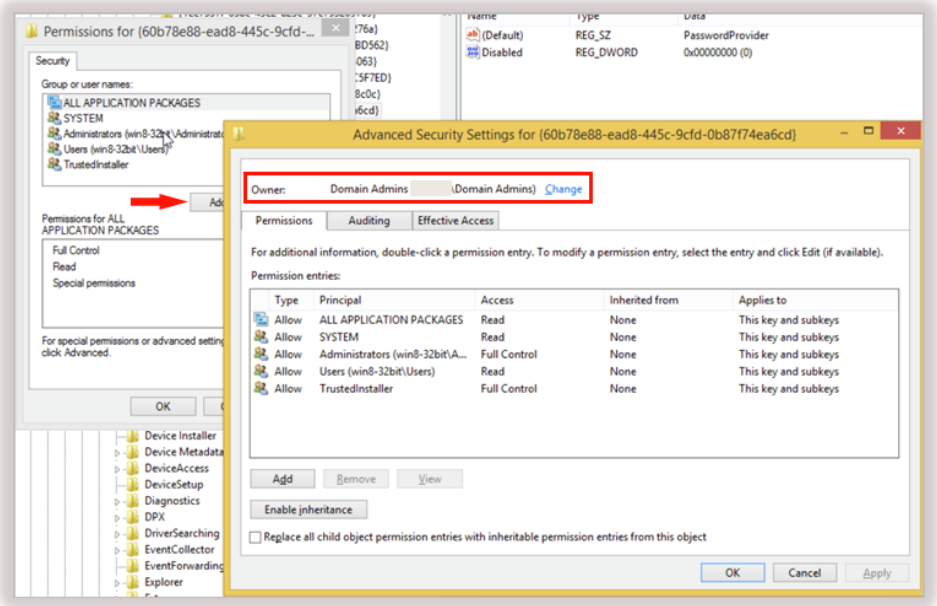
Follow the steps below to change the ownership of the relevant Credential Providers registry key from *TrustInstaller* to *Domain Admins*.

To update the registry key ownership:

1. Connect to the machine registry and navigate to:
   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{60b78e88-ead8-445c-9cfd-0b87f74ea6cd}]
2. Right-click on the registry key and select **Permissions**.



   Then click **Advanced** to open the **Advanced Security Settings** dialog.
3. The *Owner* value should appear at the top of the dialog. Click **Change** and set the ownership to *Domain Admins*.



Appendix D: Enabling / Disabling the Octopus Authentication CP Post-installation

Octopus Desk for Windows supports the ability to control availability of the Octopus Authentication 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 Octopus Authentication CP is manually disabled post-installation will not support Octopus Authentication as a means of logging into Windows. The installation of Octopus Desk will be transparent to users, who will not see the Octopus CP on the Login screen and will continue to login as they did prior to installation.

To disable the Octopus Authentication CP post-installation, use the following syntax:

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

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

To enable the Octopus Authentication CP, use the following syntax:

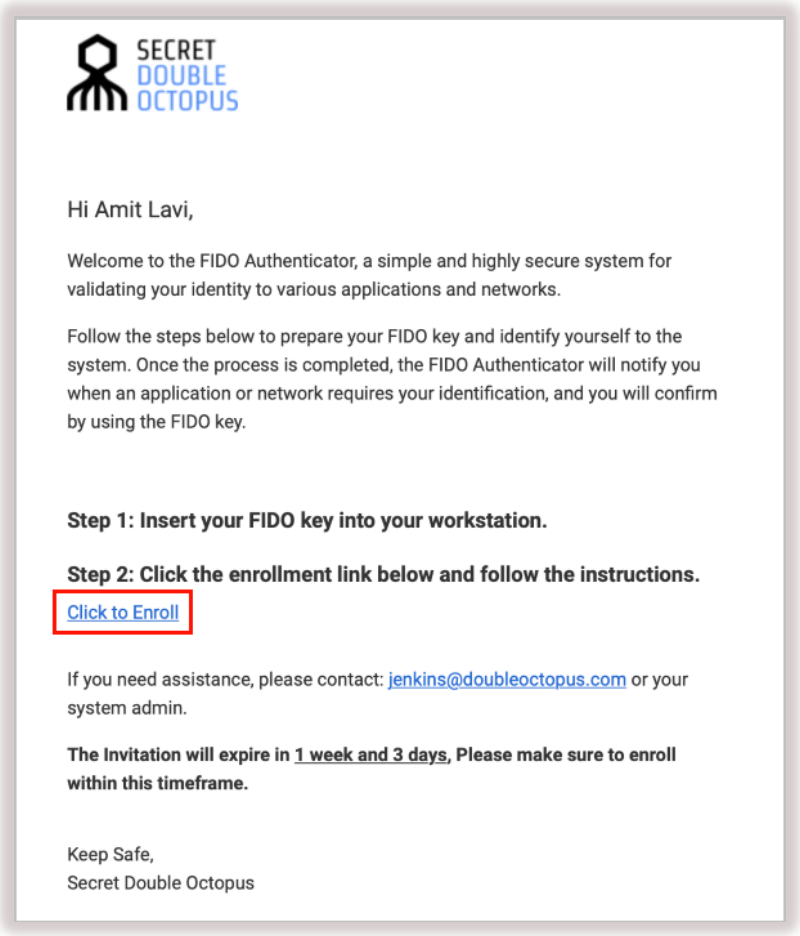
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication
\Credential Provider Filters\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SDOCredentialProvider"
"Disabled"=dword:00000000

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

Appendix E: FIDO + Fingerprint Enrollment and Authentication

This appendix presents the flow for registration using the FIDO key + fingerprint authentication mechanism. Following successful enrollment, users can log into Windows by simply touching the key (entering a PIN is not required).

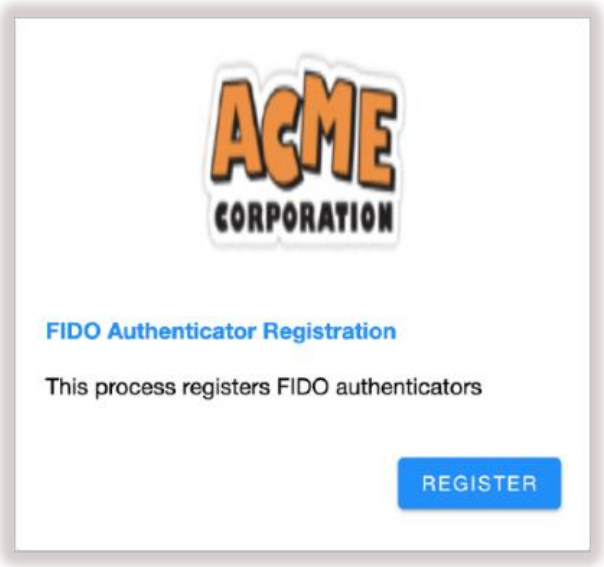
To enroll in the system using FIDO + fingerprint:

1. Insert your FIDO key into the workstation.
2. Click the enrollment link presented in the invitation email.



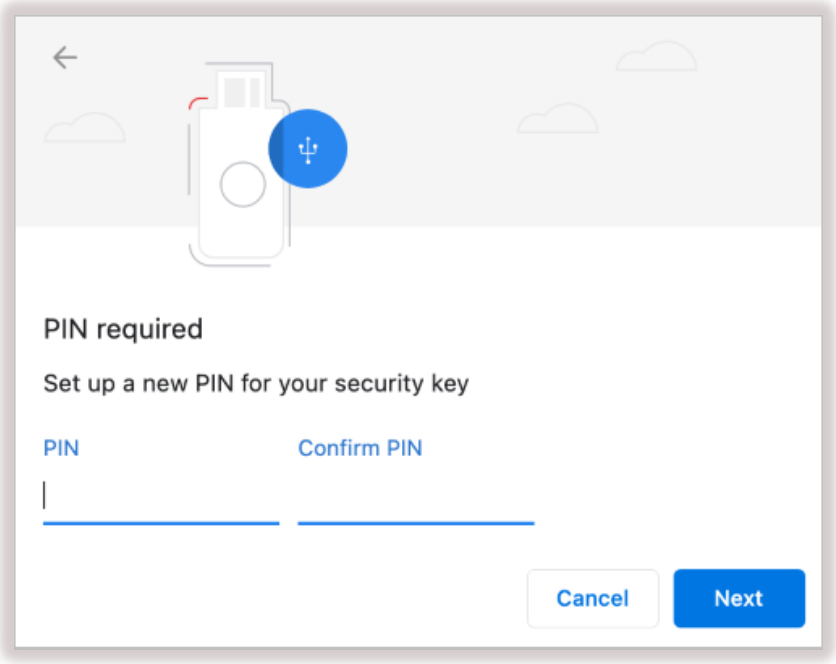
You will be redirected to the FIDO Authenticator Registration page.

3. Click **Register**.

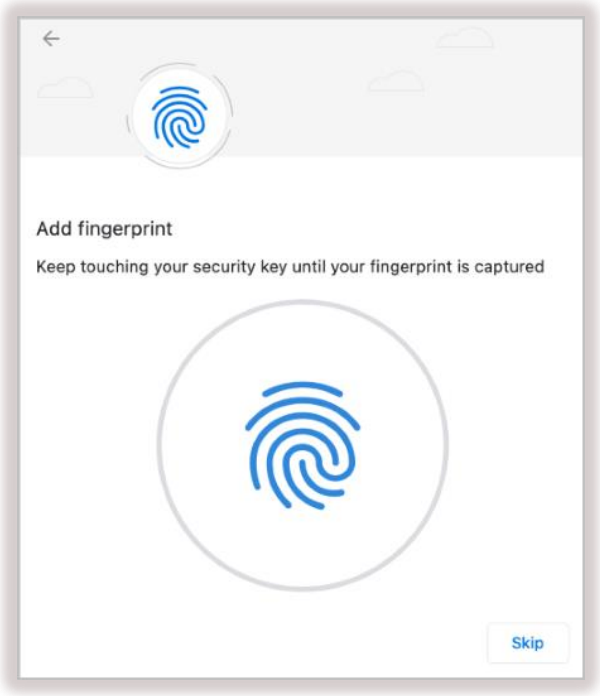


You will be prompted to set up a PIN for your FIDO key. This PIN is used as a backup for your fingerprint.

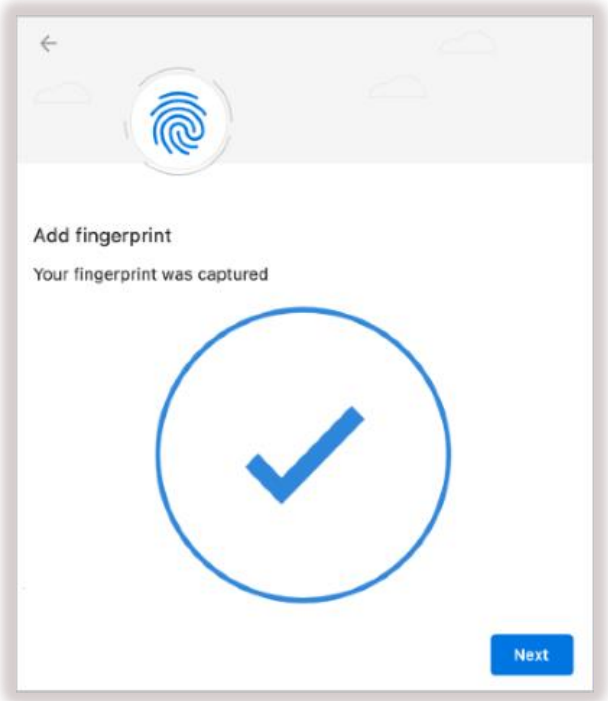
4. Enter your PIN in the **PIN** field and re-enter it in the field to the right. Then, click **Next**.



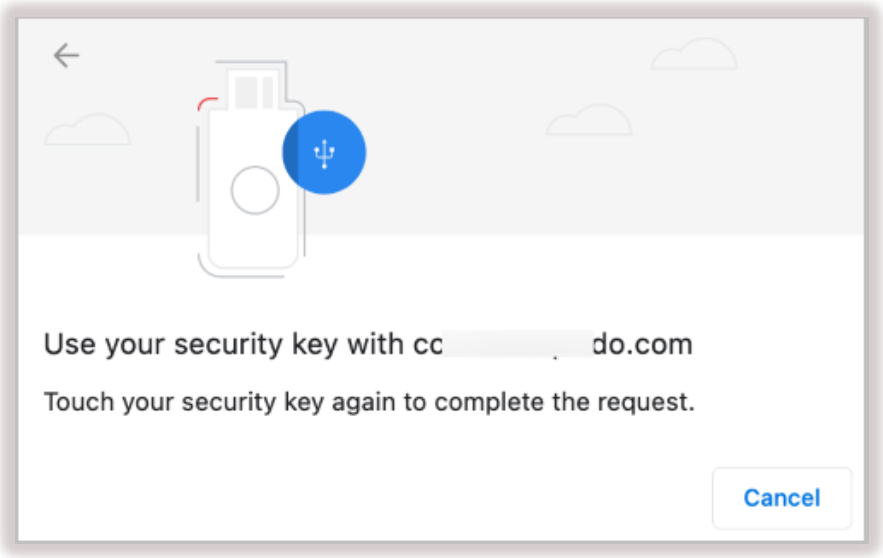
5. Add your fingerprint by touching your security key. You may need to touch it several times before your fingerprint is captured.



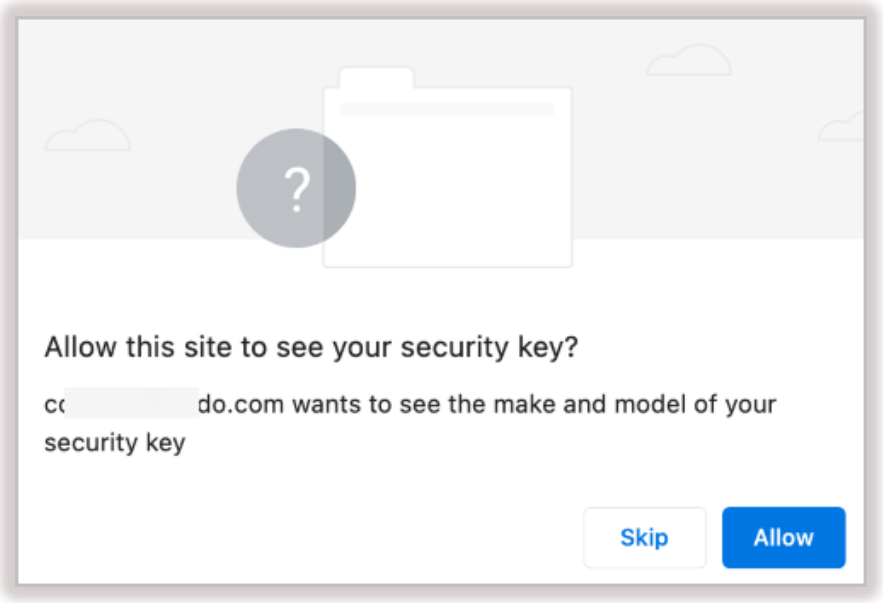
After your fingerprint is captured, click **Next**.



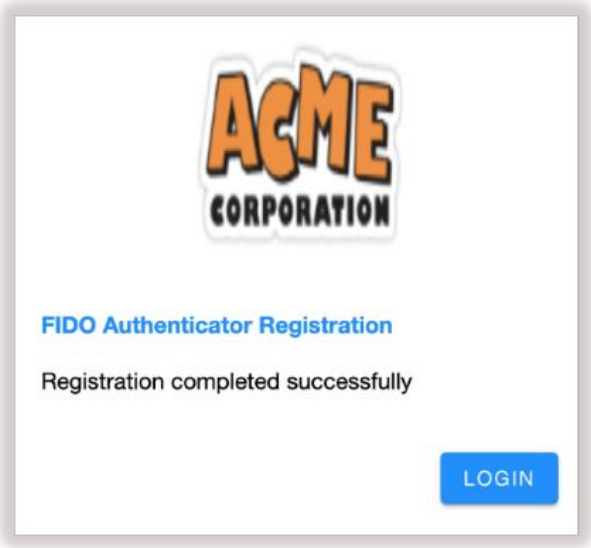
6. To confirm your enrollment, touch your security key again.



7. To approve the authentication, click **Allow**.



A confirmation message is displayed on successful enrollment.



Authenticating to Windows with FIDO Authentication

When logging into Windows, users select the **FIDO2 Authenticator** login option and then touch their FIDO keys. There is no need to enter a PIN during the authentication process.