Enterprise Connect Passwordless for Windows Installation Guide v3.8.2

For Octopus Authentication Server v5.4.4 and above

Table of Contents

Preface	3
Product overview	3
Prerequisites	3
Creating the Active Directory authentication service	4
Windows client installation with MSIUpdater	8
Installing the MSIUpdater Client	8
Configuring the MSIUpdater Client	11
MSI deployment	31
Performing silent installation	31
Performing deployment using Installation Wizard	32
Performing installation through distribution tools	34
Enabling the password free experience	34
Management console configuration	35
Windows MSIUpdater configuration	36
Password free experience: user authentication	37
Enabling FIDO BIO user bypass	38
Bypassing users in the management console	38
Configuring the MSIUpdater	39
User authentication experience	41
Windows authentication methods	42
Uninstalling Enterprise Connect Passwordless for Windows	44
Appendix A: Remote desktop Windows login	44
Editing the remote desktop script	45
Configuring Windows PC system properties settings	45
Appendix B: Importing the Self-signed certificate	46
Appendix C: Enabling / Disabling the Octopus Authentication CP Post-installation	50
Appendix D: Troubleshooting	51
Launching the Check Point VPN from the Systray	51
Viewing Windows Agent Events	52
Appendix E: Known Issues	56

Preface

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

Product overview

Secret Double Octopus (SDO) 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.



Prerequisites

Before beginning installation, verify that:

- Octopus Authentication Server **v5.4.4 (or higher)** is installed and operating with a valid enterprise certificate.
- For Active Directory or Azure AD:
 - Your Corporate Active Directory Server or Azure AD 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, for example, ForgeRock LDAP or Oracle.
- Enrolled users are assigned to use one or more authentication methods -- Octopus Authenticator, FIDO Authenticator, a 3rd party authenticator (for example the ForgeRock authenticator app), or SMS / Email OTP from Twilio

- Workstations support TPM version 2.0
- The Enterprise Connect Passwordless for Windows MSI and MSIUpdater packages have been downloaded from Backstage.
- 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 Octopus 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 third-party directory (such as ForgeRock LDAP) 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**.

Active Directory Authentication	000000
lssuer	8 📢 8
Secret Double Octopus	

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 JPG or PNG file of your choice. Supported image size is 488x488 pixels.

Active Dir	ectory Authentication	:		
General Info	Parameters	Sign on	Directories	User
Service Name *			Display Icon	
Active Directory A	uthentication			
issuer*			Aller Andread	
Secret Double Oct	copus			
Description				
Description				
		11		
SAVE				

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 Azure AD).

Active D	i	
General Info	Parameters	Sign on
Parameters		
Service Paramete	ers	-
.ogin Identifier *		
Username		*
+ ADD PARAME	TER	

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.
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 .
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.

General Info	Parameters	Sign on	Directo	ories l	Jsers
Bypass Unassigned (Users		Bypass Unenro	olled Users	
Sign on Method			Authentication	n Token Timeout (1 mi	nute - 1 year) *
Active Directory			1	WEEKS	•
Endpoint URL			Rest Payload S	Signing Algorithm	
https://	o.com/adpa/303be3ce-	-641b-448 🖒	SHA-256		-
Service Keys *			X.509 Certifica	ate *	
Default		-	2022-05-11	11:42 SHA-256 2048	3-bit 👻
VIEW		+ ADD	VIEW] DOWNLOAD	🗘 REGENERATE
Custom Message *					
Active Directory a	authentication			METADATA	
		1.			

- 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. 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. 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 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**.

🕷 Enterprise Connect Passwordless MSIUpdater - Installation Wizard



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

Enterprise Connect Passwordless M	ISIUpdater - Installation Wizard	1
Ready to Install the Program		4
The wizard is ready to begin installation	on.	
Click Install to begin the installation.		
If you want to review or change any exit the wizard.	of your installation settings, click Back	. Click Cancel to

Enterprise Connect Passwordless for Windows Copyright © 2023 ForgeRock, All Rights Reserved. ×

A confirmation is displayed when installation is complete.

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.

Arganize • New folder OneDrive OneDrive - Person This PC 3 3D Objects Desktop	Date modified 15/05/2023 5:07 15/05/2023 5:08	Type Windows Ins Windows Ins	Size taller 98,907 KB taller 86,941 KB
 OneDrive OneDrive - Person This PC 3D Objects Desktop 	Date modified	Type	Size
	15/05/2023 5:07	Windows Ins	taller 98,907 KB
	15/05/2023 5:08	Windows Ins	taller 86,941 KB
OneDrive - Person ConeDrive - Person Connect Passwordless For Windows 32bit.msi This PC 3 3D Objects Desktop	15/05/2023 5:07	Windows Ins	taller 98,907 KB
	15/05/2023 5:08	Windows Ins	taller 86,941 KB
 Documents Downloads Music Pictures Videos S OS (C) Network 			

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:

ganize • New folde				• 📶
OneDrive	Name	Date modified	Туре	Size
OneDrive - Person	2023-05-15_145953552	15/05/2023 14:59	File folder	
Chiconice - reison	1 Enterprise Connect Passwordless For Windows 32bit.msi	15/05/2023 5:07	Windows Installer	98,907 KB
This PC	1 Enterprise Connect Passwordless For Windows 64bit.msi	15/05/2023 5:08	Windows Installer	86,941 KB
3D Objects				
Desktop				
Documents				
Downloads				
Music —				
Pictures				
Videos				
OS (C:)				

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.

🙎 Open						×
🗧 -> -> -^ 📙 « Pr	ogram Files > SecretDoubleOctopus > 3.8.0.809	2 → 2022-10-31_123150925		~ Ö	Search 2022-10-31_123150925	٩
Organize 👻 New fold	er				III • 🔲	0
This PC	Name	Date modified	Туре	Size		
3D Objects	My-Configuration.json	10/31/2022 12:31 PM	JSON File	18 KB		
Desktop						
Documents						
Downloads						
Music						
Pictures						
Videos						
Local Disk (C:)						
· · · · · · · · · · · · · · · · · · ·						
File n	ame:			~	JSON file (.json) (*.json)	\sim
					Open Cancel	I.

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.

rganize • New folder					JII • 🔟	
• OneDrive	Name	Date modified	Туре		Size	
Our Drive Dreves	2023-05-15_145953552	15/05/2023 14:59	File fo	lder		
OneDrive - Person	2023-05-15_153742552	15/05/2023 15:37	File fo	older		
This PC	1 Enterprise Connect Passwordless For Windows	32bit.msi 15/05/2023 5:07	Winde	ows Installer	98,907 KB	
3D Objects	👘 Enterprise Connect Passwordless For Windows	64bit.msi 15/05/2023 5:08	Winde	ows installer	86,941 KB	
Desktop						
Documents						
Downloads						
h Music						
Notures						
Videos						
💐 OS (C:)						

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.

General Info	Parameters	Sign on	Direc	tories l	Jsers	
Bypass Unassigned U	Users		Bypass Unen	rolled Users		
Sign on Method			Authenticatio	on Token Timeout (1 mir	nute - 1 year) *	
Active Directory			1	WEEKS		•
Endpoint URL			Rest Payload	Signing Algorithm		
https://	o.com/adpa/303be3ce	-641b-448 🖺	SHA-256			•
Service Keys *			X.509 Certific	cate *		
Default		•	2022-05-1	1 11:42 SHA-256 2048	3-bit	-
VIEW		+ ADD	VIEW	DOWNLOAD		RATE
Custom Message *						
Active Directory a	authentication		± SERVIC	E METADATA		
		1.				

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).

ganize • New folder						H · 0	1
OneDrive	Name	^	Date modified	Туре		Size	
OneDrive - Person	🕵 Enterprise Connect 📌 Enterprise Connect	t Passwordless For Windows 32bit.ms t Passwordless For Windows 64bit.ms	i 15/05/2023 5:07 i 15/05/2023 5:08	Windo Windo	ws Installer ws Installer	98,907 KB 86,941 KB	
This PC							
Desktop							
Documents							
Downloads							
Music							
Pictures							
Videos							
🗯 OS (C:)							
Network							
~							

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.

Parameters Load from XML (Optional)					
EndPoint URL					
External EndPoint URL (optional)					
Certificate EndPoint URL (optional if certificate authenticator not selected)					
Proxy EndPoint URL (optional)					
Service Key					
X509 Certificate	Browse				

- 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.
- **Proxy EndPoint URL:** Allows the Windows agent to connect via web proxy. Enter the address of the Proxy Server in the field.
- 5. Select one or more of the following authenticators:

Authenticator	Description / Notes
Octopus App	Octopus Authenticator mobile app (iOS/Android)
Octopus BLE	Select this checkbox to enable Octopus Bluetooth authentication. (Octopus App must be selected to enable this option.)
FIDO2	FIDO authenticator from Yubico or Feitian
FIDO2 (BIO)	FIDO authenticator with biometric fingerprint
ForgeRock Authenticator	Select this checkbox to enable login to Windows using ForgeRock authentication.
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 ForgeRock OTP 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: 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.

Authenticators
Octopus BLE
Hide Octopus BLE
FID02
🗖 FID02 (BIO)
ForgeRock Authenticator
Certificate Authenticator
ОТР
SMS
Email
Voice Call
Passphrase

Note: If you configured an External Endpoint URL (in Step 2), 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. Click **Next** to open the **Settings** tab. Note that the MSIUpdater version appears at the top of the tab.
- 7. Enable the settings as required by selecting the relevant checkboxes.

Enterprise Connection	ct Passwordless Update	r						
Parameters	Settings	MFA	Advanced	SysTray	Menu/Messages	CredUI	Errors	
Settings - V Show De Change F Lock Sor Use Last Enforce M TPM Sup Change F	Version 3.8.4.842 fault Credential Prov Password on Unlock een Authenticate Us Username UFA port Password on RDP	4 viders (In Addition to : er Automatically on	Enterprise Connect	t Passwordless)				
C Local Us	er Support							
POC Moc	ie							
Azure AD	Joined Machine							
Passwor	d Free Experience							
Use Sync	hronous HTTPS							
TLS Min O TLS 1.0 O TLS 1.1 O TLS 1.2 O TLS 1.3	Version) I 2 3							
UWrap Che	eckpoint Credential	Provider						
Allow Us	e of FIDO2 (PIN) wit	h FIDO2 (BIO)						
Enable Tr	race							
DirectAce	cess Support							
Network	LogonUser							
Bypass C	redentials Check							
FID02 US	ser Presence Requir	ed						
Bypass f	rom NLA Login		Group Name		oup Name (Domain\Gro			

Setting

Description / Notes

Show	Determines whether Windows default credential providers
Default	(Windows and Active Directory) are displayed when logging into
Credentia	Windows.
1	

Providers	
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 Authentic ate User Automati cally 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 or ForgeRock authenticators immediately after pressing <ctrl> <alt> </alt></ctrl> .
Use Last Username	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 (2 nd factor) when using domain username and password. This setting is relevant for users with Octopus or ForgeRock 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, Enterprise Connect Passwordless 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 .
SafeGuar d Support	Selecting this option enables Enterprise Connect Passwordless for Windows to login to the SafeGuard client (session).
POC Mode	When selected, Enterprise Connect Passwordless 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.
Azure AD Joined Machine	Select this checkbox when the workstations are configured to connect with the Azure AD domain. When the setting is selected, users will be prompted to login with UPN and not Username.
Password Free	Select this checkbox to enable a Passwordless authentication experience for MFA users. When selected, users are required to

Experienc e	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.
Use Synchron ous HTTPS	By default, the system uses Microsoft libraries with an asynchronous connection. When the checkbox is selected, the system will switch to a synchronous connection if issues with asynchronous connection occur.
TLS Min Version	
Wrap Check Point Credentia l Provider	Select this checkbox to enable Octopus Authenticator to work together with the Check Point Full Disk Encryption credential provider.
Allow User 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.
Enable Trace	Select this checkbox to enable the logs by default immediately after installation.
DirectAcc ess Support	Select this checkbox to enable support of the DirectAccess VPN.
Bypass Credentia ls Check	When selected, an alternate Windows API will be used in the event of rare timeout issues in password-free mode.
FIDO2 User Presence	When selected (default setting) , FIDO2 users are required to to touch the token after entering their PIN. To disable this requirement, verify that the checkbox is NOT selected.
kequirea	This checkbox is enabled only when the FIDO2 authenticator is selected in the Parameters tab.
	Note: This feature requires configuration of relevant settings in the Management Console.

BypassWhen selected, users who are members of the Bypass Group(s)from NLAwill not require authentication when using NLA login. Enter the
group name(s) in the required syntax in the field to the right.

- 8. Click **Next** to open the **MFA** tab.
- 9. 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 the Octopus or ForgeRock authenticator. 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.

Parameters	Settings	MFA	Advanced	SysTray	Menu/Messages	CredUI	Errors	
MFA Settin	gs							
Enable M	ulti-Factor Authentic	ation (MFA)						
MFA Cha	nge Password Suppo	ort						
Bypass L	ocal User Login							
E Force Off	ine OTP After Install	ation						
🔲 Bypass N	IFA on Unlock when	Connected to AD						
III Hide MFA	Password							
Force Loc	k After Offline OTP							
Bypass N	IFA Groups							

10. 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 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 Installatio n	When selected, users are unable to perform offline authentication until they have had at least one successful online login.
Bypass MFA on Unlock when Connected	When selected, users connected to the enterprise network who have already authenticated with MFA are not required to authenticate with 2 nd factor again when unlocking the workstation. This will work as long as you are inside the network (no time limit).

to AD	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).
Bypass MFA Groups	When selected, you may specify ONE group in the AD that will not require MFA authentication. Enter <domain>\>Group Name></domain> in the field to the right.
	IMPORTANT: When selecting this option, verify that the Bypass MFA on Unlock when Connected to AD checkbox is

11. Click **Next** to open the **Advanced** tab.

NOT selected.

Interprise Connect Passwordless Updater								
Parameters	Settings	MFA	Advanced	SysTray	Menu/Messages	CredUI	Errors	
Advanced	Settings							
Enable St	DO SSO			https://centos7	https://centos77/ 3m:8443/login			
Change C	Octopus Name			Octopus Name				
🛄 Change C	OTP Name			OTP Name				
Change ForgeRock Authenticator Name								
Change SMS Name		SMS Name						
Change Email Name		Email Name						
Change Voice Call Name		Voice Call Name						
Change Passphrase Name								
Change Certificate Name		Certificate Name						
Enable CP Bypass List								
🗌 Use Moni	itor Prefix							
Change Trace Log Directory								

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

Setting	Description / Notes
Enable SDO SSO	After selecting the checkbox, enter the 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.
Change Octopus Name	Allows you to change the default name of the 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.

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., <i>ForgeRock OTP</i>). This setting is available only when the OTP checkbox in the Parameters tab is selected.
Change ForgeRoc k Authentic ator Name	Allows you to change the default name of the ForgeRock 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 ForgeRock 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 Passphra se 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 Certificat e 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 (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.
Use Monitor Prefix	When selected (and when there is a prefix match), the Windows Login screen presents users with the Octopus 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.

🛃 Device Manager		
File Action View Help		
🗢 🌳 📰 🖾 🖬 💆	Generic PnP Monitor Properties	×
 alurentI-lap alurentI-lap alurentI-lap alurentI-lap Batteries Bluetooth Cameras 	General Driver Details Events Generic PnP Monitor	
> 💻 Computer	Property	
> 🚽 DellInstrumentation	Hardware Ids	~
 Disk drives Display adapters Firmware Human Interface Devices Keyboards Mamony technology data 	Value MONITOR\DELD0C2	
Mice and other pointing Monitors Generic PnP Monitor Generic PnP Monitor Generic PnP Monitor		
 Network adapters Ports (COM & LPT) 		
> 🖻 Print queues		
> 🚍 Printers		
 Processors Processors Security devices 	ОК	Cancel

Change Trace Log Directory

13. If desired, customize the Windows login experience by replacing the default logo and icons with your own images.

Organization Logo	
Organization Logo File	Browse
Phone Icon	
Phone Icon File	Browse
Fido Icon	
Fido Icon File	Browse

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

The following options are available:

- **Organization Logo:** Displays your company's logo on the Windows Login screen instead of the default Secret Double Octopus logo. For example:

	O.E.M. Products
	\Administrator →
	Sign in to
	Octopus App 🗸 🗸
	Login with Username and Password
Administrator	
CIEM! Secret Double Octopus	
Switch user	

- **Phone Icon:** Displays the icon of your choice on the **Check Your Phone** prompt instead of the default Secret Double Octopus icon.



- Fido Icon: Displays the icon of your choice on the prompt to touch the Fido key.
- 14. 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:

Help Image On Login Screen		
Enable Help Link		
	For any assistance please contact help desk support center: Tel: +2345646678755 Email: support@domain.com	
Click here to see support details	×	

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

CORPORATION	
Ibername	
Sign in to:	
How do I sign in to another domain? Octopus App	
Login with Username and Pilisword Click to close Help support	
For assistance contact Help desk	
Tel: +2344567789977 Tel: - 301444556677 Fmail: superfilidomain.com	

- 15. At the bottom of the **Advanced** tab, click **Next**.
- 16. Open the **SysTray** tab. To activate the system tray actions menu that allows users to perform self-service flows, select the **Enable SysTray** checkbox.



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

Important: The options related to FIDO authentication are enabled only when **FIDO2** is selected as an authenticator in the **Parameters** tab.

Action	Description / Notes
Retrieve Password with SDO Authenticator /Admin Bypass Token	When selected, users are able to view and copy the AD password after performing passwordless authentication on the authenticator mobile app. (The password is stored in memory for 30 seconds.) Admin users in Bypass mode need to enter the temporary token to retrieve the password.
Retrieve Password with ForgeRock Authenticator /Admin Bypass Token	When selected, users are able to view and copy the AD password after performing passwordless authentication on the ForgeRock authenticator mobile app. (The password is stored in memory for 30 seconds.) Admin users in Bypass mode need to enter the temporary token to retrieve the password.
Retrieve Password with FIDO2	When selected, users are able to view and copy the AD password after performing passwordless authentication using a FIDO key. (The password is stored in memory for 30 seconds.)
Retrieve Password with	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. (The password is stored

	Certificate	in memory for 30 seconds.)
	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. The token will be available for 60 seconds and will then expire.
	Check Credentials Status	When selected, users are able to view the time remaining until password expiration.
	Launch ForgeRock SSO Portal with SDO Authenticator / Admin Bypass Token	When selected, users are able to open the Portal from the desktop after performing passwordless authentication on the authenticator mobile app. Admin users in Bypass mode need to enter the temporary token to launch the Portal.
	Launch ForgeRock SSO Portal with FIDO2	When selected, users are able to open the Portal from the desktop after performing passwordless authentication using a FIDO key.
	Launch ForgeRock SSO Portal with Certificate	When selected, users are able to open the Portal from the desktop after performing authentication using a smart card signed by the organization's root CA.
	Launch ForgeRock SSO Portal with ForgeRock Authenticator /Admin Bypass Token	When selected, users are able to open the Portal from the desktop after performing passwordless authentication on the ForgeRock authenticator mobile app. Admin users in Bypass mode need to enter the temporary token to launch the Portal.
	Kiosk Mode	When selected, users are able to work in Windows kiosk mode.
	Do Not use User with Cisco VPN	
	Use Cisco Secure Client (V5)	
Ent Cop	Launch Check Point VPN erprise Connect Passy pyright © 2023 Forge	When selected, users are able to connect to the Check Point VPN directly from the desktop after performing passwordless wordless for Windows Rock, All Rights Reserved.
	0	<u> </u>

with SDO Authenticator	authentication on the 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: <i>office,C:\Program Files (x86)\CheckPoint\Endpoint Security\Endpoint Connect</i>
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 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 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 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 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 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	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

Using FIDO2 name of the Cisco VPN, as set on the Cisco client.

Note: After deployment of Enterprise Connect Passwordless 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.)

18. 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.

- 19. Click Next.
- 20. In the **Menu/Messages** tab, review 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: Reset	s the Strings list	t with the original	default texts.

Metal Dode String Type Mexul, D., 24L, UNIC+PORTAL Launch 550 Orbral with Systery Minu Mexul, D., 24L, UNIC+PORTAL Launch 550 Orbral with Systery Minu Mexul, D., 24L, UNIC+PORTAL Launch 550 Orbral with 52D Authenticators / Admini Spass Token Systery Minu Mexul, D., 24L, UNIC+PORTAL Launch 55D Orbral with 52D Authenticators / Admin Spass Token Systery Minu Mexul, D., LAUNC+PORTAL, ERT Launch 55D Orbral with 52D Authenticators / Admin Spass Token Systery Minu Mexul, D., LAUNC+PORTAL, ERT Launch 55D Orbral with 52D Authenticators / Admin Spass Token Systery Minu Mexul, D., LAUNC+PORTAL, ERT Launch 55D Orbral with 52D Authenticators / Admin Spass Token Systery Minu Mexul, D., LAUNC+PORTAL, ERT Launch 55D Orbral with 52D Authenticators / Admin Spass Token Systery Minu Mexul, D., PASSYORD Entrefe Passand with 52D Authenticators / Admin Spass Token Systery Minu Mexul, D., PASSYORD, D., EHCOPART, CERT Launch 52D Orbral with 52D Authenticators / Admini Spass Token Systery Minu Mexul, D., PASSYORD, D., EHCOPART, CERT Launch 52D Orbral with 52D Authenticators / Admini Spass Token Systery Minu Mexul, D., PASSYORD, D., EHCOPART, CERT		Errors	CredUI	Menu/Messages	SysTray	Advanced	MFA	Settings	rameters
Menu String Type Code String Type Menu, D., Suk, NUCHFORTAL, Laundh Sonsord with System Menu, D., Sea, NUCHFORTAL, Laundh Sonsord with System Menu, D., LORED, MINI Ablue System Menu, D., LORED, MINI Ablue System Menu, D., LORED, MINI Ablue System Menu, D., LORED, MINI Reline Cedentials System Menu, D., LAUNCHFORTAL, Launch SSD Portal with SIDA Authenticator /Admin System Striken System Menu, D., LAUNCHFORTAL, ED0 Launch SSD Portal with SIDA / Authenticator /Admin System System Menu, D., LAUNCHFORTAL, ED0 Launch SSD Portal with SIDA / Authenticator /Admin System Striken System Menu, D., LAUNCHFORTAL, ED0 Launch SSD Portal with FIDO (Pin) System / Menu Menu, D., LAUNCHFORTAL, PID0 Launch SSD Portal with FIDO (Pin) System Menu, D., LAUNCHFORTAL, PID0 Launch Check-Port VPN with FIDO (Pin) System / Menu Menu, D., PASSVORD, DEFIDORINT, VPN SID Launch Check-Port VPN with FIDO (Pin) System / Menu Menu, D., PASSVORD, DEFIDORINT, VPN SIDO Launch Check									
Load time USV (piperal) Code String Type Code String Amulton Proof TAL Launch SID Portal with Systemy Minu Metra, UD, SHIN, UNKOHPORTAL, Launch SID Portal with Systemy Minu Systemy Minu Metra, UD, SHIN, UNKOHPORTAL, Launch SID Portal with Systemy Minu Systemy Minu Metra, UD, SHIN, UNKOHPORTAL, Launch SID Portal with SID Authenticator / Admin Sysass Token Systemy Minu Metra, UD, CHERN CHORTAL, CERT Launch SID Portal with SID Authenticator / Admin Sysass Token Systemy Minu Metra, UD, LAUNCHORTAL, CERT Launch SID Portal with SID O (Bin) Systemy Minu Metra, UD, LAUNCHORTAL, CERT Launch SID Portal with SID O (Bin) Systemy Minu Metra, UD, LAUNCHORTAL, CERT Launch SID Portal with SID O (Bin) Systemy Minu Metra, UD, SASKVORD Retrive Passord with Certificate Systemy Minu Metra, UD, SASKVORD, CHERT CERT Launch CheckFormt VPN ath TO(D (Pin) Systemy Minu Metra, UD, SASKVORD, CHERT VER, Metra Launch CheckFormt VPN ath TO(D (Pin) Systemy Minu Metra, UD, SASKVORD, CHERT VER, Metra Launch CheckFormt VPN ath TO(D (Pin) Systemy Minu									Menu
Odd String Tiple Mexu, D., 20, 40, 40400744. Launch 550 Portal with Spritzy Mmu Spritzy Mmu Mexu, D., 20, 2040, 20074 About. Spritzy Mmu Spritzy Mmu Mexu, D., 20, 2040, 20074 About. Spritzy Mmu Spritzy Mmu Mexu, D., 20, 20074 About. Spritzy Mmu Spritzy Mmu Mexu, D., 20, 20074 Clock App Spritzy Mmu Spritzy Mmu Mexu, D., LAUNCHFORTAL, CET Launch 550 Portal with 500 Authenticator/Admin Bypass Token Spritzy Mmu Mexu, D., LAUNCHFORTAL, CET Launch 550 Portal with 500 Portal with 500 Authenticator/Admin Bypass Token Spritzy Mmu Mexu, D., LAUNCHFORTAL, CET Launch 550 Portal with 500 Portal with 500 Authenticator/Admin Bypass Token Spritzy Mmu Mexu, D., Spritzy Mmu Launch 550 Portal with 500 Portal with 500 Authenticator Mmu Bypass Token Spritzy Mmu Mexu, D., Spritzy Mmu Launch CheckPort VPN with FIG0 IPO Spritzy Mmu Mexu, D., Spritzy Mmu Launch CheckPort VPN with FIG0 IPO Spritzy Mmu Mexu, D., Spritzy Mmu Launch CheckPort VPN with FIG0 IPO Spritzy Mmu Mexu, D., Spritzy Mmu Launch CheckPort VPN with FIG0								SV (Optional)	Load from CS
Menu, D., Jack, MINO-PORTAL Launch SD0 Portal with Spirtury Menu Menu, D., Jack, SNOORD Retrieve Passion with Spirtury Menu Menu, D., Jack, SNOORD Retrieve Passion with Spirtury Menu Menu, D., Jack, SNOORD Retrieve Passion with Spirtury Menu Menu, D., LARDUT About. Spirtury Menu Menu, D., LARDUT Close App Spirtury Menu Menu, D., LARNO-PORTAL, CERT Launch SSD Portal with SDO Authenticator /Admin Bypass Token Spirtury Menu Menu, D., LAINO-PORTAL, CERT Launch SSD Portal with SDO Alphaneticator /Admin Bypass Token Spirtury Menu Menu, D., LAINO-PORTAL, CERT Launch SSD Portal with SDO Alphaneticator /Admin Bypass Token Spirtury Menu Menu, D., ALSINO-PORTAL, FLOD Launch SSD Portal with SDO Alphaneticator /Admin Bypass Token Spirtury Menu Menu, D., ALSINO-BO, DIEGO MIT, FERT Launch SDD Portal with SDO Alphaneticator /Admin Bypass Token Spirtury Menu Menu, D., ALSINO-BO, CHEORYONT, VERT Launch Diceo/Vert VIN with ToD (Pri) Spirtury Menu Menu, D., ALSINOBO, CHEORYONT, VERT Launch Diceo/VPI VIN with TADD (Apple: Admenicator /Admin Bypass Token Spirtury Menu Menu, D., ALSINOBO, CHEORYONT, VERT <	Type				tring	4			Code
Menu, D., Jaskinskov ORP Refere Plassord with Systep Menu Menu, D., D., DRD, MENU About. Systep Menu Menu, D., D., DRD, MENU Refere Ordentials Systep Menu Menu, D., D., DRD, MENU Close App Systep Menu Menu, D., D., ALNO-HORTAL, CERT Launch SSD Prist with SDD Althouting Systep Stein Systep Menu Menu, D., LAUNCHORTAL, CERT Launch SSD Prist with SDD Althouting Systep Stein Systep Menu Menu, D., LAUNCHORTAL, CERT Launch SSD Prist with SDD Althouting Systep Stein Systep Menu Menu, D., LAUNCHORTAL, CERT Launch SSD Prist with SDD Prist With SDD Althouting Systep Stein Systep Menu Menu, D., D., SSNORD, CHECKTONT, VEN, SDD Enterine Step Stein Menu Systep Menu Menu, D., D., SSNORD, CHECKTONT, VEN, SDD Launch Doeskinner VIN with SDD Althouting Stein Systep Menu Menu, D., D., SSSNORD, CHECKTONT, VEN, SDD Launch Doeskinner VIN with SDD Althouting Stein Using Stein OTP Systep Menu Menu, D., D., SSSNORD, CHECKTONT, VEN, SDD Launch Doeskinner VIN with SDD Althouting Stein Using Stein OTP Systep Menu Menu, D., D., SSSNORD, CHECKTONT, VEN, SDD Launch Dicke VIN with SDD Althouting Stein Using Stein OTP Systep Menu	Systray Menu			th	unch SSO Portal w	1		dLAUNCHPORTAL	Menu ID 3
Meru, J., Abdurf Abort. Sprigre Meru Meru, J., ORED, MENU Retrive Profestional Sprigre Meru Meru, J., DLRND, VIENU Close App Sprigre Meru Meru, J., DLRND, VIENU Launch SSD Partal with SDD Authenticator //Admin Bypass Token Sprigre Meru Meru, J., LAUNCHPORTAL, EERT Launch SSD Partal with SDD Authenticator //Admin Bypass Token Sprigre Meru Meru, J., LAUNCHPORTAL, EDD Launch SSD Partal with SDD Authenticator //Admin Bypass Token Sprigre Meru Meru, J., LAUNCHPORTAL, EDD Launch SSD Partal with SDD Authenticator //Admin Bypass Token Sprigre Meru Meru, J., LAUNCHPORTAL, EDD Launch SSD Partal with SDD Authenticator //Admin Bypass Token Sprigre Meru Meru, J., JAUNCHPORTAL, EDD Launch SSD Authenticator //Admin Bypass Token Sprigre Meru Meru, J., MSSWORD, DEBRY Meru Launch Decelority VIII with DD (Phi) Sprigre Meru Meru, J., MSSWORD, DEBRY Meru Launch Decelority VIII with PDD (Phi) Sprigre Meru Meru, J., MSSWORD, DEBRY Meru Launch Decelority VIIII with PDD (Phi) Sprigre Meru Meru, J., MSSWORD, DEBRY Meru Launch Doceol VIIII with PDD (Phi) Sprigre Meru Meru, J., MSSWORD, DEBRY MERU Launch Do	Systray Menu			th	etrieve Password w	P		rdPASSWORD	Menu ID 3t
Menu, J., D. RED, MENU Retrieve Ordentialis Systep: Menu Menu, J., D. ZHO, CRED, MENU Globe App Systep: Menu Menu, J., D. J. ALNO-HPORTAL Launch SSD Pathal with SDD Authenticator / Admin Bypass Token Systep: Menu Menu, J., D. J. ALNO-HPORTAL, CERT Launch SSD Pathal with Certificate Systep: Menu Menu, J., D. J. ALNO-HPORTAL, ERT Launch SSD Pathal with Certificate Systep: Menu Menu, J. D. J. ALNO-HPORTAL, ERT Launch SSD Pathal with FIDD (Bin) Systep: Menu Menu, J. D. J. ALNO-HPORTAL, ERD E Bathal With Certificate Systep: Menu Menu, J. D. J. ALNO-HPORTAL, ERD E Bathal With Certificate Systep: Menu Menu, J. D. J. ASSNORD, DERT Bettern Passend with Pitch Fidate Systep: Menu Menu, J. D. ASSNORD, CHECK POORT, YVPL Launch Dicks/Ponr VVPL with PIDD (Pin) Systep: Menu Menu, J. D. ASSNORD, CHECK POORT, YVPL, SDD Launch Dicks/Ponr VVPL with SDD Authenticator Systep: Menu Menu, J. D. ASSNORD, CHECK POORT, YVPL, SDD Launch Dicks/Ponr VVPL with SDD Authenticator Systep: Menu Menu, J. D. ASSNORD, CHECK PONT, YVPL, SDD Launch Dicks/Ponr VVPL with SDD Authenticator Systep: Menu Menu, J. D. ASSNORD, CHECK PONT, YVP	Systray Menu				bout	A		BOUT	Menu ID Al
Merul, DL, XIM: CMORTAL Close App Systery Meru Merul, DL, ALMON-PORTAL Launch SSD Partial with SDD Authenticator /Admin Bypass Token Systery Meru Merul, DL, ALMON-PORTAL, EDBT Launch SSD Partial with SDD Authenticator /Admin Bypass Token Systery Meru Merul, DL, ALMON-PORTAL, EDBT Launch SSD Partial with SDD Authenticator /Admin Bypass Token Systery Meru Merul, DL, ALMON-PORTAL, EDD Launch SSD Partial with FDD (Pin) Systery Meru Merul, DL, ALMON-PORTAL, EDD Launch SSD Partial with FDD (Bin) Systery Meru Merul, D, ASSWORD, DLEXPRONT, CBIT Retrieve Password with Certificate Systery Meru Merul, D, ASSWORD, DLEXPRONT, CBIT Launch CheckForder /VM with FDD (Pin) Systery Meru Merul, D, ASSWORD, DLEXPRONT, VIN, Launch CheckForder /VM with FDD (Pin) Systery Meru Systery Meru Merul, D, ASSWORD, DLEXPRONT, VIN, Launch CheckForder /VM with FDD (Pin) Systery Meru Systery Meru Merul, D, ASSWORD, DLEXPRONT, VIN, LBD Launch CheckForder /VM with FDD (Pin) Systery Meru Merul, D, ASSWORD, DLEXPRONT, VIN, LBD Launch CheckForder /VM with FDD (Pin) Systery Meru Merul, D, ASSWORD, DLEXPRONT, VIN, LBD Launch CheckFore Win with FDD (Pin) Systery Meru	Systray Menu				strieve Credentials	P		RED_MENU	Menu ID_C
MemL, DL, ALKNOHPORTAL, CERT Laurch 550 Petral with 500 Aukhenkiakov/Admin Bypass Token Systery MemL MemL, DL, ALKNOHPORTAL, CERT Laurch 550 Petral with PC00 (Pin) Systery MemL MemL, DL, ALKNOHPORTAL, CERT Laurch 550 Petral with PC00 (Pin) Systery MemL MemL, DL, ALKNOHPORTAL, CERT Laurch 550 Petral with PC00 (Pin) Systery MemL MemL, DL, ALKNOHPORTAL, CERT Bittery MemL Systery MemL MemL, DL, ALKNOHPORTAL, EPDB, SO Laurch 550 Petral with PC00 (Bin) Systery MemL MemL, DL, ALKNOHPORTAL, PDB, SO Bittery MemL Systery MemL MemL, DL, ALKNOHPORTAL, PDB, SO Bittery MemL Systery MemL MemL, DL, ALSKOHPORT, CERT Reinver Password with SDG Authenticator/Admin Bypass Token Systery MemL MemL, DL, ALSKOHPORT, VPNL SDL Laurch Dickohom VPN with PDD (Pin) Systery MemL MemL, DL, ASSKOHPORT, SOND, SDL, SDL, SDL, SDL, SDL, SDL, SDL, SD	Systray Menu				ose App	C		XIT	Menu ID_E
Memu, D, LANKOHPORTAL, CERT Launch SSD Portal with Certificate Systey Memu Memu, D, LANKOHPORTAL, EDD Launch SSD Portal with PEOD (Ph) Systey Memu Memu, D, LANKOHPORTAL, PIDD Launch SSD Portal with PEOD (Ph) Systey Memu Memu, D, LANKOHPORTAL, PIDD Launch SSD Portal with PEOD (Ph) Systey Memu Memu, D, ASSWORD, DLEXPIN Retrieve Password with Certificate Systey Memu Memu, D, ASSWORD, DLEXPIN T, CERT Launch CheckPoint VPN with PIDD (Ph) Systey Memu Memu, D, ASSWORD, DLEXPIN T, VPN, LBD Launch CheckPoint VPN with PIDD (Ph) Systey Memu Memu, D, ASSWORD, DLEXPIN T, VPN, LBD Launch CheckPoint VPN with PIDD (Ph) Systey Memu Memu, D, ASSWORD, DLEXPIN T, VPN, LBD Launch CheckPoint VPN with PIDD (Ph) Systey Memu Memu, D, ASSWORD, DLEXPIN T, VPN, LBD Launch CheckPoint VPN with SDD Authenticator Systey Memu Memu, D, ASSWORD, DLEXD, VPN, LBD Launch CheckPoint VPN with SDD Authenticator Systey Memu Memu, D, ASSWORD, DLEXD, DLEXD, VPN, LBD Launch CheckPoint VPN with SDD Authenticator Systey Memu Memu, D, ASSWORD, DLEXD, DLEXD, VPN, LBD Launch CheckPoint VPN with PDD (B) Systey Memu Memu, D, ASSWORD, DLEXD, VPN, L	Systray Menu		min Bypass Token	ith SDO Authenticator/Ad	sunch SSO Portal w	L		AUNCHPORTAL	Menu_ID_L
Memu, D., LAND-HORTAL, FJO.0 Launch SSD Pertail with FJO.00 Systay Memu Memu, D., LAND-HORTAL, FJO.0, BIO Launch SSD Pertail with FJO.00 Systay Memu Memu, D., JALSHOVERDL, FJO.0, BIO Retrieve Passancet with SDO Aubenticator/Admin Bypass Token Systay Memu Memu, D., PASSWORD, CERT Retrieve Passancet with SDO Aubenticator/Admin Bypass Token Systay Memu Memu, D., PASSWORD, CERT Launch DickeVionit VPN with Derificate Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN Launch DickeVionit VPN with FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch DickeVionit VPN with FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch DickeViont VPN with FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch DickeViont VPN with FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch DickeViont VPN with FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch DickeViont VPN with FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch DickeVIN With FDO IBIO Systay Memu Memu, D., PASSWORD, CHECKPOINT, VPN, BIO Launch Dicke VPN with FDO IBIO Systay Memu	Systray Menu			ith Certificate	unch SSO Portal w	L	RT	AUNCHPORTAL_CE	Menu ID_L
Memu, D., ASSWORD, CHEVRIAL, PIDD, BID Laurch BISD PotRi with PIDD (Bib) Systey Memu Memu, D., ASSWORD, CHEVR Retrieve Password with Certificate Systey Memu Memu, D., ASSWORD, CHEVR Retrieve Password with Certificate Systey Memu Memu, D., ASSWORD, CHEVR Laurch Discovery VM with Certificate Systey Memu Memu, D., ASSWORD, CHEVR Laurch Discovery VM with Certificate Systey Memu Memu, D., ASSWORD, CHEVRY ONT, VM, BID Laurch Discovery VM with PIDD (Ph) Systey Memu Memu, D., ASSWORD, CHEVRY ONT, VM, BID Laurch Discovery VM with PIDD (Ph) Systey Memu Memu, D., ASSWORD, CHEVRY CORD, Status, DC, OTP Laurch Discovery VM with PIDD (Ph) Systey Memu Memu, D., MSSWORD, CHEVRY CORD, Status, DC, OTP Laurch Discovery VM with SIDD Authenticator Systey Memu Memu, D., MSSWORD, CHEVR, DEGO, STATUS, DC, OTP Laurch Discovery VM with SIDD Authenticator Systey Memu Memu, D., MSSWORD, CHEVR, DEGO, STATUS, DC, OTP Laurch Discover VM with FIDD (Ph) Systey Memu Memu, D., MSSWORD, CHEVR, DEGO, TH, BL, OTP Laurch Discover VM with FIDD (Ph) Systey Memu Memu, D., MSSWORD, CHEVR, DEGO, TH, BL, OTP Laurch Discover VM with FIDD (SH) UWH SIDD Authenticator Systey Memu<	Systray Menu			th FIDO (Pin)	unch SSO Portal w	L	0	AUNCHPORTAL_FIC	Menu_ID_L
Memu, D., ASSWORD, CERT Retrieve Password with SDD / Aukhenicator/Johnn Bypass Token Systey Menu Memu, D., ASSWORD, CERT Retrieve Password with Cetificate Systey Menu Memu, D., ASSWORD, CHECKPOINT, CERT Launch Decklorint VPN with Cetificate Systey Menu Memu, D., ASSWORD, CHECKPOINT, CERT Launch Decklorint VPN with TDD (Bin) Systey Menu Memu, D., ASSWORD, CHECKPOINT, VPN, BIO Launch Decklorint VPN with TDD (Bin) Systey Menu Memu, D., ASSWORD, CHECKPOINT, VPN, BIO Launch Decklorint VPN with TDD (Bin) Systey Menu Memu, D., ASSWORD, CHECKPOINT, VPN, BIO Launch Discov VPN with TDD (Bin) Systey Menu Memu, D., ASSWORD, CIRCO, CIR	Systray Menu			ith FIDO (Bio)	unch SSO Portal w	L	0_80	AUNCHPORTAL_FIC	Menu JD_L
Memu, D., ASSWORD, CERT Retrieve Passand with Certificate Systay, Menu Memu, D., ASSWORD, CHEXPN DT, VPN Launch CheckPoint VPN with Definition Systay, Menu Memu, D., ASSWORD, CHEXPN DT, VPN, Launch CheckPoint VPN with PIOD (Ph) Systay, Menu Systay, Menu Memu, D., ASSWORD, CHEXPN DT, VPN, LBD Launch CheckPoint VPN with PIOD (Ph) Systay, Menu Memu, D., ASSWORD, CHEXPN DT, VPN, LBD Launch CheckPoint VPN with PIOD (Ph) Systay, Menu Memu, D., ASSWORD, CHEXPN DT, VPN, LBD Launch CheckPoint VPN with PIOD (Ph) Systay, Menu Memu, D., ASSWORD, CHEXPLOYD, Source, Sour	Systray Menu		min Bypass Token	th SDO Authenticator/Ad	etrieve Password w	R		ASSWORD	Menu_ID_P
Mem. U., D. ASSIVNORD, CHECKPOINT_CERT Launch Dickskörind VPN with Certificate Systey Mem. Mem. U., D. ASSIVNORD, CHECKPOINT_VPN LIL aunch Dickskörind VPN with POD (Bio) Systey Mem. Mem. U., D. ASSIVNORD, CHECKPOINT_VPN, BIO Launch Dickskörind VPN with POD (Bio) Systey Mem. Mem. U., D. ASSIVNORD, CHECKPOINT_VPN, BIO Launch Dickskörind VPN with POD (Bio) Systey Mem. Mem. U., D. ASSIVNORD, CHECKPOINT_VPN, BIO Launch Dickskörind VPN with SDO Authenticator Systey Mem. Mem. U., D. ASSIVNORD, CIRCO, C	Systray Menu			ith Certificate	strieve Password w	8		ASSWORD_CERT	Menu_ID_P
Memu, U, ASSWORD, CHECK/PONT, VPN Launch Dicks/brint VPN with FIDO (Pin) Systey Memu Memu, U, ASSWORD, CHECK/PONT, VPN, SID Launch Dicks/brint VPN with FIDO (Pin) Systey Memu Memu, U, ASSWORD, CHECK/PONT, VPN, SID Launch Dicks/brint VPN with FIDO (Pin) Systey Memu Memu, U, ASSWORD, CHECK/PONT, VPN, SID Launch Dicks/brint VPN with FIDO (Pin) Systey Memu Memu, U, ASSWORD, CHECK, VPN, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, VPN, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, VPN, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, VPN, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, VPN, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, URL, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, URL, VPN, SIDO Launch Dicks/VPN with SIDO Authenticator Systey Memu Memu, U, ASSWORD, CHECK, LEDO, VPN, LEDO Check redential Statas Systey Memu Memu, U, ASSWORD, EXPIRED Check redential Statas Systey Memu	Systray Menu			PN with Certificate	aurich CheckPoint V	Ł	POINT_CERT	ASSWORD_CHECK	Menu_ID_P
Memu, D, ASSKYNGR, CHECKPONT, VPN, BIO Launch DheckPoint VPN with PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CHECKPONT, VPN, BIO Launch DheckPoint VPN with PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, DSD, BIO, OTP Launch DickeVPI VPN with PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, DSD, BIO, OTP Launch DickeVPI VPN with PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, CIRECX, VPN, Launch DickeVPI with PDO (Bio) Systey Memu Systey Memu Memu, D, ASSKYNGR, CIRECX, VPN, LBIO Launch DickeVPI with PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, VPN, LBIO, CIRECX, LBIO, CIRECX, VPN, With PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, VPN, LBIO, CIRECX, VPN, With PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, VPN, LBIO, CIRECX, VPN, With PDO (Bio) Systey Memu Memu, D, ASSKYNGR, CIRECX, VPN, LBIO, CIRECX, VPN, With SDO Aldrenicator Systey Memu Memu, D, ASSKYNGR, CIRECX, PLEXPED Check Ordential Status Systey Memu Memu, D, ASSKYNGR, PLEXPED Check Ordential Status Systey Memu	Systray Menu			PN with FIDO (Pin)	aunch CheckPoint V	L	POINT_VPN	ASSWORD_CHECK	Menu, ID, P
Mem_U_D_ASSWORD_CHEEORPOIT_VPN_SDD Launch Dhock>Point VPN with SDD Authenticator Systay Memu Mem_U_D_ASSWORD_CREDCS_DDB_00_07P Launch Diose VPN with SDD Authenticator Systay Memu Mem_U_D_ASSWORD_CREDCS_VPN Launch Diose VPN with SDD Authenticator Systay Memu Mem_U_D_ASSWORD_CREDCS_VPN Launch Diose VPN with SDD Authenticator/Amin Bypass Token Using Stient OTP Systay Memu Mem_U_D_ASSWORD_CREDCS_VPN_LBD_CTP Launch Diose VPN with FDD Big Using Stient OTP Systay Memu Mem_U_D_ASSWORD_CREDCS_VPN_LBD_CTP Launch Diose VPN with FDD Big Using Stient OTP Systay Memu Mem_U_D_ASSWORD_CREDCS_VPN_LBD_CTP Launch Diose VPN with SDD Authenticator Systay Memu Mem_U_D_ASSWORD_CREDCS_VPN_LBD_CTP Launch Diose VPN with SDD Authenticator Systay Memu Mem_U_D_ASSWORD_DRED_VPRED Check Credential Status Systay Memu Systay Memu Mem_U_D_ASSWORD_FIDE Check Credential Status Systay Memu Systay Memu Systay Memu	Systray Menu			PN with FIDO (Bio)	sunch CheckPoint V	L	OINT_VPN_BIO	ASSWORD_CHECK	Menu_ID_P
Memu, D, ASSVORD, CISCO, 2000, JBO, CPP Launch Cisco VPN. with SDO Authenticater/Admin Bysess Token Using Silent OTP Systey Memu Memu, D, ASSVORD, CISCO, CPN Launch Cisco VPN. with FDO (Pin) Systey Memu Memu, D, ASSVORD, CISCO, CPN, LBIO Launch Cisco VPN. with FDO (Pin) Systey Memu Memu, D, ASSVORD, CISCO, VPR, LBIO Launch Cisco VPN. with FDO (Bio) Systey Memu Memu, D, ASSSVORD, CISCO, VPR, LBIO, CTP Launch Cisco VPN. with FDO (Bio) Using Silent OTP Systey Memu Memu, D, ASSSVORD, CISCO, VPR, LBIO, CTP Launch Cisco VPN with FDO (Bio) Using Silent OTP Systey Memu Memu, D, ASSSVORD, CISCO, VPR, LSRT Launch Cisco VPN with SDO Authenciator Systey Memu Memu, D, ASSSVORD, CISCO, VPR, LSRT Launch Cisco VPN with SDO Authenciator Systey Memu Memu, D, ASSSVORD, DEOR, DFNDED Check Credential Status Systey Memu Memu, D, PASSVORD, FIDO Referve Password with FDO (Pin) Systey Memu	Systray Menu		or	PN with SDO Authenticat	sunch CheckPoint V	L	POINT_VPN_SDO	ASSWORD_CHECKR	Menu_ID_P
Memu, D., ASSWORD, CIRCO, VPN Launch Dicos VPN with FIDO (PIn) Systay Memu Memu, D., ASSWORD, CIRCO, VPN, BIO Launch Dicos VPN with FIDO (Bio) Systay Memu Memu, D., PASSWORD, CIRCO, VPN, BIO, CITP Launch Dicos VPN with FIDO (Bio) Using Slent OTP Systay Memu Memu, D., PASSWORD, CIRCO, VPN, BIO, CITP Launch Dicos VPN with FIDO (Bio) Using Slent OTP Systay Memu Memu, D., PASSWORD, CIRCO, VPN, LBO, CITP Launch Dicos VPN with FIDO (Bio) Using Slent OTP Systay Memu Memu, D., PASSWORD, CIRCO, VPN, LBO, CITP Launch Dicos VPN with FIDO (Bio) Using Slent OTP Systay Memu Memu, D., PASSWORD, CIRCO, CIRCO, CIRC, CIRCO, CIRC, CIRCO, CIRC, CIRCO, CIRC	Systray Menu	Using Silent OTP	min Bypass Token	th SDO Authenticator/Ad	sunch Cisco VPN w	L	SDO_BIO_OTP	ASSWORD_CISCO_!	Menu_ID_P
Mem.LD, ASSIVICRD, CIRCO, VPR.LBIO Laurch Circo VPN with FDO (Bio) Systey Menu Mem.LD, ASSIVICRD, CIRCO, VPR.LBIO, CIRCO Laurch Circo VPN with FDO (Bio) Using Silent OTP Systey Menu Mem.LD, ASSIVICRD, CIRCO, VPR.LBIO, CIRCO Laurch Circo VPN with FDO (Bio) Using Silent OTP Systey Menu Mem.LD, ASSIVICRD, CIRCO, VPR.LBIO, CIRCO Laurch Circo VPN with Certificate Systey Menu Mem.LD, ASSIVICRD, CIRCO, VPR.LBIO Laurch Circo VPN with SOC Alditericator Systey Menu Mem.LD, ASSIVICRD, EXPRED Check Credential Status Systey Menu Mem.LD, ASSIVICRD, FIDO Refereive Passavord with FDO (Pin) Systey Menu	Systray Menu			th FIDO (Pin)	aunch Cisco VPN w	L	/PN	ASSWORD_CISCO_	Menu_ID_P
Memu, D., ASSWORD, CISCO, VPN, LBIO, OTP Launch Gloso VPN with FDO (BIO) Using Slient OTP Systey Menu Memu, D., ASSWORD, CISCO, VPN, LBIO, OTP Launch Gloso VPN, with SDO (BIO) Using Slient OTP Systey Menu Memu, D., PASSWORD, CISCO, VPN, LBIO, OTP Launch Gloso VPN, with SDO Authenticator Systey Menu Memu, D., PASSWORD, CISCO, VPN, LSOO Launch Cisco VPN, with SDO Authenticator Systey Menu Memu, D., PASSWORD, CISCO, VPN, LSOO Check Credential Status Systey Menu Memu, D., PASSWORD, FIDO Refereve Password with FDO (Pin) Systey Menu	Systray Menu			th FIDO (Bio)	unch Cisco VPN w	L	/PN_8I0	ASSWORD_CISCO_1	Menu_ID_P
Mem. JD, ASSWORD, CISCO, VPN. CERT Launch Cisco VPN with Certificate Systay Mem Mem. JD, ASSWORD, CISCO, VPN. SCO Launch Cisco VPN with SOG Authencistor Systay Mem Mem. JD, ASSWORD, EXPRED Check Credential Status Systay Mem Mem. JD, ASSWORD, FIDO Retrieve Password with FDO (PP) Systay Mem	Systray Menu		OTP.	ith FIDO (Bio) Using Silent	aunch Cisco VPN w	L	PN_8IO_0TP	ASSWORD_CISCO_	Menu_ID_P
Memu, ID, PASSWORD, CISCO, VPM, SDO Launch Gisco VPN with SDO Authentication Systary Menu Memu, ID, PASSWORD, EXPIRED Check Credential Status Systary Memu Memu, ID, PASSWORD, FJDD Refrieve Tassword with FIDO (Pin) Systary Memu	Systray Menu			th Certificate	aurich Ciscó VPN w	L	/PN_CERT	ASSWORD_CISCO_)	Menu_ID_P
Menu_ID_PASSWORD_EXPIRED Check Credential Status Systray Menu Menu_ID_PASSWORD_FIDO Retrieve Password with FIDO (Pin) Systray Menu	Systray Menu			th SDO Authenticator	aunch Cisco VPN w	L	/PN_SDO	ASSWORD_CISCO_1	Menu_ID_P
Menu_ID_PASSWORD_FID0 Retrieve Password with FID0 (Pin) Systray Menu	Systray Menu			tus	neck Credential Sta	C	>	ASSWORD_EXPIRE	Menu_ID_P
	Systray Menu			th FIDO (Pin)	etrieve Password w	B		ASSWORD_FID0	Menu_ID_P
Menu_ID_PASSWORD_FID0_BIO Retrieve Password with FID0 (Bio) Systray Menu	Systray Menu			ith FIDO (Bio)	strieve Password w	R	0	ASSWORD_FIDO_BI	Menu_ID_P
Menii ID PASSWORD FILO VPM Betrieve Lonin Token with FILO (Pin) System Menii	Custrau Marsu			with EIDO (Pin)	etrieve Looin Token	9	2NI.	ASSWORD FIDD 18	Manu ID P.

- 21. Click Next.
- 22. 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.

arameters	Settings	MFA	Advanced	SysTray	Menu/Messages	CredUI	Errors
CredUI Sett	ings						
Bypass Al	1						
Bypass R	un as Administrator						
🗌 Bypass U	NC						
Bypass R	un as Other User						
🗌 Bypass W	ebAuthN						
Bypass Ri	DP						
Bypass C	ertificate PIN						

- 23. Click Next.
- 24. 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.

Errors Cad Terror for Control (Deformation Card Terror (Deformation Card Terror) Cad Terrors Card Terror Card Card Cad Cad Cad Cad Cad Cad Cad Cad Cad Ca	
Lines Parstinough 3rd Party Plagn Eren Messages Code Parstinough 3rd Party Plagn Party Plagn Parstinough 3rd Party Plagn Parstinou	
Asstruction to Carlo (Optional) Code Metage Load from CoV (Optional) Code Metage	
Laad fram CBY (piptonel) Code Code Code Code Code Code Code Cod	
Voter since transported Votes Vote Votes	
Code Message 1000 Internal case Internal case Internal case 1001 Internal case Internal case Internal case 1002 Interprise Connect Passacodies & Executedry syna later or contact you administration (firm 1002, impre Report Passacodies & Later Passacodies & L	
Internal cale Interpret Connect Passendersis: We cannot verify your identity. Please contact your administrator (timor 1005: there in not valid) Interpret Connect Passendersis: System more, Please by years later or contact your administrator. (timor 1005: there it more) Interpret Connect Passendersis: System more, Please by years later or contact your administrator. (timor 1005: there it more) Interpret Connect Passendersis: Authoritocoln hale Please by open later or contact your administrator. (timor 1005: there Please there and there administrator.) Interpret Connect Pleasendersis: Authoritocoln hale Please by open later or contact your administrator. (timor 1006: Sincer Please there administrator.) Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. (timor 1006: Sincer Please there administrator.) Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. (timor 1006: Contact your administrator.) Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. (timor 1006: Contact your administrator.) Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. (timor 1006: Contact your administrator.) Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. Interpret Connect Pleasendersis: Authoritocoln hale Please or contact your administrator. Intere Difference Connect Pleasendersis: Authoritocoln hal	
Ioin Deterging Connect Passicolds Silve cannot verify your administration. (Item 1001: Token in not valid). ID02 Enterging Connect Passicolds Silve cannot verify your administration. (Item 1002: Testing Fassicolds Silver Connect Your Administration. (Item 1002: Testing Fassicolds Silver Connect Your Administration. (Item 1002: Testing Fassicolds Silver Connect Your Administration. (Item 1002: Testing Fassicolds Silver Administration.) ID04 Enterging Connect Passicolds Silver Administration. (Item 1002: Testing Connect Your Administration.) ID05 Enterging Connect Passicolds Authentication Islee Passes on testing your administration. (Item 1002: Testing Connect Passicolds Authentication Islee Passes on testing your administration.) ID05 Enterging Connect Passicolds Authentication Islee Passes on testing your administration. (Item 1002: Testing Connect Passicolds Authentication Islee Passes your administration.) ID06 Enterging Connect Passicolds Authentication Islee Passes on testing your administration. (Item 1002: Testing Connect Passicolds Authentication Islee Passes on testing your administration.) ID05 Enterging Connect Passicolds Authentication Islee Passes on testing your administration.) ID06 Enterging Connect Passicolds Authentication Islee Passes on testing your administration.) ID07 Enterging Connect Passicolds Authentication Islee Passes on testing your administration on your mole (Item 1010). Enterging Connect Passicolds Authentication Islee Passes on testing your administration (Item 1010). ID08 <	
1002 Enterprise Correct Passesodies: Signet more: Passes try spaniliser or contract your administrator, fitting 1002, string fitting 1000, string 10000, string 1000, string	
103 Enterprise Correct Passionalises. We cannot well by and entity. Please contact your administration (Enter 100): Entertrate Enterprise Correct Passionalises. Authentication Intello Passes yang and litter or contact your administration (Enter 100): Entertrate Enterprise Correct Passionalises. Authentication Intello Passes yang and litter or contact your administration (Enter 100): Entertrate Enterprise Correct Passionalises. Authentication Intello Passes yang and litter or contact your administration (Enter 100): Entertrate Enter Passionalises. Authentication Intello Passes yang and litter your 2016 (Enter 100): Entertrate Correct Passionalises. Authentication Intello Passes ontact your administration (Enter 100): Entertrate Correct Passionalises. Authentication Intello Passes ontact your administration (Enter 100): Entertrate Correct Passionalises. Authentication Intello Passes ontact your administration (Enter 100): Entertrate Correct Passionalises. Authentication Intello Passes ontact your administration (Enter 100): Entertrate Correct Passionalises. Authentication Intello Passes and the ontact your administration (Enter 100): Entertrate Correct Passes administrate (Enter 100): Entertrate Correct Passionalises. Authentication Intello Passes administrate (Enter 100): Entertrate Passes ontact your administrate (Enter 100): Entertrate Intello Passionalises. Authentication Intello Passes administrate (Enter 100): Entertrate Intello Passionalises. Authentication Intello Passes administrate (Enter 100): Entert Passionalises. Authentication Intello Passes administrate (Enter 100): Entert Passes administrate (Enter 100):	
1014 Prespire Correct Passendess Aufbertoston failed Passes by again later or context-jou administrator. (from 1004. Sime Repet request) 1016 Prespire Correct Passendess. Aufbertoston failed Passes by again later or context-jou administrator. (from 1004. Sime Repet request) 1017 Prespire Correct Passendess. Aufbertoston failed Passes or taxis 1018 Prespire Correct Passendess. Aufbertoston failed Passes or taxis 1018 Prespire Correct Passendess. Aufbertoston failed Passes or taxis 1018 Prespire Correct Passendess. Passes entry faile Batecht en enfolded in you anche end on Windexs and them to again. (If the pressing pressing, use adherent aufbertoston) 1019 Detempsi Correct Passendess. Passes entry faile Batecht en enfolded on you mobile end on Windexs and them to again. (If the pressing pressing, use adherent aufbertoston) 1019 Detempsi Correct Passendess. Passes entry faile Batecht en enfolded on you mobile end on Windexs and them to again. (If the pressing pressing, use adherent aufbertoston) 1019 Detempsi Correct Passendess. Passes entry faile Batecht en enfolded on you mobile end on Windexs and them to again. (If the pressing correct Passendess. Passes)	
105 Tempsing Connect Passing Saudhardson Ingelde Seauwe Ordentialia en missing (Error 1005 Enrogic Connectina) 106 Enterpsing Connect Passing Saudhardson Inale Passes contact you administration (Error 1006 Registry end) 107 Enterpsing Connect Passing Saudhardson Inale Passes contact you administration (Error 1006 Enterpsing Connect you administration (Error 1006 Enterpsing Connect you administration (Error 1007 Enteror))	
1056 Enterprise Connect Passandos Authentication Islatel Paese contract your administrator (Enter 100: Registry emor) 1057 Enterprise Connect Passandos Authentication Islatel Paese contract your administrator (Enter 100: Registry emor) 1058 Enterprise Connect Passandos Manhameter emole paes you are connected to the interret. If the potelem parisits, contract your administrator (Enter 100) 1059 Enterprise Connect Passandos Authentication Islatel Paese contract you administrator (Enter 100) application administrator (Enter 100) 1059 Enterprise Connect Passandos Paese maise una you are contracted to the interret. If the potelem parisits, use a different authentication 1010 Enterprise Connect Passandos Authentication Islatel Try again and agroup authentication on your mobile (Enter 1010) as Elicited request) 1011 Enterprise Connect Passandos Authentication Islatel Try again and agroup authentication on your mobile (Enter 1010) as Elicited request)	
1007 Entropios Correct Passionadas: Authentication Intella Passes contact you administrativ (timri 1007: net centinges timm) 1008 Enterpios Correct Passionadas: Automicitation (timri net Passes and equip usa contracted to territeris): if or explorements, ortized you administrativ (timri 1007: net) 1009 Enterpios Correct Passionadas: Automicitation (timri net) 1000 Enterpios Correct Passionadas 1000 Enterpios 1000 Enterpios 1000 Enterpios 1000 Enterpios	
1008 Entropies Connect Passuodies. Network emp: Passe make sure you are connected to the internet. If the pottem pensis, constrainty our administrator (Emp 1008). Networks 1009 Entropies Connect Passuodies. National with the Bluetkon is enabled on you make and on Worksu, and the pottem passis, use all different authenticats 1010 Entropies Connect Passuodies. Nationation is the postem passe and provide and on Worksu, and postem to the postem passis, use all different authenticats 1011 Entropies Connect Passuodies. Nationation of the postem passis and approximation on you mobile (Emp 1018). BLIC Postem passis 1011 Entropies Connect Passuodies. Nationation of the postem passis and approximation on you mobile (Emp 1018). BLIC Postem passis	
1009 Enterprise Connect Passwordless. Please writy that Eluization is entible do your mobile and on Windows, and then by again. If the problem presists, use a different authenticats 1010 Enterprise Connect Passwordless. Authentication failed Try again and approve authentication on your mobile (Error 1010 BLE Client Reject request) 1011 Enterprise Connect Passwordless. Authentication failed Try again and approve authentication on your mobile (Error 1010 BLE Client Reject request)	or)
1010 Enterprise Connect Passurotless. Authentication failed: Try again and approve authentication on your mobile (Emr 1010. BLE Client Repet request) 1011 Enterprise Connect Passurotless. Authentication failed: Try again and approve authentication on your mobile (Emr 1011. Use Denied request)	on method. (Error 1009: BLE Em
1011 Enterprise Connect Passwordless: Authentication failed. Try again and approve authentication on your mobile (Error 1011) User Denied request)	
1012 Enterprise Connect Passwordless: Authentication bypass denied. Try again with a username and password. (Error 1012. User Bypass not allowed)	
1013 Internal use	
1014 internal use	
1015 Enterprise connect rasswordess: ettor intrangical creativities, invisionent and creativities round	
1016 Enterprise Connect Passwordest: Authentication raise: Pease check your Fluo token and try again (Enter 1016 Fluoz Enter)	
1017 Enterprise Contract, Passwordesa, Fold carried on its worksatton with a parsword, Enter 1017, User harre yeasword enter)	
1016 Enterprise Contract Hassivorcense Austerincetorin salve Prese enter your nucl Austerincetor Hink (Enter 1016 Pri Hequites) 2020 Enterprise Contract Hospitalitation Enter Relate enter your nucl Austerincetorin (Enter 1010 Related in Austerin	
1019 Enterprise Control - Passworkers Automation and Press by again. (Chie 1019, 111600, no response) 1000 Enterprise Control - Data and Enterprise Data and Enterprise (2000, 2011)	
Control of the pre-control of assumptions and accessing that index code of the second and takened (fine 1991) (for these of allowed) Control of the second accessing the second accessing the second accessing (fine 1991) (for these of allowed)	
Deep te contect asservates, mai enclanar rypes te tec, in yigen mini ademante enclassanda (una rozi), dee opesa na enveroi	
1023 Determine Connect Dissuprises 4 are time password cannot be used for passwordies authentication (Pror 1023 OTP passwordies is not allowed)	
1073 Enterraise Connect Descurvinges: Viv a non-time nessured excised. Plasta authenticiste online and renew unix OTD trian (Entry 1024 OTD excised)	
Even to Elia	
and the second se	
Destone Default List	

25. At the bottom of the **Errors** 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. (In the example below, the name is **Monitor Prefix**.)

Verification messages are displayed upon creation of each of these files. Click **OK** to close the popups.



Note

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.

r. Plea		√ f th	e proble
that E		^ ws	, and th
n fail		no	bile.(Err
n fail	Failure : Certificate format error :	no	bile.(Err
n byp		/or	d. (Erro
	OK		

MSI deployment

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 Octopus Desk For Windows 64bit.msi
- 2. Run Octopus Authentication for windowsxx.msi /qn:

C:\> Octopus Desk For Windows 64bit – xx_xxx_xx.msi /qn

Administrator: Command Prompt

:\Users\administrator>msiexec -i "C:\Octopus Desk For Windows 64bit - 2021-04-11_171214718.msi" _

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 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 Octopus Desk For Windows 64bit.msi
- 4. Run Octopus Authentication for windowsxx.msi /qn:

C:\> Octopus Desk For Windows 64bit - xx_xxx_xx.msi /qn

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 \checkmark .

😑 🐇 Enterpr	ise Connect Passwordless			PUBLISH	۵	=
System Settings	Directories All Directories and Agents in the System. Agents ar	e used to support remote d	directories.			
Manage Users	CREATE DIRECTORY			Search		۹
Devices Services	AD - sync: false Active Directory	:	AD - sync: true Active Directory May 12, 2023, 9:00:00 PM		:	
Portal Auditing	ORACLE - sync: false Oracle/Open LDAP	1	ORACLE - sync: true Oracle/Open LDAP O		:	

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

🗅 AD - sy	nc: true : 🔹	Active Directory	🗘 🛛 Jun 10, 2022, 4	4:00:00 PM		
Details	Domain Controllers	Links	Authenticators	Policy	Groups	
PASSWORD SET	TINGS					
Password-Free	Experience					
Password Lengl	th		Password Ag	e (0-1 year)		
		8 Chars	20	DAYS		~
Special Chars			Alphanumeri	C		

Then, go to Step 5 (below).

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

PASSWORD SETTINGS			
Password-Free Experience			
Password Length	— 8 Chars	Password Age (0-1 year) *	
Special Chars	-	Alphanumeric	•

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

5. At the bottom of the **Policy** tab, 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.



Enabling FIDO BIO user bypass

FIDO BIO 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.

AUTHENTICAT	DR
BYPASS USE	R 🔻
	CE BYPASS
SAVE	BYPASS with Temporary Token

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

🐣 Amit L	: AD -	sync: true/com,	qa		
Personal	Security	Authenticators	Devices	Services	Invitations
Status • Active (By	pass) Ma	Enrolled At y 20, 2021, 12:07:17 PM	La: May 20, 2	st Activity 2021, 5:44:32 PM	Bypass 59 minutes

- 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.

Active Directory Authentication				
General Info Parameters	Sign on	Director	ies	Users
Bypass Unassigned Users		Bypass Unenrol	led Users	
Sign on Method		Authentication	Token Timeout (1	minute - 1 year) *
Active Directory		1	WEEKS	-
Endpoint URL		Rest Payload Sig	jning Algorithm	
https:// p.com/adpa/303be3ce-641b	-448 🖺	SHA-256		•
Service Keys *		X.509 Certificat	e *	
Default	*	2022-05-11 1	1:42 SHA-256 20	048-bit 👻
VIEW	+ ADD	VIEW D	DOWNLOAD	

Configuring the MSIUpdater

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

• In the **Authenticators** sections of the **Parameters** tab, select both **FIDO2 (BIO)** and **ForgeRock Authenticator**.

_	
	Authenticators
	Octopus App
	Octopus BLE
	Hide Octopus BLE
	FID02
	FID02 (BI0)
	ForgeRock Authenticator
	Certificate Authenticator
	OTP
	SMS
	Email
	Voice Call
	Passphrase

• 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 Octopus Authenticator login option only. If there is no match, users are presented with the FIDO2 (BIO) and / or FIDO Bypass login options.

arameters	Settings	MFA	Advanced	SysTray	Menu/Messages	CredUI	Errors
Advanced	Settings						
🕑 Enable St	DO SSO			https://centos7	7i sm:8443/	login	
🛄 Change C	Octopus Name			Octopus Name			
Change OTP Name			OTP Name				
🗌 Change F	orgeRock Authentic	ator Name			ne		
Change SMS Name			SMS Name				
Change Email Name			Email Name				
Change Voice Call Name			Voice Call Name				
🔲 Change P	Passphrase Name			Passphrase Name			
Change Certificate Name		Certificate Name					
🗌 Enable Ci	P Bypass List			CP Bypass List			
🗹 Use Moni	itor Prefix			Monitor Prefix			
Change T	Trace Log Directory			Directory (For Exa	mple C:\WINDOWS\TEMP	0	

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.

🛓 Device Manager		
File Action View Help		
🗢 🏟 💷 🖾 🖾 💭	Generic PnP Monitor Properties	×
 Iaurentl-lap I Audio inputs and output 	General Driver Details Events	
Batteries Bluetooth	Generic PnP Monitor	
> 🖤 Cameras	Property	
 DellInstrumentation Disk drives 	Hardware Ids	~
Display adapters		
 Hirmware Human Interface Devices 	MONTORIDELDUCZ	
 Keyboards Memory technology dev 		
 Mice and other pointing Monitors 		
Generic PnP Monitor		
Generic PhP Monitor		
 Network adapters Ports (COM & LPT) 		
> 🖻 Print queues		
Processors Processors	ОК	Cancel

User authentication experience

When FIDO BIO 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.



Windows authentication methods

Once installation is completed, users will be able to authenticate to Windows machines using Octopus Authenticator, 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 Meth od	User Experience (On mobi le)	User Experience (Not on mobi le)
ForgeRock App	 Passwordless: Username + ForgeRock (Push) 	N/A
	 MFA: Username + Password + ForgeRock (Push) 	
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 Meth od	User Experience (On Mobi le)	User Experience (Not On Mobi le)
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)
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 Octopus Desk 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:

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.

System Properties	×
Computer Name Hardware Advanced System Protection Remote Remote Assistance	
Allow Remote Assistance connections to this computer	
What happens when I enable Remote Assistance?	
Advanced	
Remote Desktop	
O Don't allow remote connections to this computer	
 Allow remote connections to this computer 	
Low connections only from computers running Remote Desktop with Network Level Authentication (recommended)	
Help me choose Select Users	-
OK Cancel	Apply

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 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**.

			1	Derected and pintas	
ap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor				Bomovo
Authorization Manager	Microsoft Cor				Remove
Certificates	Microsoft Cor				
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				Maria Davia
Device Manager	Microsoft Cor		Add >		Move <u>D</u> own
Disk Management	Microsoft and		<u>a</u> ud >		
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor				
Local Users and Gro	Microsoft Cor	~			Advanced
		-	1	L	
ription					

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

Certificates snap-in	×
This snap-in will always manage certificates for: <u>My</u> user account <u>Service account</u> <u>Computer account</u> 	
< <u>B</u> ack <u>N</u> ext > Cancel	

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

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: (the computer this console is running on) Another computer: Another computer: Browse Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< <u>B</u> ack Finish Cance	9

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

Add or Remove Snap-ins				2	×	
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.						
Available snap-ins:				Selected snap-ins:		
Snap-in	Vendor	^		Console Root Edit Extensions		
ActiveX Control	Microsoft Cor			Certificates (Local Computer)		
Authorization Manager	Microsoft Cor			<u>R</u> emote		
Certificates	Microsoft Cor			Maria Ha		
Component Services	Microsoft Cor			Move <u>U</u> p		
Device Manager	Microsoft Cor			Move <u>D</u> own		
T Disk Management	Microsoft and		<u>A</u> dd >			
Event Viewer	Microsoft Cor					
Folder	Microsoft Cor					
IP Security Monitor	Microsoft Cor					
IP Security Policy M	Microsoft Cor					
Link to Web Address	Microsoft Cor				-	
Cocal Users and Gro	Microsoft Cor	۷		Ad <u>v</u> anced		
Description:						
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.						
				OK Cancel		

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

- 🔿 🖄 🛅 📋 🖓 🔒 🚺 📷					
Console Root V 💭 Certificates (Local Computer)	Issued To	Issued By AddTrust External CA Root	Expiration Dat ^ 5/30/2020	Actions Certificates	
	Affirm Trust Commercial Affirm Trust Commercial Certum CA Certum CA Certum CA Certum CA Common Commence Cyber Primary Certificat Common Common Commence Cyber Camera Common Common Common Common Commence Common Commo	Affim Trust Commercial Baltimore CyberTrust Root Certum CA Certum CA Contum Trusted Network CA Class 3 Public Primary Certificatio COMODO RSA Certification Auth Copyright (c) 1997 Microsoft Corp. DigiCert Hoyal Root CA DigiCert Global Root CA DigiCert Hong Assurance EV Root DST Root CA X3 Entrust Root Certification Authority Equifax Secure Certificate Authority Equifax Secure Certification Authority Equifax Secure Certification Authority	12/31/2030 5/13/2025 6/11/2027 12/31/2029 8/2/2028 1/19/2038 12/31/2029 11/10/2031 11/10/2031 11/10/2031 11/10/2031 11/10/2031 11/10/2031 9/30/2021 11/27/2026 12/7/2030 7/24/2029 8/22/2018 5/21/2022 7/17/2030 7/24/2029 8/22/2018 5/21/2022 7/17/2030 7/24/2029 8/22/2018 5/21/2022 7/17/2030 7/24/2029 8/22/2018 5/21/2022 7/17/2030 7/24/2029 8/22/2018 5/21/2022 7/17/2030 7/24/2029 8/22/2018 5/21/2029 8/22/2018 5/21/2029 8/2/20	More Actions	,

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).

		×
←	🐓 Certificate Import Wizard	
	File to Import	
	Specify the file you want to import.	
	File name:	
	Browse	
	Note: More than one certificate can be stored in a single file in the following formats:	
	Personal Information Exchange- PKCS #12 (.PFX,.P12)	
	Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	
	Microsoft Serialized Certificate Store (.SST)	
	Next Cance	el 🛛

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 Octopus Authentication CP post-installation

Enterprise Connect Passwordless 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 Enterprise Connect Passwordless 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\Authenticatio
n
\Credential Provider Filters\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SD0CredentialProvider"
"Disabled"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticatio
n
\Credential Providers\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SD0CredentialProvider"
"Disabled"=dword:0000001
```

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

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authenticatio
n
\Credential Provider Filters\{a95d85be-778f-4ed1-9ded-9f62ecc8a744}]
@="SD0CredentialProvider"
"Disabled"=dword:0000000
```

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

@="SDOCredentialProvider"
"Disabled"=dword:0000000

Appendix D: Troubleshooting

This section provides guidance for issues that you may encounter when working with Enterprise Connect Passwordless for Windows.

Launching the check point VPN from 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:

Registry Editor			
Computer\HKEY_LOCAL_MACHIN	P E\SOFTWARE\SecretDoubleOctopus\SYSTRAY		
Computer\HKEY_LOCAL_MACHIN BCD0000000 HARDWARE SAM SSCURITY SOFTWARE Classes Clients Classes Clients CVSM DefaultUserEnvironmen Sogle Intel Microsoft Mozilla mozilla.org ODBC ODBC ODBC Partner	SOFTWARE\SecretDoubleOctopus\SYSTRAY Name CheckPoint VPN FIDO2 CheckPoint VPN FIDO2 CheckPoint VPN Server CheckPoint VPN Server Cisco VPN FIDO2 Cisco VPN FIDO2 Cisco VPN SDO Cisco VPN SDO Cisco VPN SDO Cisco VPN SDO OTP CisCO VP	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x00000000 (0) 0x00000000 (0) 0x0000000 (1) office, C:\Program Files (x86)\CheckPoint\Endpoin 0 0x00000000 (0) 0x00000000 (0)
> Policies RegisteredApplications	aunch sso portal fido use fido vpn	REG_DWORD REG_DWORD	0x00000000 (0) 0x00000000 (0)
CREDUI	🗱 use fidoBio	REG_DWORD	0x00000000 (0)

Endpoint Security Configuration

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



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**.

🕨 🔿 🙍 🔟 🖉 📷					
B Event Viewer (Local)	SecretDoubleOctopus Nur	nber of events: 358 (!) New events available			
Custom Views Windows Logs	Level	Date and Time	Source	Event ID	Task Category
Applications and Services Lo	(1) Information	03/11/2022 13:21:26	WCP	1000	(1)
Hardware Events	(1) Information	03/11/2022 13:20:14	WCP	1000	(1)
Internet Explorer	(1) Information	03/11/2022 13:19:17	WCP	1000	(1)
🗑 Key Management Service	(1) Information	02/11/2022 18:28:40	WCP	1000	(1)
> 🎽 Microsoft	(1) Information	02/11/2022 18:25:14	WCP	1000	(1)
Microsoft Office Alerts	(1) Information	02/11/2022 17:19:38	WCP	1000	(1)
> OpenSSH	Error	02/11/2022 17:15:42	WCP	1000	(1)
SecretDoubleOctopus	(1) Information	02/11/2022 17:11:48	WCP	1000	(1)
Windows PowerShell	(1) Information	02/11/2022 17:05:34	WCP	1000	(1)
Saved Logs	Event 1000 WCP				

Authentication Type, Status, Mode and SessionId are displayed for every authentication event. The SessionId provided is identical to the SessionId that appears in the Windows logs.

rvel	Date and Time	Source	Event ID	Task Category	
Information	27/11/2022 06:00:19	WCP	1000	Rest Events	
Information	27/11/2022 05:54:06	WCP	1000	Rest Events	
Information	27/11/2022 05:53:05	WCP	1000	Rest Events	
Information	27/11/2022 05:52:57	WCP	1000	Rest Events	
Information	27/11/2022 05:50:25	WCP	1000	Rest Events	
Information	27/11/2022 05:49:04	WCP	1000	Rest Events	
ent 1000, WCP					,
User: lebron Doma 24C3C089A91B	in: Authentication Type: Octopu	BLE <mark>Status</mark> Success Reason: C <mark>Mode</mark>	Offline SessionId: 29375EF	F-F751-47CA-881E-	7
General Details	in: Authentication Type Octopu	BLE <mark>Status</mark> Success Reason: Q <mark>Mode</mark>	Offlin <mark>e SessionId:</mark> 29375EF	F-F751-47CA-881E-	8
General Details	in: Authentication Type: Octopu SecretDoubleOctopus WCP Logaed:	BLE <mark>Status</mark> Success Reason: C <mark>Mode</mark>	Offline <mark> Session1d: 2</mark> 9375EF	F-F751-47CA-881E-	
General Details	sin: Authentication Type: Octopu: SecretDoubleOctopus WCP Logged: 1000 Task Cate	BLE <mark>Status:</mark> Success Reason: O <mark>Mode</mark> 27/11/2022 05:50:25 00Y: Rest Events	Offline SessionId: 29375EF	F-F751-47CA-881E-	
User: lebron Doma 24C3C089A918	in: Authentication Type Octopu SecretDoubleOctopus WCP Logged: 1000 Task Cate Information Kewwords	BLE Status Success Reason: (Mode 27/11/2022 05:50:25 079: Rest Events Classic	Offlind <u>Session(d:</u> 29375EF	F-F751-47CA-881E-	
User: lebron Dome 24C3C089A91B Log Name: Source: Event ID: Level: User:	Authentication Type Octopus SecretDoubleOctopus WCP Logged: 1000 Task Cate Information Keywords N/A Compute	BLE Status Success Reason: OMode 27/11/2022 05:50:25 1079: Rest Events Classic DESKT0P-050TVBP.casdo.com	Offlind Session1d: P9375EF	F-F751-47CA-881E-	
General Details User: lebron Dome 24C 3C 089A 91B Log Name: Source: Event ID: Level: User: OocCode:	Authentication Type: Octopus SecretDoubleOctopus WCP Logged: 1000 Task Cate; Information Keywords N/A Compute Info	BLE Status Success Reason: (Mode 27/11/2022 05:50:25 00y: Rest Events Classic : DESKTOP-05OTVBP.qasdo.com	Offlind <mark>Session1d:</mark> Þ9375EF	F-F751-47CA-881E-	

Error codes are provided as the Fail **Reason**. In the example below, the error code is **1004**.

SecretDoubleOctopus Number of events: 9					
Level	Date and Time	Source	Event ID	Task Category	^
Error	29/11/2022 3:40:24	WCP	1000	Rest Events	
(i) Information	29/11/2022 3:40:51	WCP	1000	Rest Events	
Information	29/11/2022 1:56:07	WCP	1000	Rest Events	
 Information 	29/11/2022 1:57:00	WCP	1000	Rest Events	
(i) Information	29/11/2022 3:41:15	WCP	1000	Rest Events	
 Information 	29/11/2022 3:58:05	WCP	1000	Rest Events	
(1) Information	29/11/2022 3:58:26	WCP	1000	Rest Events	*
Event 1000, WCP ×				×	
General Details					
User: lebron Domain	User: lebron Domain Authentication Type: OTP Status: Fai Reason: 1004 Aode: Online SessionId: C01618CB-8423-4F80-A676-5CFA6C176AAB				

The following table lists each error code and its corresponding message. 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. Please reach out to support@doubleoctopus.com for assistance with this download. Keep in mind that the process will require stopping the service.

Error Code	Technical Reason	Error Message
1001	TOKEN_NOT_VALID	Octopus Authentication: We cannot verify your identity.
1002	SERVER_ERROR	Octopus Authentication: System error. Please try again later or contact your administrator.
1003	CERT_ERROR	Octopus Authentication: We cannot verify your identity. Please contact your administrator.
1004	REJECT	Octopus Authentication: Authentication failed. Please try again later or contact your administrator.
1005	PASSWORD_EMPTY	Octopus Authentication: Authentication

		rejected because Credentials are missing.
1006	REG_ERROR	Octopus Authentication: Authentication failed. Please contact your administrator.
1007	GET_CERT_ERROR	Octopus Authentication: Authentication failed. Please contact your administrator.
1008	NETWORK_ERROR	Octopus Authentication: Network error. Please make sure you are connected to the internet. If the problem persists, contact your administrator.
1009	BLE_ERROR	Octopus Authentication: 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_REJECT	Octopus Authentication: Authentication failed. Try again and approve authentication on your mobile.
1011	DENY	Octopus Authentication: Authentication failed. Try again and approve authentication on your mobile.
1012	BYPASS	Octopus Authentication: Authentication bypass denied. Try again with a username and password.
1013	EXPIRED	
1014	NOEXPIRED	
1015	NO-OLD-PASSWORD-FOUND	Octopus Authentication: Error finding old credentials. Try again.
1016	FIDO2ERROR	Octopus Authentication: Authentication failed. Please check your FIDO token and try again.
1017	USER-NAME-PASS-NO- TALLOW	Octopus Authentication: You cannot log into this workstation with a username and password.
1018	FIDOERRPINREQUIRED	Octopus Authentication: Authentication failed. Please enter your FIDO Authenticator PIN.
1019	TIMEOUT	Octopus Authentication: Authentication failed. Please try again.
1020	CANTSETLOCALPASSWORD	Octopus Authentication: Set Local Credentials error.

1021	NOTFOUND	Octopus Authentication: Authentication bypass denied. Try again with a username and password.
1022	WEBAUTHN	Octopus Authentication: Authentication failed. Please try again.
1023	OTPNMFA	A one time password cannot be used for passwordless authentication.
1024	OTPOFFLINEENDOFBUFFER	Your one time password expired. Please authenticate online and renew your OTP token.
1026	AUTHTIMEOUT	Octopus Authentication: Authentication failed. Please try again.
1027	MFABYPASS	Octopus Authentication: MFA Bypass not allowed. Please try again.
1028	NOMEMORY	Octopus Authentication: Your computer needs more memory to run. Contact your administrator.
1029		Octopus Authentication: Can't decrypt credentials. (Error 1029: Credentials Decrypt Error)
1030	OTHER	Octopus Authentication: Oops, something went wrong. Please contact your administrator.
1031	OTP1MIN	Octopus Authentication: Your Computer is locked for 1 minute. Please try again later.
1032	OTP30MIN	Octopus Authentication: Your Computer is locked for 30 minutes. Please try again later.
1033	OTP1H	Octopus Authentication: Your Computer is locked for 1 hour. Please try again later.
1034	OTPBLOCKED	Octopus Authentication: Your Computer is locked. Please try again later.
1035	NOTSUPPORTED	Octopus Authentication: Reset Credentials is not set. Please contact your administrator.
1036	MUSTCHANGEPASSWORD	Octopus Authentication: Your Credentials are out of sync. Please contact your administrator.
1037	ACCOUNTLOCKEDOUT	Octopus Authentication: Your account is locked. Please contact your administrator.
1040	REJECTANDALLOWBLE	Octopus Authentication: Authentication failed. Please try again later or contact your

administrator.

Appendix E: Known issues

The following issue, discovered during software testing, will not be resolved in version 3.8.2:

• **Offline BLE fail following online strong authentication:** When Enforce Adaptive Authentication is enabled, users authenticating for the first time from a unrecognized workstation need to enter a verification code for successful login. Once this strong authentication has been done, they are then able to perform regular online and offline login from that device. However, currently offline authentication **via BLE** fails after an online strong authentication, and succeeds only following a second regular (without a verification code) online authentication.