Authlogics Windows Desktop Agent Integration Guide

For PSM and MFA

Product Version: 4.2.1030.0

Publication date: February 2023

Call us on: +44 1344 568 900 (UK/EMEA)
+1 408 706 2866 (US)

Email us: sales@authlogics.com

Table of Contents

Introduction

Integrating Authlogics Password Security Management (PSM) and Multi Factor Authentication (MFA) with Windows is an ideal way to deploy a modern password policy and add strong authentication to Windows desktops. The Windows Desktop Agent supports both online and offline logon functionality for Windows 10 & 11 and Windows Server 2016, 2019 & 2022 - so it can be used virtually anywhere.

Password Security Management

Password Change: The Windows Desktop Agent provides intuitive user feedback when they change their password to help them create a password which complies with the current password policy.

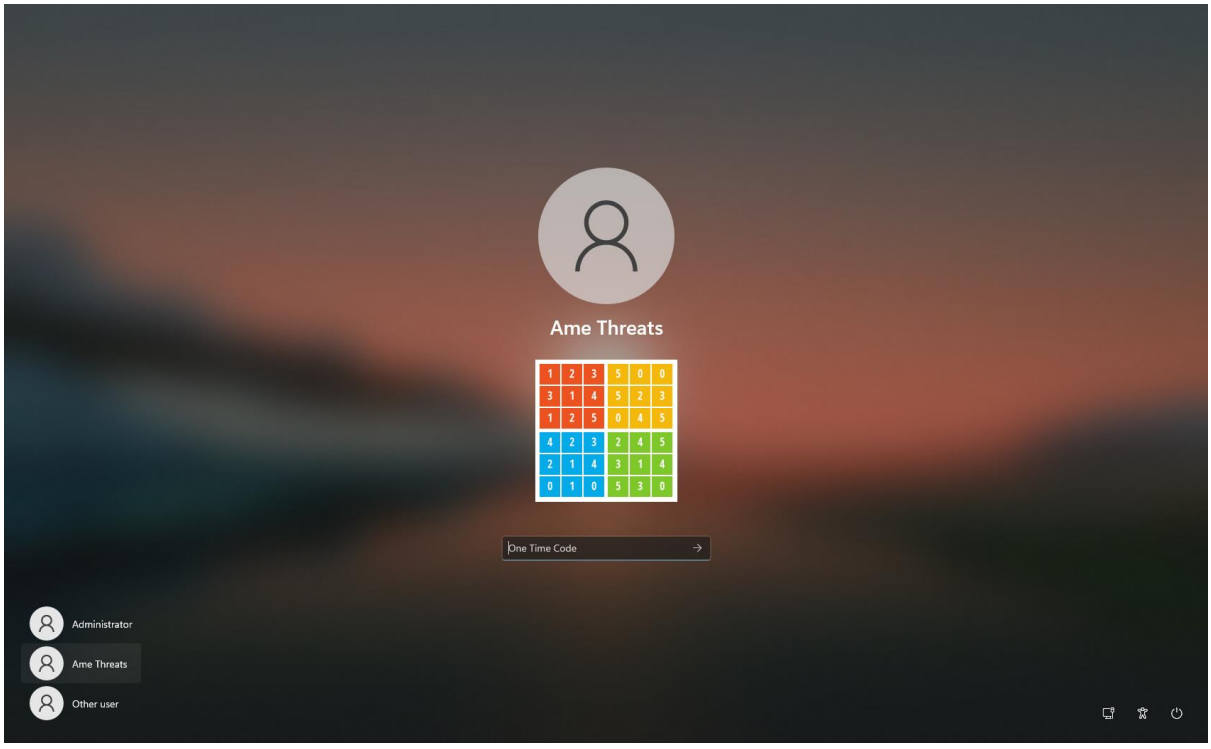
Self Service Reset: Users can click a "Forgot Password" link on the login screen which will send them a One Time Code via email/SMS to allow them to reset their password.

Multi Factor Authentication

The Windows Desktop Agent provides MFA and deviceless OTP logon capabilities to Windows as well as Self Service device management giving users the ability to add/remove MFA devices.

Deviceless and Passwordless login screen example

This example shows the Authlogics Windows Desktop Agent installed on a Windows 11 PC. Deviceless OTP and Passwordless logins have been enabled configured.



Passwordless MFA for Active Directory

Overview

The Authlogics Windows Desktop Agent allows users to logon to Windows with MFA without having to enter their Windows password. This form of passwordless logon is achieved by storing the users AD Password in a secure Password Vault which is retrieved and delivered to the Windows desktop on the user's behalf when logging on. Logging onto Windows in this way ensures compatibility with existing Windows applications that rely on Active Directory credentials. Passwordless logon is disabled by default and can be enabled by setting the "Enable Passwordless functionality to remove the Active Directory password for logon" group policy option on the Windows Desktop Agent.

The Offline Password Vault

Each PC with the Authlogics Windows Desktop Agent installed is able to work offline (if allowed via group policy). To cater for offline logons, a subset of the AD user account information is stored in an encrypted cache on the PC, this includes AD passwords to cater for offline passwordless logons.

The Offline Cache is similar to the Authlogics Authentication Server Password Vault in that it uses RSA 2048 bit asymmetric keys in a certificate to protect the data. Each Offline Cache uses a unique certificate installed in the Windows Certificate Store which is created during the agent installation; thus ensuring that no two Offline Cache databases use the same encryption keys.

The Authlogics Authentication Server Password Vault is disabled by default and must be enabled prior to use. When disabled, the Offline Cache will not store AD passwords however the remaining metadata is still protected in the same way.

The Offline Cache update process

For a Windows Desktop to receive an AD password for storage in the Offline Cache:

- The Windows machine must have a local certificate installed.
  - This can be restricted to a specified trusted root.
- The user must successfully authenticate to the server with MFA.

When a user is authenticated with the Authentication Server for passwordless logon, the public key in the certificate installed on the Windows Desktop is also sent to the Authentication Server. If the authentication request is successful the Authentication Server retrieves the password from the Authlogics Password Vault and decrypts it using its private key, then immediately re-encrypts the password using the supplied public key and returns it to the Windows Desktop. The Windows Desktop then verifies that it can decrypt the returned password using its private key and stores the password in its Offline Password Vault for later offline passwordless logon use.

This process ensures that:

- The password is never transmitted in cleartext.
  - Even when SSL is not used, the password is still protected.
- The password is always stored in the Vault using the correct key pairs.
- The password can only be decrypted on the machine that the user used to authenticate from.

Note

The offline cache is updated periodically for all user accounts stored in it, except for AD passwords which are only updated after a successful user online logon. This is similar to how Windows caches AD passwords for offline logon purposes.

The Domain Controller Agent

The Domain Controller Agent is a lightweight service designed to ensure that compliant passwords are set in Active Directory, as well as capture password changes made on the Windows Domain and store them securely in the Authlogics Authentication Server Password Vault. This keeps the AD password database and the Authlogics Authentication Server Password Vault in sync at all times regardless of what mechanism is used to change/reset an AD password.

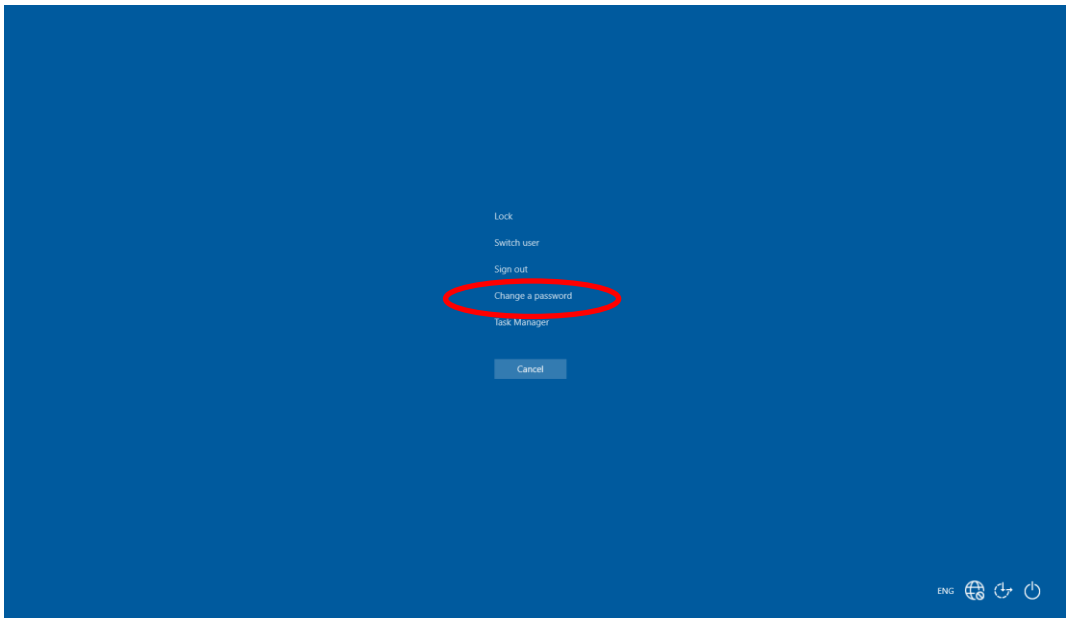
Note

The Domain Controller Agent MUST be installed on all domain controllers in the Active Directory domain when using passwordless logon.

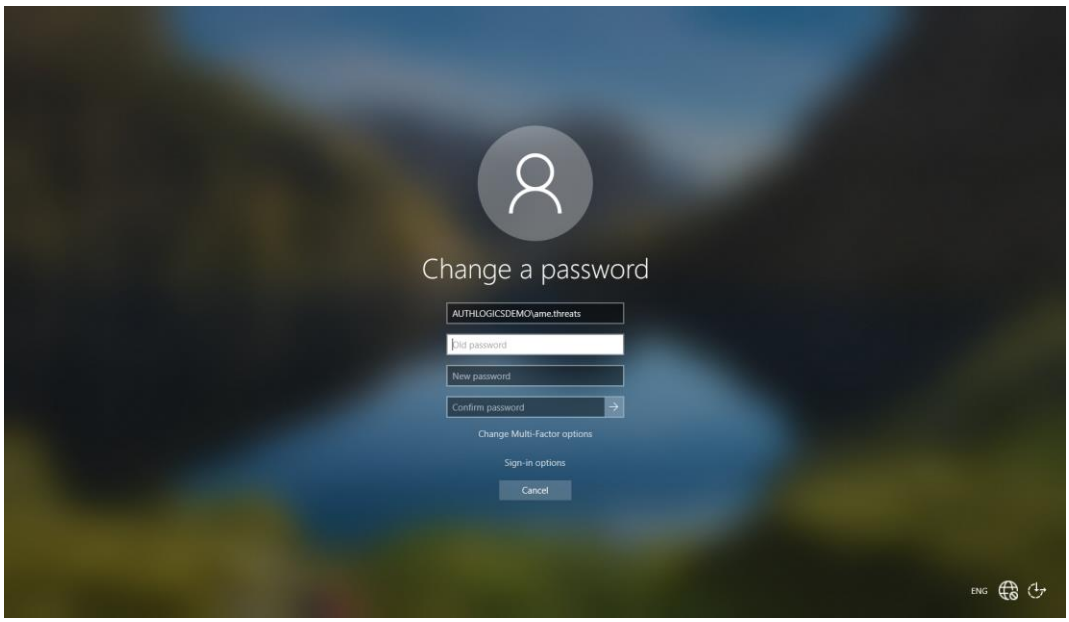
Changing an Active Directory Password

The Windows Desktop Agent allows users to manage (add, remove, enabled and disabled) their own MFA devices, similar to what can be done via the Authlogics Self Service Portal.

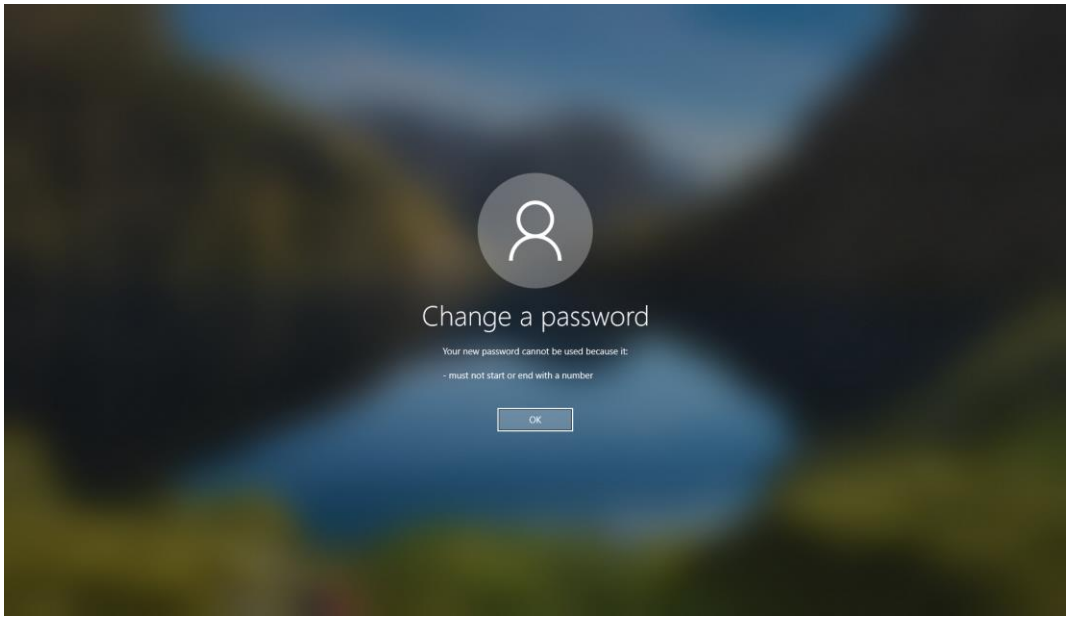
(1) Press CTRL + ALT + DEL to show the Windows security screen.

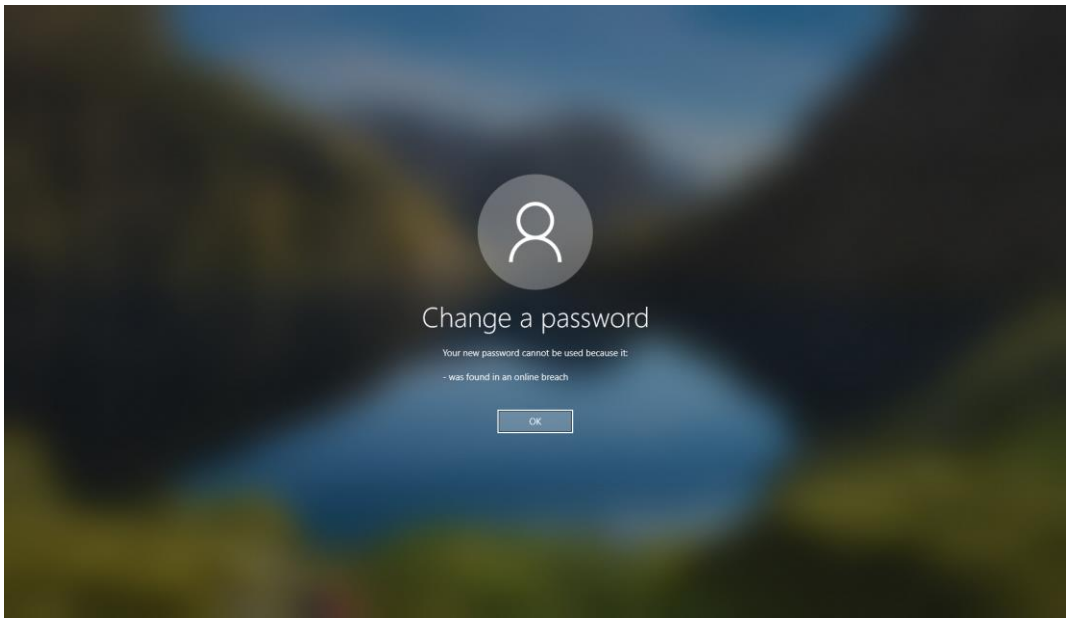


(2) Click *Change a password*.



(3) Enter the old password and enter the new password twice to confirm it.



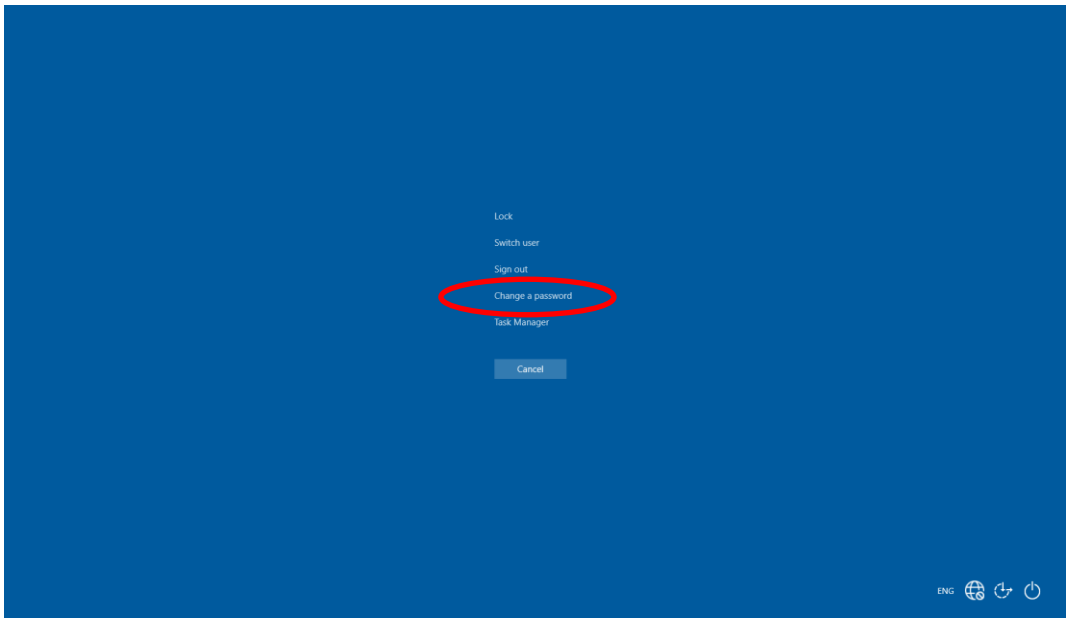


(4) If the new password does not comply with the policy the exact reason it failed will be displayed to the user instead of a generic error message. This helps the user choose a new valid password without having to call the helpdesk.

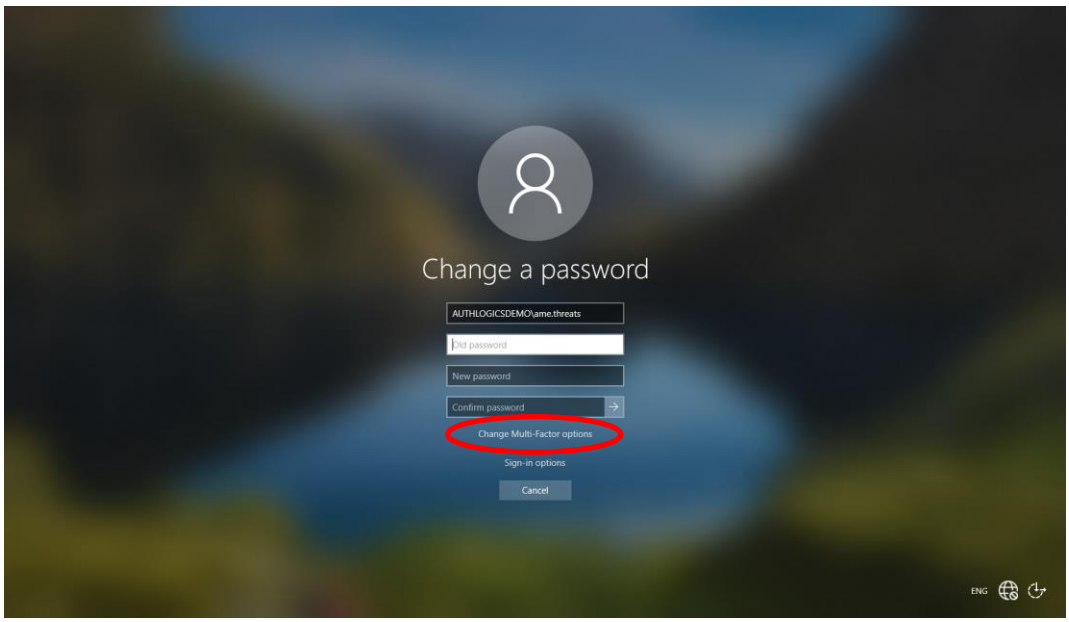
Managing Multi-Factor Options

The Windows Desktop Agent allows users to manage MFA knowledge factors, similar to what can be done via the Authlogics Self Service Portal.

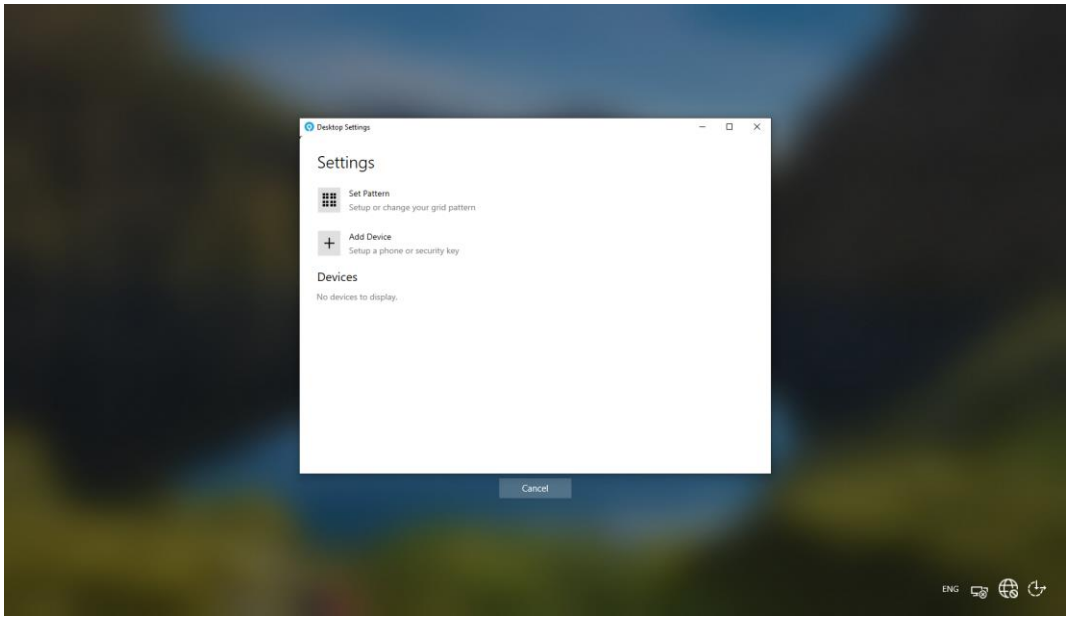
(1) Press CTRL + ALT + DEL to show the Windows security screen.



(2) Click *Change a password*.

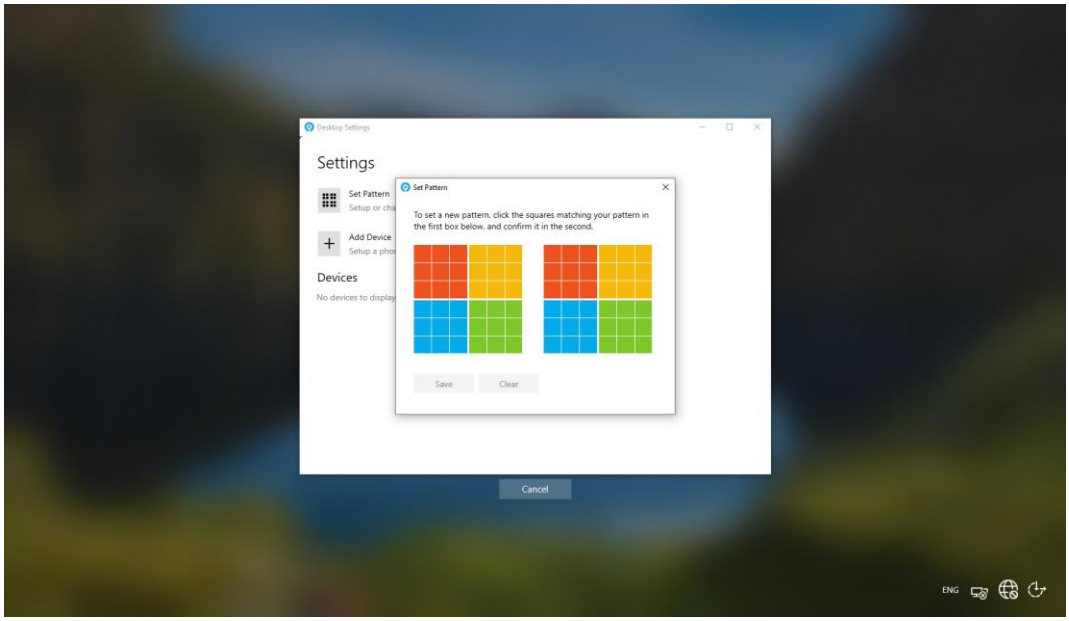


(3) Click *Change Multi-Factor options*.



Changing a PINgrid Pattern

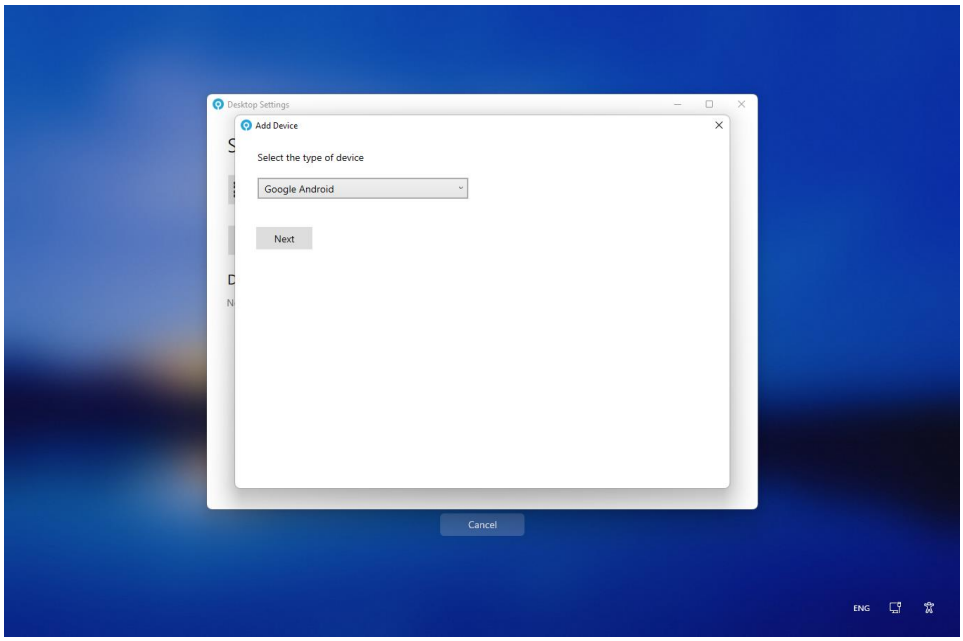
(1) Click *Set Pattern*.



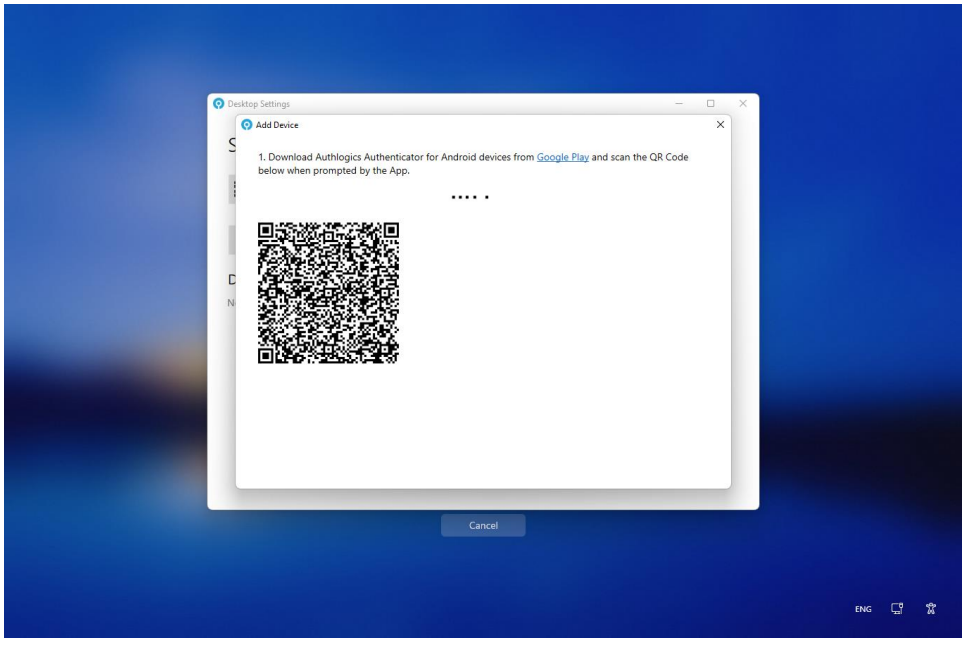
(2) Enter a new pattern by clicking on the desired squares. The same pattern must be entered on both grids to confirm it. Click *Save* when done.

Adding a new MFA Device

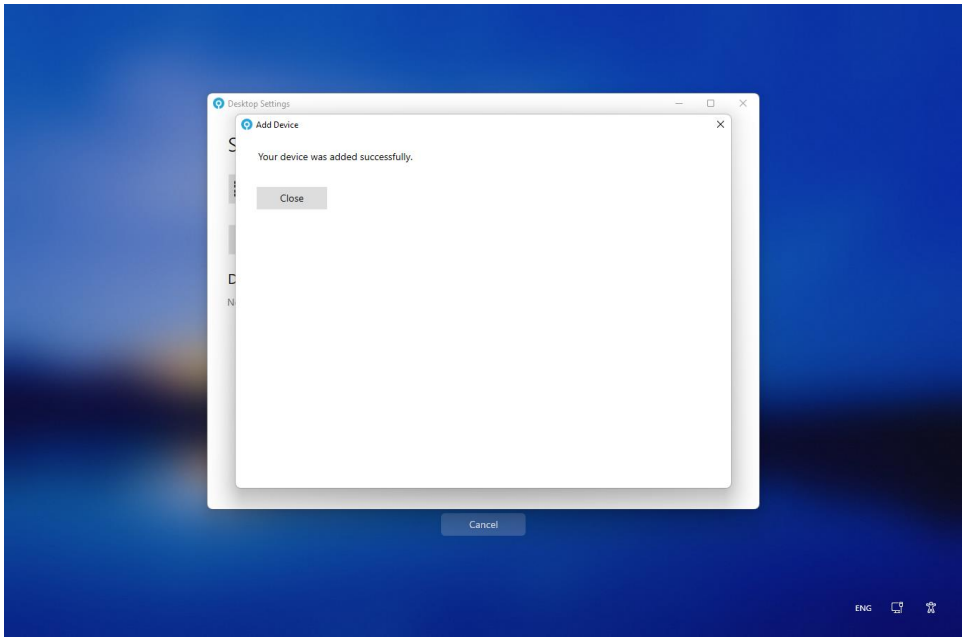
(1) Click *Add Device*.



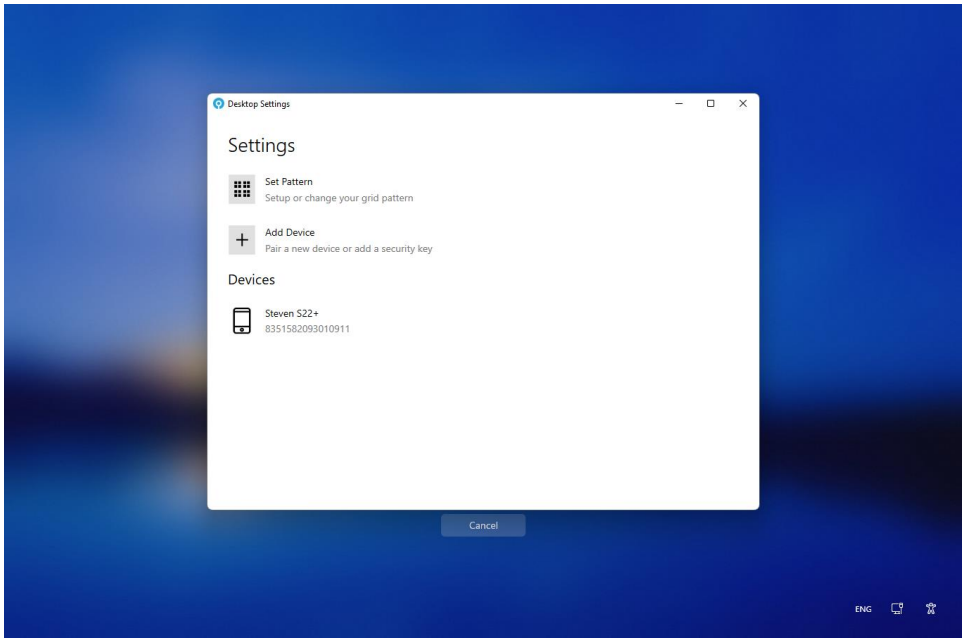
(2) Choose the device type and click *Next*.



(3) Scan the QR code with the Authlogics Authenticator App.



(4) Click *Close*.

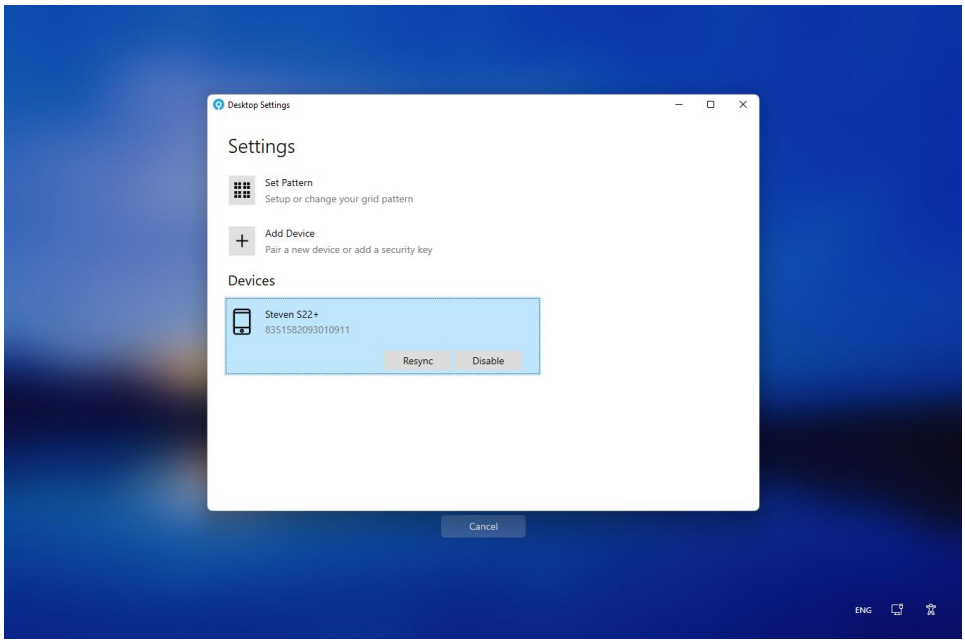


(5) The new device is shown in the *Devices* list.

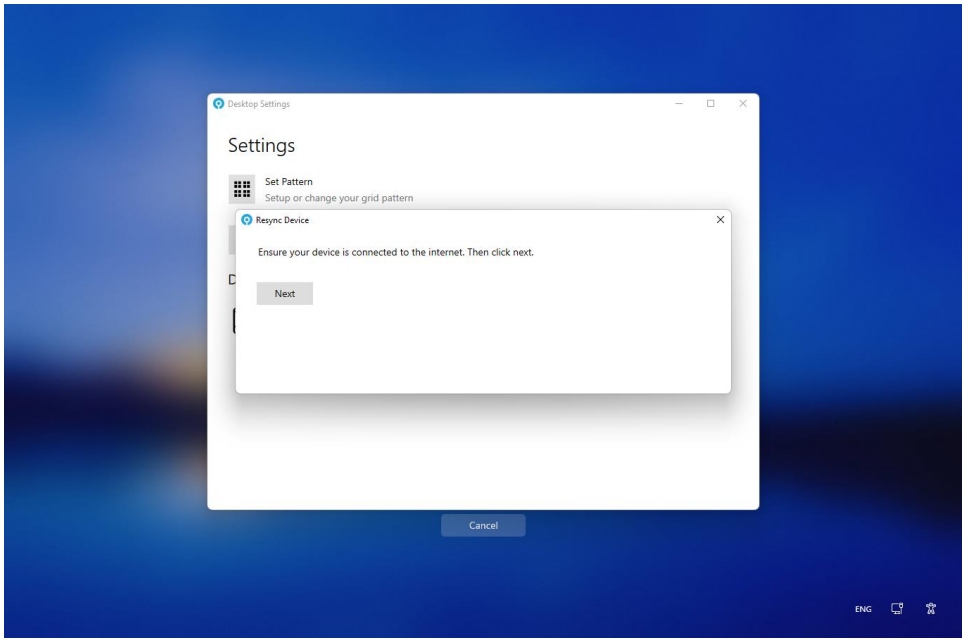
Resyncing a device

Authlogics Desktop Agent can resync an already paired device. This is useful if user account settings have change that affect the App, e.g. the user is provisioned for a new authentication factor.

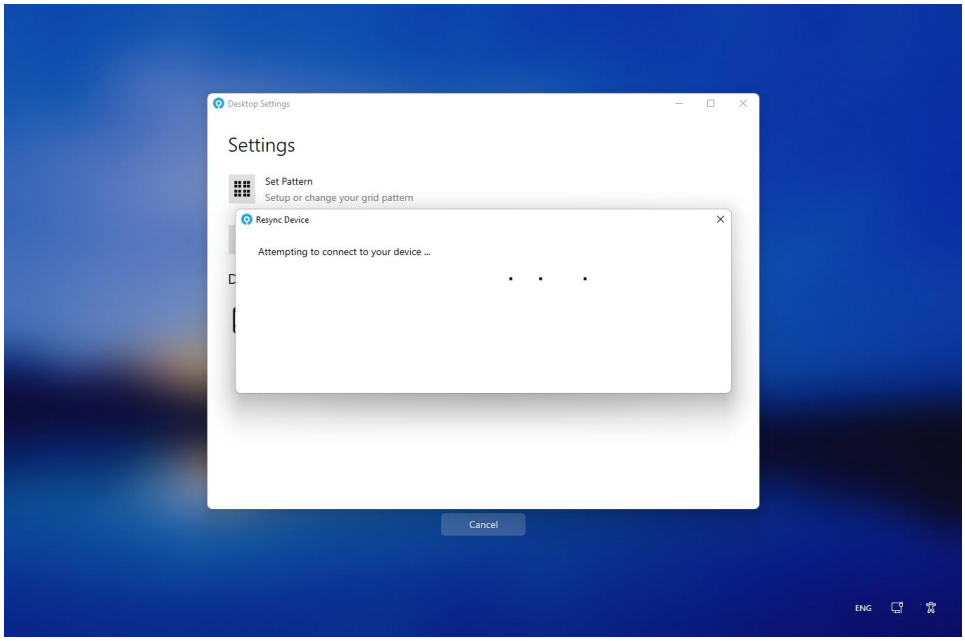
(1) Select the device to resync



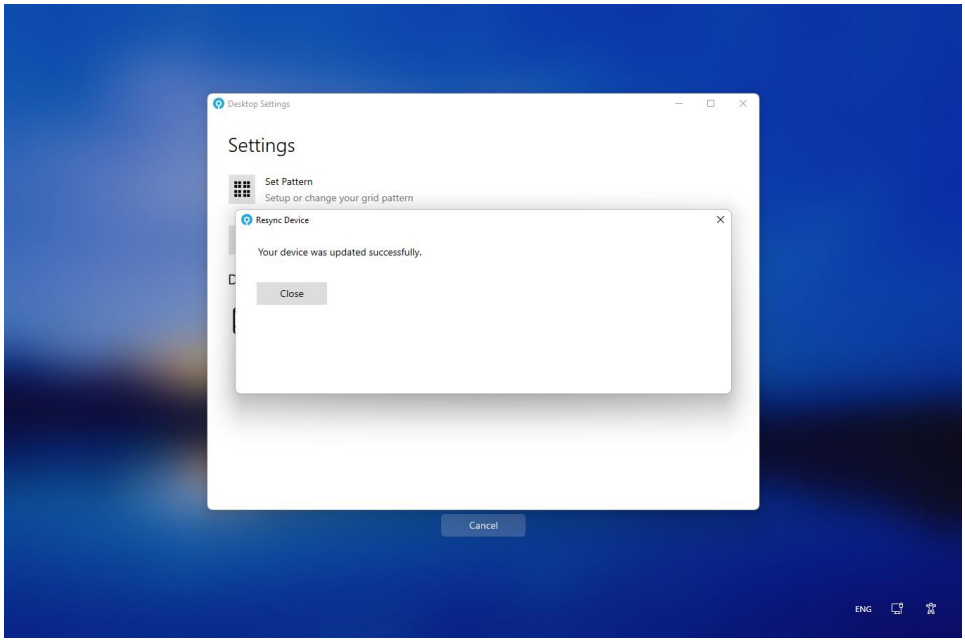
(2) Click *Resync*.



(3) Click *Next*.



(4) Check the Authenticator App for any steps required, e.g. biometric verification.

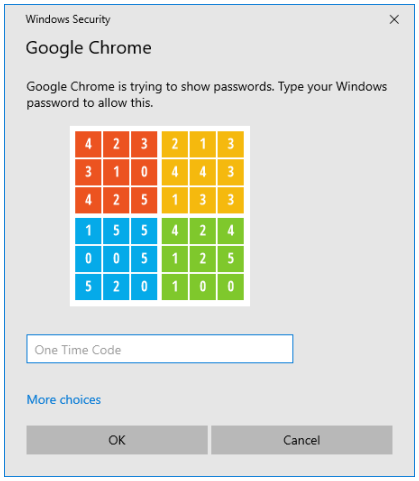


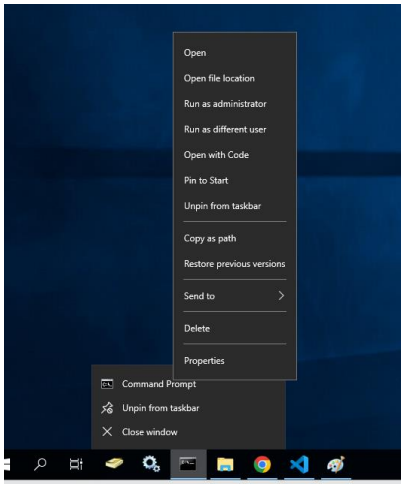
(5) Click *Close*.

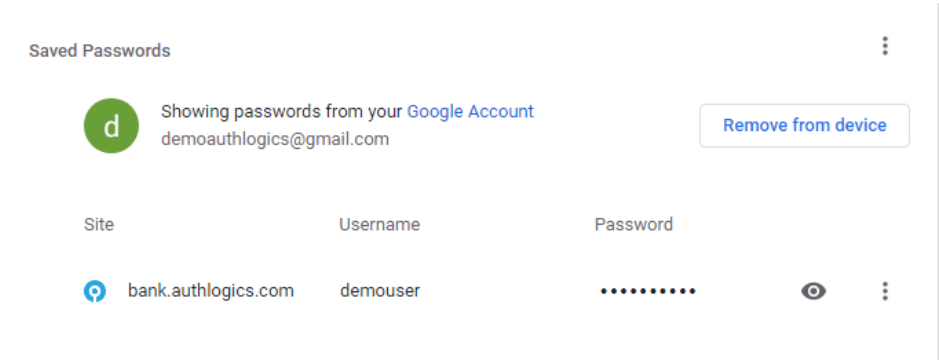
Using MFA for Windows Credential Prompting

Authlogics Desktop Agent can enforce MFA onto Windows credential prompting when operations such as ***Run as different user*** and ***Show password*** within Saved Passwords in a browser are initiated.

Authlogics MFA options for the Credential Prompting operations (Deviceless and Passwordless) are configurable via Group Policy and can be disabled by enabling the ***DisableMfaCredentialPrompting*** GPO.







Considerations

Requirements

An Authlogics Authentication Server 4.2.1030.0 or higher must be deployed and functional for all functionality to be available. The agent is backwards compatible with older Authentication Server versions but can only deliver the functionality applicable to the deployed server version. In addition, care should be taken to examine the various Active Directory Group Policy options to assist in planning for the deployment of the Windows Desktop Agent for both MFA and PSM.

Deviceless logon limitations with PINgrid on Server 2016

Deviceless logon with PINgrid is supported on Windows 10, Windows 11, Windows Server 2019 and Windows Server 2022 only, not Windows Server 2016. This is due to Microsoft limitations in the Windows Credential provider v2 which limits the ability to display the required grid graphic. This limitation does not apply to PINphrase deviceless logons. All other product features are supported on Server 2016.

Upgrades

Upgrading to version 4.2 is supported and existing cache data will be migrated. Upgrades are only supported from version 4.x.

When upgrading from Authentication Server version 4.x and Windows Desktop Agent version 4.x, you must upgrade the Windows Desktop Agent to version 4.2 first and then upgrade the Authlogics Authentication Server to version 4.2.1030.0 or higher. The Authlogics Windows Desktop Agent version 4.2 is backwards compatible with version 4.0 Authentication Servers.

Example starting point: Authentication Server 4.0 and Windows Desktop Agent 4.0

1. Deploy new Group Policy template for version 4.2.
2. Upgrade all Windows machines to Windows Desktop Agent 4.2.
3. Upgrade all Authentication Servers to version 4.2.1030.0 or higher (see separate Installation and Configuration Guide for this process)

Authlogics Windows Desktop Agents are backwards compatible with older Authentication Server versions, not the other way around. Thus, as a general rule, the Windows Desktop Agent should be upgraded before the Authentication Server.

Language Requirements

Authlogics Windows Desktop Agent is available in the following languages:

- English
- German

Additional languages may be provided for in the future.

Product support and documentation are only available in English.

Design and Deployment Scenarios

The Authlogics Windows Desktop Agent has been designed to work seamlessly in a Windows Workgroup and Active Directory environment.

The agent is contained in an MSI installation package which can be automated and deployed via Active Directory Group Policy or an alternative software deployment tool. The agent settings are controlled via Active Directory Group Policy for flexible, centralised management.

Deployment is as simple as configuring a GPO to target a machine and install the agent software. The agent will automatically and dynamically locate Authlogics Authentication Servers in the Active Directory forest to process logons.

When installed on a workgroup based machine the agent must be configured using the local machine policy.

Offline Logons

The Authlogics Windows Desktop Agent supports offline logon and Passwordless logon. This works very similarly to the password-based Windows offline logon functionality whereby user details are cached on the PC for future logons in cases where the authentication server is not available. The agent can even perform an MFA logon via a soft token while offline. Offline logon functionality is enabled by default and can be controlled / disabled via AD Group Policy. The offline cache is also used to accelerate the generation of Deviceless OTP challenges.

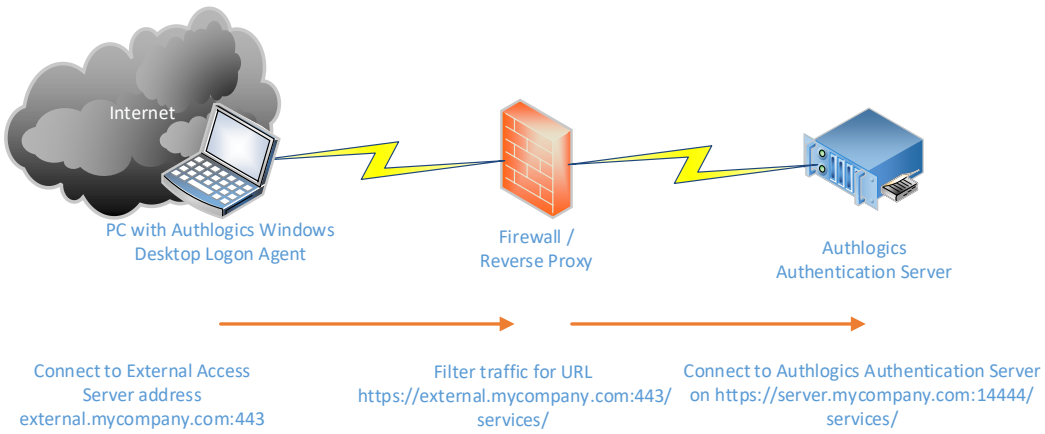
The Authlogics Windows Desktop Agent can use an “External Access Server” configuration when it needs to communicate with the Authlogics Authentication Server but isn’t on the internal network. This allows mobile PCs which are connected to the Internet but are not on the LAN to authenticate without working offline allowing the server to trigger the sending of Mobile Push and SMS/TEXT messages and caters for central auditing and logging.

External Access Server configuration

In this scenario, the agent must utilise a HTTPS connection to an External Access Server address. This facilitates central logging and also provides the ability to send SMS/Text message tokens to users while their PC is on the move.

The address of the External Access Server is configured on the PC via AD Group Policy. It is recommended to use a reverse proxy server or SSL capable firewall to allow external access to the External Access URL of the Authlogics Authentication Server.

The External Access Server role is an optional component on the Authlogics Authentication Server which runs on a dedicated port and IIS web site. It can be configured to use a different SSL certificate to the Self Service Portal if required.



Note

Authlogics Authentication Servers older than version 4.1.3200.0 uses port 14443 instead of the dedicated External Access Server role on port 14444.

Only require OTP when working remotely

The Authlogics Windows Desktop Agent can be configured automatically to disable itself when the PC is on the LAN thereby only requiring the user to enter an OTP when logging on remotely. This caters for remote access policies which require 2FA for remote connections but not for local connections.

To enable this functionality, configure the "Disable Windows Desktop Agent when on the LAN" group policy setting.

Workgroup based installations

The Authlogics Windows Desktop Agent supports installations on Workgroup (non-domain joined) systems. When doing so Active Directory is not available for deploying the policy to the machine or for detecting the Authlogics Authentication Server.

When installed on a Workgroup system, a local Authlogics Policy Editor is installed which allows for the configuration of the policy where at least the name of the Authlogics Authentication Server MUST be specified.

To enabled MFA for a local SAM based user account simply create a Realm on the Authlogics Authentication Server which matches the local computer name, then within the Realm create a user account which matches the name of the SAM based user.

Remote Desktop / Terminal Services

Terminal servers may also be secured using the Authlogics Windows Desktop Agent. This allows for strong authentication to be enforced on RDP connections independent of any remote access or gateway security.

Note

The Windows Desktop Agent is not required to be installed on the RDP client, only on the RDP server.

Deployment

The following deployment overview walks through the installation process for deploying the Authlogics Windows Desktop Agent.

Overview

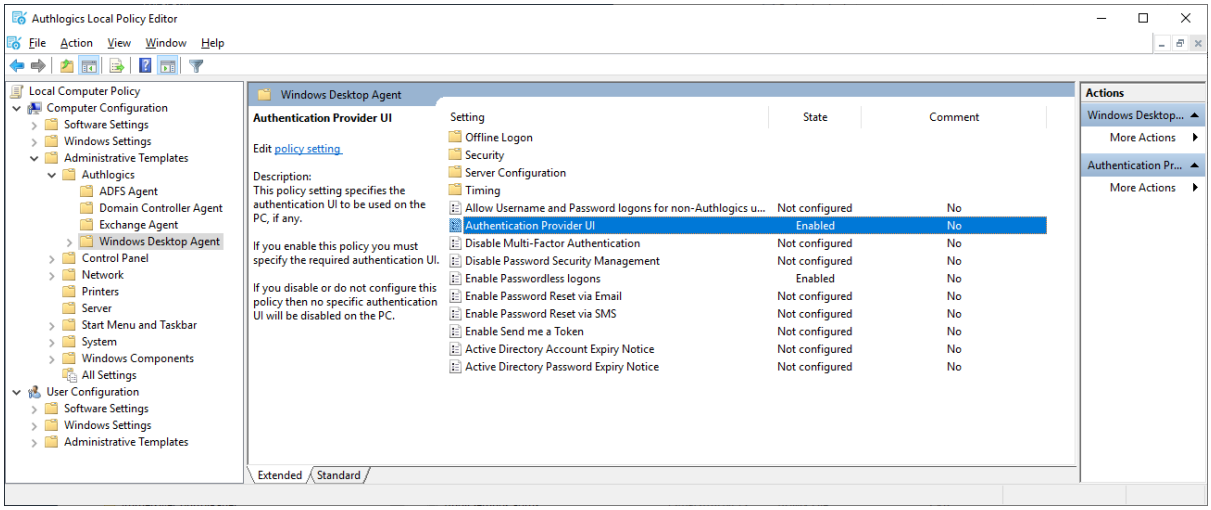
This deployment section assumes that at least one Authlogics Authentication Server has already been installed and is functional. See the Authlogics Authentication Server Installation and Configuration Guide for further information on setting up the Authlogics Authentication Server. In addition, Authlogics user accounts should already be configured for users.

(1) Configure a Group Policy object to target the systems you are installing the Authlogics Windows Desktop Agent onto with the required agent settings.
(2) Install the Authlogics Windows Desktop Agent on a Windows system.
(3) Test user logins.

The agent installation can be performed manually, via an automated script or via Group Policy Software Distribution, however this is beyond the scope of this document.

Working with and locating Group Policy Templates

Application specific policy settings are configured using the Group Policy Management Editor:



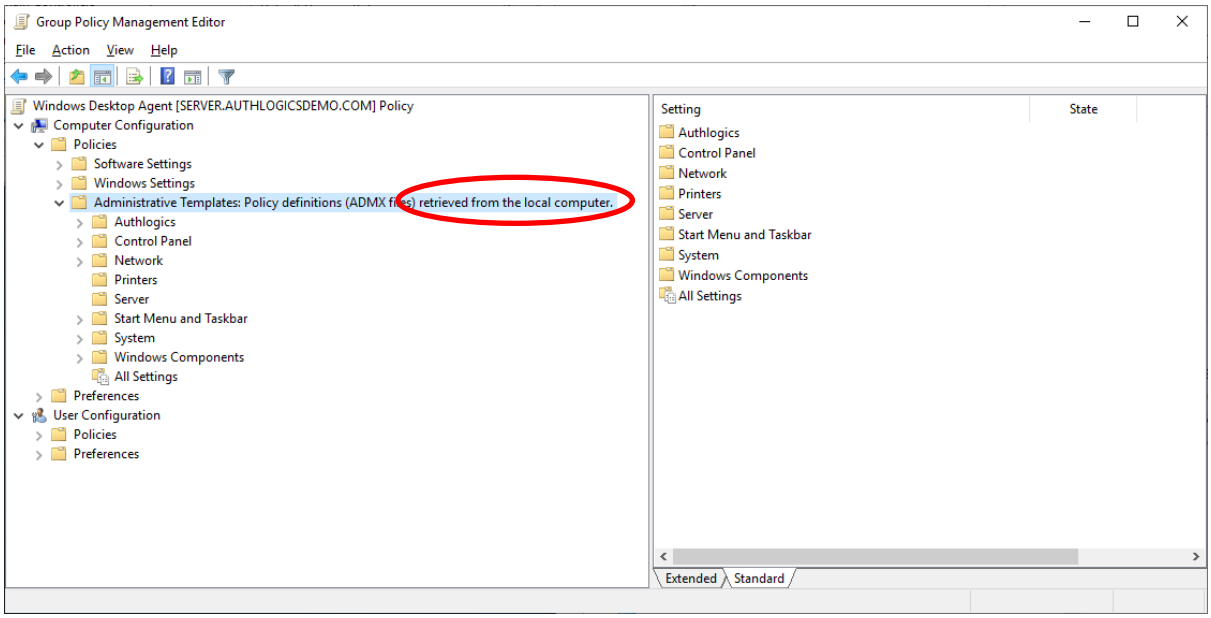
The Group Policy Management Editor loads application specific settings from template files. The template files can either be loaded from the *Local Computer* via the `C:\Windows\PolicyDefinitions` folder (Added by the Agent installer) or the Active Directory *Central Store*.

Note

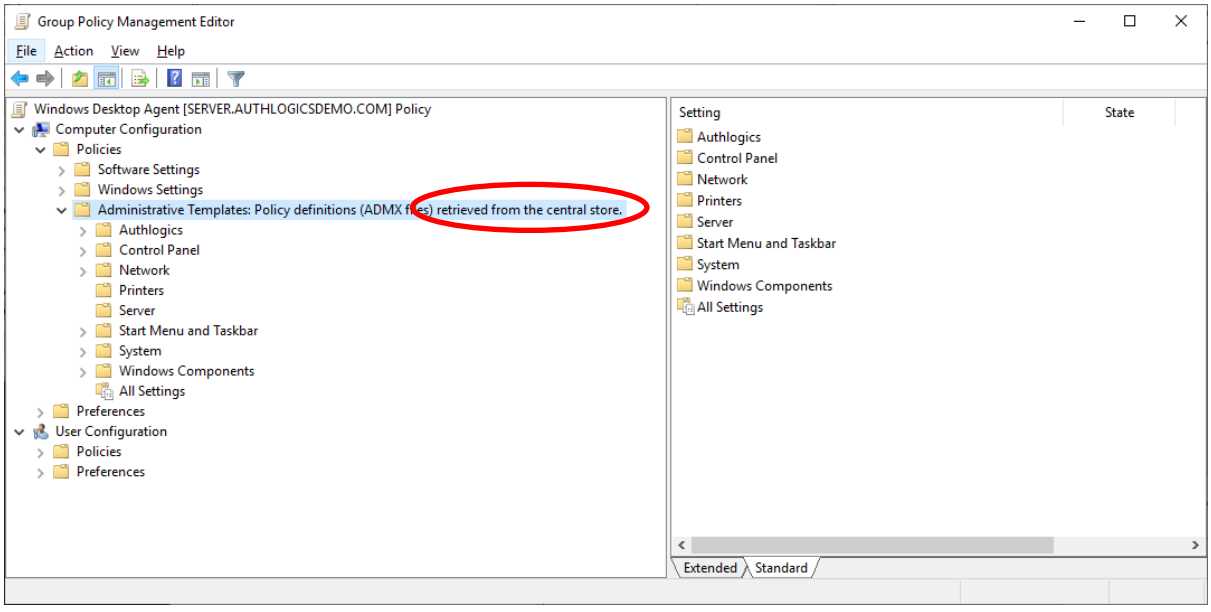
The template files are only required by the Group Policy Management Editor during the editing of Group Policy objects. They are NOT required on PC's where the policy is being applied.

The Group Policy Management Editor will state if templates (ADMX files) are being loaded from the Local Computer or the Central Store. This will vary depending on the Active Directory environment setup.

ADMX located on Local Computer:

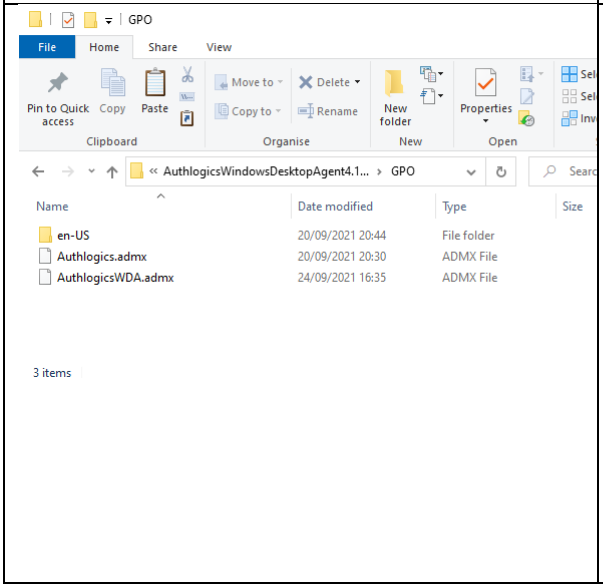
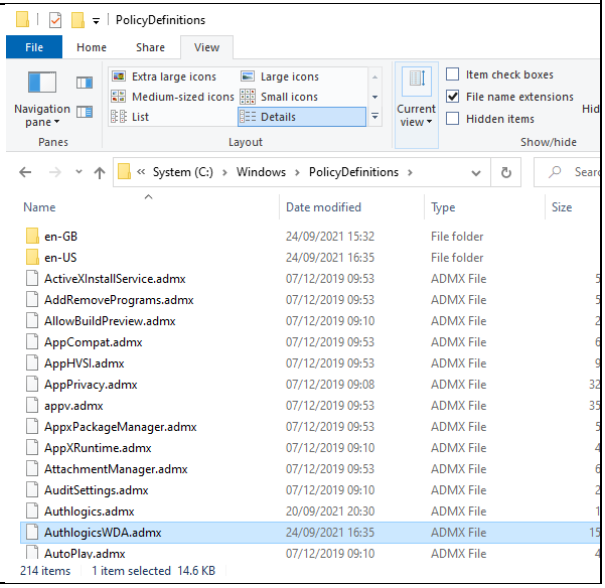


ADMX located in Central Store:



Adding Group Policy ADMX Templates to the Local Computer

If the Group Policy is being created/edited on a PC that does NOT have the Agent installed and there is no Central Store configured in AD then all of the template files, including the en-US language folder, must be copied from the `\GPO` folder of the installation media to the `C:\Windows\PolicyDefinitions\` folder where the Group Policy Management Editor is being run.

Source:	Destination:
`\GPO\*.*`	`C:\Windows\PolicyDefinitions\`
	

> **Note**
>
> The Authlogics templates folder includes an en-US language folder which must be coppied. If the destination computer does not have an en-US language folder then it must be created. Do not copy the language files from the en-US folder to a different language folder on the destination computer.

Using a Group Policy "Central Store"

The storage of Group Policy Administrative Template can be centralised a *Central Store* in Active Directory. If a Central Store is already being used simply copy the files from the installation media `\GPO` folder to the following folder on the domain controller:

```
\\{dnsdomain}\SYSVOL\{dnsdomain}\policies\PolicyDefinitions
```

If the *PolicyDefinitions* folder does not exist then a Central Store has not been configured. For further information regarding creating and managing a Group Policy Central Store see the following Microsoft documentation: https://docs.microsoft.com/en-us/troubleshoot/windows-client/group-policy/create-and-manage-central-store

Configuring the Group Policy Settings

When the Group Policy Templates are correctly installed the settings are visible in the Group Policy Management Editor. The *User Configuration* section of the GPO can be disabled as the settings only apply to the *Computer Configuration*.

By default, installing the Authlogics Windows Desktop Agent does NOT disable the existing Windows Credential Providers and will only add an additional Credential Provider for Authlogics MFA. Group Policy must be used to disable other providers which are not required.

The following Active Directory Group Policy settings are available for configuring the agent:

General Settings

Setting	Active Directory Account Expiry Notice
Values	(0-365)
Default	10 (Days)
Description	
This policy setting sets the number of days before an Active Directory account will expire for a notice is displayed to the user. Setting this value too high can cause excessive prompts, whereas setting this value too low may not give the user enough notice. If you enable this policy you must specify the number of days before an Active Directory account expires for a notice is displayed to the user. Setting this value to 0 will disable the notice. If you disable or do not configure this policy the Windows Desktop Agent will not display a notice to the user.	

Setting	Active Directory Password Expiry Notice
Values	(0-365)
Default	10 (Days)
Description	
This policy setting sets the number of days before an Active Directory password will expire for a notice is displayed to the user. Setting this value too high can cause excessive prompts, whereas setting this value too low may not give the user enough notice. If you enable this policy you must specify the number of days before an Active Directory password expires for a notice is displayed to the user. Setting this value to 0 will disable the notice. If you disable or do not configure this policy the Windows Desktop Agent will not display a notice to the user.	

Setting	Allow Username and Password logons for non-Authlogics users
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting allows users who do not have an Authlogics account to logon to the PC via the Authlogics Windows Desktop Agent. Users who are configured with an Authlogics account are required to logon with an OTP. If you enable this policy AD users who do not have an Authlogics account are able to logon. If you disable or do not configure this policy then only users who have an Authlogics account are able to logon.	

Setting	Authentication Provider UI
Values	Off / PINgrid / PINphrase / Mobile Push
Default	Off
Description	
This policy setting specifies the authentication UI to be used on the PC, if any. If you enable this policy you must specify the required authentication UI. If you disable or do not configure this policy then no specific authentication UI will be disabled on the PC.	

Setting	Disable Multi-Factor Authentication
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables Multi-Factor Authentication on the PC. If you enable this policy, users will not be prompted to enter Multi-Factor Authentication credentials at logon. If you disable or do not configure this policy then Multi-Factor Authentication will be enabled on the PC.	

Setting	Disable Password Security Management
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables Password Security Management on the PC. If you enable this policy, password policy checks will not be performed. If you disable or do not configure this policy then password policy checks will be performed when a user changes their password.	

Setting	Enable Password Reset via Email
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enables a 'Forgot Password' link to be displayed on the logon screen which when clicked sends a One Time Code to the user via email. If you enable this policy a 'Forgot Password' link will appear on the Windows logon screen if the user has a configured email address. If you disable or do not configure this policy then a 'Forgot Password' link will not be displayed on the Windows logon screen.	

Setting	Enable Password Reset via SMS
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enables a 'Forgot Password' link to be displayed on the logon screen which when clicked sends a One Time Code to the user via SMS. If you enable this policy a 'Forgot Password' link will appear on the Windows logon screen if the user has a configured phone number. If you disable or do not configure this policy then a 'Forgot Password' link will not be displayed on the Windows logon screen.	

Setting	Enable Passwordless logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting removes the Active Directory password from the Windows logon screen allowing users to logon with only a Username and One Time Passcode. If you enable this policy the Windows Desktop Agent will not ask for an AD password when a user logs on; unless there is no password available in the Password Vault. If you disable or do not configure this policy then users will be required to enter their AD password together with a One Time Passcode at each logon.	

Setting	Enable the 'Send me a Token' link
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enables a 'Send me a Token' link to be displayed on the logon screen which when clicked sends a Real-Time token to the user. If the user is not configured for MFA or is set to use a soft token only then no token will be sent. If you enable this policy a 'Send me a Token' link will appear on the Windows logon screen. If you disable or do not configure this policy then a 'Send me a Token' link will not be displayed on the Windows logon screen.	

Security Settings

Setting	Allow logon with local SAM accounts
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting allows the use of local SAM username and password for logon to the PC. If you enable this policy local SAM accounts can be used for logon without an OTP. If you disable or do not configure this policy local SAM accounts cannot be used for logon.	

Setting	Disable MFA for Windows Credential Prompting
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables MFA for Windows Credential Prompting. If you enable this policy MFA be not be available for use when Windows prompts users for credentials. If you disable or do not configure this policy the Windows Desktop Agent will use MFA when Windows prompts users for credentials.	

Setting	Disable Windows Cloud Experience logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Cloud Experience logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Cloud Experience logon functionality will not be available for use. If you disable or do not configure this policy the Windows Cloud Experience logon functionality will be available for use.	

Setting	Disable Windows Desktop Agent when on the LAN
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the Windows Desktop Agent functionality when the PC is connected to the local area network. If you enable this policy the Windows Desktop Agent functionality will not be available for use when the PC is on the LAN and will only function when the PC is working remotely. If you disable or do not configure this policy the Windows Desktop Agent functionality will be available at all locations.	

Setting	Disable Windows FIDO2 logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows FIDO2 logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows FIDO2 logon functionality will not be available for use. If you disable or do not configure this policy the Windows FIDO2 logon functionality will be available for use.	

Setting	Disable Windows Hello for Business Face Recognition logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Hello for Business Face Recognition logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business Face Recognition logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business Face Recognition logon functionality will be available for use.	

Setting	Disable Windows Hello for Business Fingerprint logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Hello for Business Fingerprint logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business Fingerprint logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business Fingerprint logon functionality will be available for use.	

Setting	Disable Windows Hello for Business PIN logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Hello for Business PIN logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business PIN logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business PIN logon functionality will be available for use.	

Setting	Disable Windows Hello for Business Trusted Signal logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Hello for Business Trusted Signal (Phone proximity, Network location etc) logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Hello for Business Trusted Signal logon functionality will not be available for use. If you disable or do not configure this policy the Windows Hello for Business Trusted Signal logon functionality will be available for use.	

Setting	Disable Windows Iris logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Iris logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Iris logon functionality will not be available for use. If you disable or do not configure this policy the Windows Iris logon functionality will be available for use.	

Setting	Disable Windows Picture Password logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Picture Password logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Picture Password logon functionality will not be available for use. If you disable or do not configure this policy the Windows Picture Password logon functionality will be available for use.	

Setting	Disable Windows Smart Card logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Smart Card logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Smart Card logon functionality will not be available for use. If you disable or do not configure this policy the Windows Smart Card logon functionality will be available for use.	

Setting	Disable Windows Smart Card Password Changes
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows Smart Card logon functionality for Password Changes. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows Smart Card logon functionality will not be available for use during a password change. If you disable or do not configure this policy the Windows Smart Card logon functionality will be available for use during a password change.	

Setting	Disable Windows Username and Password logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disables the built in Windows username and password logon functionality. This should be enabled if Authlogics is the only authentication type which is required. If you enable this policy the built in Windows username and password logon functionality will not be available for use. If you disable or do not configure this policy the Windows username and password logon functionality will be available for use.	

Setting	Enable Windows Desktop Agent in Windows Safe Mode
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enables the use of Windows Desktop Agent while Windows is running in Safe Mode. By default, Windows disables 3rd party authentication providers, such as Windows Desktop Agent, and non-critical services while in Safe mode. If you enable this policy the Authlogics Windows Desktop Agent will be active and the Windows Desktop Agent service will be allowed to run while in Safe Mode. If you disable or do not configure this policy the Authlogics Windows Desktop Agent will not be available when in Safe Mode and the built in Windows Username and Password logon option will be available.	

Offline Logon Settings

Setting	Disable Offline Deviceless OTP Authentication
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting configures the Deviceless OTP authentication offline functionality of the Windows Desktop Agent. Note: If the "Disable Offline logons" policy is enabled then this policy will not take effect. If you enable this policy the Windows Desktop Agent will not provide any Deviceless OTP authentication offline functionality, including External Server Access. Only 2FA offline logons will be allowed. If you disable or do not configure this policy the Windows Desktop Agent will cache required user and settings information from the Active Directory to allow for Deviceless OTP offline logons.	

Setting	Disable Offline logons
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting configures the offline functionality of the Windows Desktop Agent. If you enable this policy the Windows Desktop Agent will not provide any offline functionality, including External Server Access. If you disable or do not configure this policy the Windows Desktop Agent will cache required user and settings information from the Active Directory to allow for offline logons.	

Setting	Offline AD sync schedule
Values	(1-9999)
Default	24 (Hours)
Description	
This policy setting specifies the interval between scheduled synchronisations between the Windows Desktop Agent and the Active Directory to refresh locally cached data for offline logons. Note: If the "Disable Offline logons" policy is enabled then this policy will not take effect. If you enable this policy you must specify the interval value in hours between synchronisations between the Windows Desktop Agent and the Active Directory. If you disable or do not configure this policy the Windows Desktop Agent will synchronise with the Active Directory every 24 hours.	

Server Configuration Settings

Setting	Authlogics Authentication Server Names
Values	Any DNS based server address (CSV)
Default	{blank}
Description	
This policy setting configures the server name(s) which PCs will use to connect to the Authlogics Authentication Server instead of searching the Active Directory for server names. If you enable this policy you must specify at least one server DNS name, however, multiple server names can be specified separated by a comma, e.g. server1.domain.com,server2.domain.com If you disable or do not configure this policy the Active Directory will be searched to locate one or more Authlogics Authentication Servers.	

Setting	Authlogics Authentication Server Standard Port (HTTPS/SSL)
Values	(1024 – 65535)
Default	14443
Description	
This policy setting configures the Authlogics Authentication Server port number which PCs will use to connect to the Authlogics Authentication Server when they are on the LAN. The server name will be located automatically via an Active Directory search unless specified in the "Authlogics Authentication Server Names" policy. If you enable this policy you must specify a TCP port number, e.g.14443 If you disable or do not configure this policy the default port 14443 will be used.	

Setting	Domain Controller Server Names
Values	Any DNS based server address (CSV)
Default	{blank}
Description	
This policy setting configures the server name(s) which PCs will use to connect to Domain Controllers instead of auto detecting them. If you enable this policy you must specify at least one Domain Controller DNS name, however, multiple server names can be specified separated by a comma, e.g. dc1.domain.com,dc2.domain.com If you disable or do not configure this policy the PC will auto detect which Domain Controller to use.	

Setting	External Access Server Address
Values	Any DNS based server address and TCP port
Default	{blank}
Description	
This policy setting configures the server name and port number which PCs will use to connect to the Authlogics Authentication Server when they are outside of the LAN. External Access allows an Authlogics Authentication Server to authenticate a user if even if the PC is not on the LAN. External Access always uses SSL encryption (HTTPS) and should be published via a reverse proxy server for extra security. If you enable this policy you must specify a DNS server address and port number, e.g. eas.mycompany.com:14443 If you disable or do not configure this policy the External Address functionality will be disabled.	

Setting	Global Catalog Server Names
Values	Any DNS based server address (CSV)
Default	{blank}
Description	
This policy setting configures the server name(s) which PCs will use to connect to Global Catalogs instead of auto detecting them. If you enable this policy you must specify at least one Global Catalog DNS name, however, multiple server names can be specified separated by a comma, e.g. gc1.domain.com,gc2.domain.com If you disable or do not configure this policy the PC will auto detect which Global Catalog to use.	

Timing Settings

Setting	Active Directory access timeout
Values	(0 – 120)
Default	15 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while connecting to an Active Directory Domain Controller before going offline. Setting this value too high can make HA failovers take longer while the AD is being located, whereas setting this value too low could result in the Windows Desktop Agent running in offline mode even when the AD is available. If you enable this policy you must specify the interval value in seconds to wait while locating an Active Directory Domain before reverting to offline mode. Setting this value to 0 will disable the timeout and connections will wait indefinitely. If you disable or do not configure this policy the Windows Desktop Agent will wait for 15 seconds while locating an Active Directory Domain before reverting to offline mode.	

Setting	Active Directory Domain Controller refresh time
Values	(1 – 1440)
Default	60 (minutes)
Description	
This policy setting sets the maximum amount of time to wait before retesting the Domain Controller connectivity for the quickest connection. Setting this value too high will make connections stay on a single server for longer, whereas setting this value too low could result in too many checks being performed. If you enable this policy you must specify the interval value in minutes to wait before retesting the Domain Controller connectivity. If you disable or do not configure this policy the Windows Desktop Agent will retest the Domain Controller connectivity every 60 minutes.	

Setting	Authenticator App device pairing timeout
Values	(30 – 300)
Default	120 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while the Authlogics Windows Desktop Agent Service pairs a new profile with the Authlogics Authenticator App and waits for a response. If you disable or do not configure this policy the Windows Desktop Agent will wait for 120 seconds for a response from the app.	

Setting	Authenticator App Mobile Push Authentication timeout
Values	(30 – 300)
Default	120 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while the Authlogics Windows Desktop Agent Service sends a Mobile Push notification to the Authlogics Authenticator App and waits for a response. If you disable or do not configure this policy the Windows Desktop Agent will wait for 120 seconds for a response.	

Setting	Authlogics Authentication Server access timeout
Values	(0 – 120)
Default	15 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while connecting to an Authlogics Authentication Server before trying an alternative server if available or going offline. If you enable this policy you must specify the interval value in seconds to wait while connecting to an Authlogics Authentication Server. Setting this value to 0 will disable the timeout and connections will wait indefinitely. If you disable or do not configure this policy the Windows Desktop Agent will wait for 15 seconds for a response from an Authlogics Authentication Server.	

Setting	Authlogics Authentication Server refresh time
Values	(1 – 1440)
Default	60 (minutes)
Description	
This policy setting sets the maximum amount of time to use the current Authlogics Authentication Server before refreshing the most suitable server. If you enable this policy you must specify the interval value in minutes to wait before refreshing which Authlogics Authentication Server to use. If you disable or do not configure this policy the Windows Desktop Agent will wait for 60 minutes before refreshing which Authlogics Authentication Server to use.	

Setting	Authlogics External Access Server timeout
Values	(0 – 120)
Default	8 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while connecting to an Authlogics External Access Server before going offline. If you enable this policy you must specify the interval value in seconds to wait while connecting to an Authlogics External Access Server. Setting this value to 0 will disable the timeout and connections will wait indefinitely. If you disable or do not configure this policy the Windows Desktop Agent will wait for 8 seconds for a response from an Authlogics External Access Server.	

Setting	Authlogics Windows Desktop Agent Service access timeout
Values	(0 – 120)
Default	45 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while the Authlogics Windows Desktop Agent Service attempts to start before timing out and reverting to a standard Windows logon. If you enable this policy you must specify the interval value in seconds to wait for the service to start. Setting this value to 0 will disable the timeout and connections will wait indefinitely preventing a fallback to standard Windows logon. If you disable or do not configure this policy the Windows Desktop Agent will wait for 45 seconds for the Authlogics Windows Desktop Agent service to start.	

Setting	Offline access timeout
Values	(1 – 30)
Default	4 (seconds)
Description	
This policy setting sets the maximum amount of time to wait while locating an available Authlogics Authentication Server or Active Directory Domain Controller going offline. Setting this value too high can make offline status detection take longer while an available Authlogics Authentication Server or Active Directory Domain Controller is being located, whereas setting this value too low could result in the Windows Desktop Agent running in offline mode even when a server is available. If you enable this policy you must specify the interval value in seconds to wait while locating an available Authlogics Authentication Server or Active Directory Domain Controller before reverting to offline mode. If you disable or do not configure this policy the Windows Desktop Agent will wait for 4 seconds while locating an available Authlogics Authentication Server or Active Directory Domain Controller before reverting to offline mode.	

Pre-requisites

The installer will check for pre-requisites and install them automatically where possible. The required pre-requisites are:

- Microsoft .NET Framework 4.8

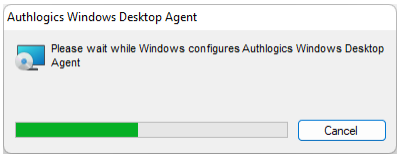
> **Note**
> .NET 4.8 has been included in Windows 10 since the May 2019 Update, however it is NOT included in any Windows Server version. A full list of included versions is available here: https://docs.microsoft.com/en-us/dotnet/framework/migration-guide/versions-and-dependencies

If the installation of a pre-requisite fails then the installation will also fail.

Installing Authlogics Windows Desktop Agent

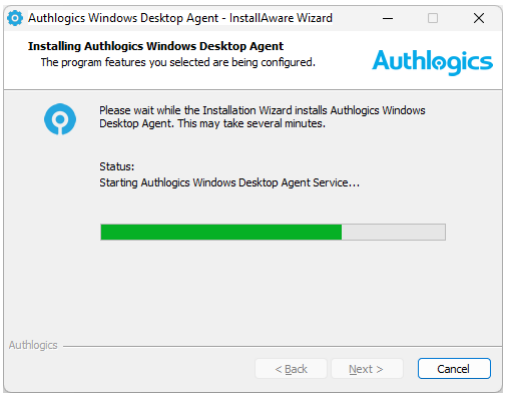
The Authlogics Windows Desktop Agent enables a Windows PC or Server to leverage Authlogics MFA and PSM services.

(1) To start the Authlogics Windows Desktop Agent installation, run the *Authlogics Windows Desktop Agent xxxxx.msi* installer with **elevated privileges**.

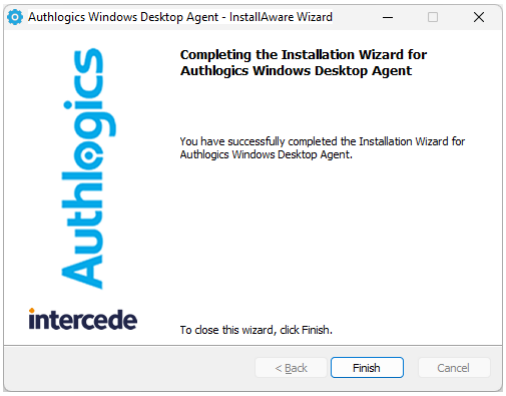


(2) Click *Next* to begin the install or *Cancel* to quit.

The installation is being performed.

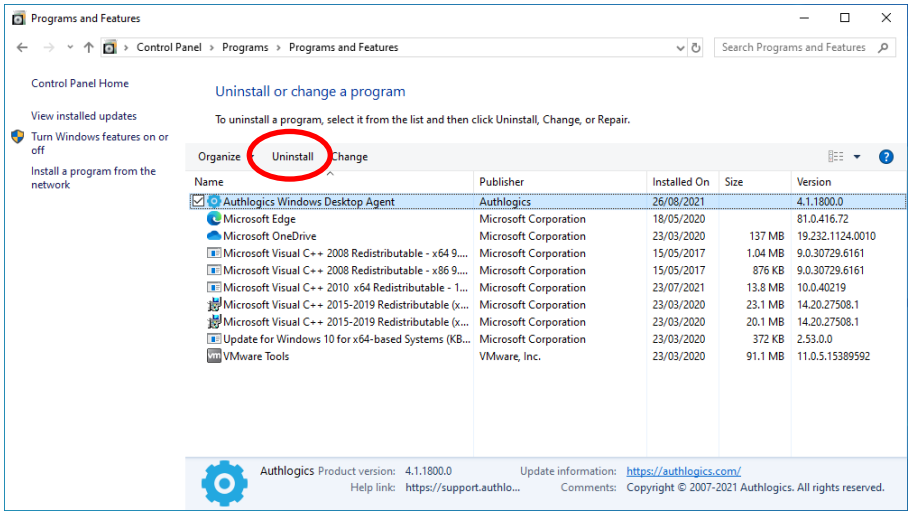


(3) All necessary Authlogics Windows Desktop Agent files have been installed. Click *Finish* to complete the installation process.



Uninstalling Authlogics Windows Desktop Agent

If you no longer require Windows Desktop Agent on a machine, you can remove it by performing an uninstall from Control Panel > Programs > Programs and Features:



Note

The offline cache database files and the certificates generated during the install are not removed after performing an uninstall.

Automated / command line Setups

Running an installation with verbose logging

In scenarios where the installation may not succeed successfully on a system, it may be necessary to run setup with logging enabled to help identify the problem. The following command will run setup and create a setup.log file containing information about the install:

```
msiexec /i "Authlogics Windows Desktop Agent xxxxx.msi" /lv setup.log
```

Fully automated silent installation

Setup can be run silently directly by simply running the MSI file with a /q switch, or via the MSI Executive interface as follows:

```
"Authlogics Windows Desktop Agent xxxxx.msi" /q
```

or

```
msiexec /i "Authlogics Windows Desktop Agent xxxxx.msi" /quiet
```

Fully automated silent removal

The agent can be removed silently using the /x switch as follows:

```
msiexec /x "Authlogics Windows Desktop Agent xxxxx.msi" /quiet
```

Network Level Authentication (NLA) and Remote Desktop

Authlogics Windows Desktop Agent is designed to work with Windows Terminal Services and Remote Desktop connections. The login process looks and works the same way as when logging onto a physical PC directly, except via the Remote Desktop client.

Network Level Authentication is an authentication method that can be used to enhance RD Session Host server security by requiring that the user be authenticated to the RD Session Host server before a session is created.

Network Level Authentication completes user authentication before you establish a remote desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software. The advantages of Network Level Authentication are:

- It requires fewer remote computer resources initially. The remote computer uses a limited number of resources before authenticating the user, rather than starting a full remote desktop connection as in previous versions.
- It can help provide better security by reducing the risk of denial-of-service attacks.

Source: http://technet.microsoft.com/en-gb/library/cc732713.aspx

Network Level Authentication uses CredSSP between the Remote Desktop Client and the server. CredSSP is a Security Support Provider (SSP) that is available in Windows which enables a program to use client-side SSP to delegate user credentials from the client computer to the target server.

Issues with NLA & Multi-Factor Authentication

Microsoft does not provided any 3rd party support in Windows for custom Security Support Providers (SSP) which can be used with NLA. As such NLA is not compatible with Multi-Factor Authentication, only via built-in Windows authentication routines, i.e. passwords and smart cards.

The Authlogics Windows Desktop Agent can be used with NLA enabled however the user may experience a *double logon* scenario:

(1) Challenged for username and password via the RDP client (used for NLA)
(2) Challenged for username, optional password, and OTP via Authlogics Windows Desktop Agent within the RDP screen.

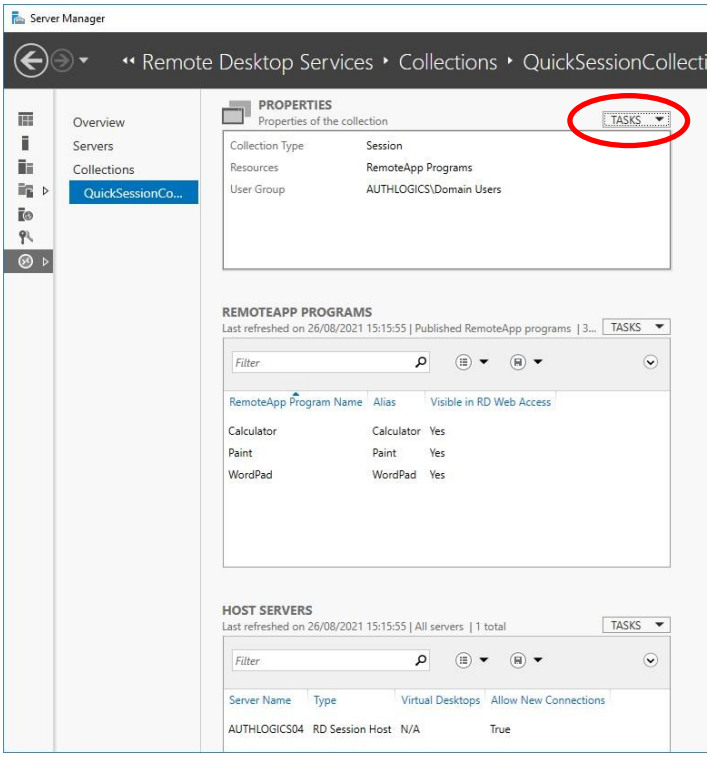
The double logon can be mitigated by either:

- NLA Enabled: Caching the user password within the remote desktop client.
- NLA Disabled: Remove the logon prompt from the RDP client via a custom .RDP file or a 3rd party RDP client that does not use NLA.

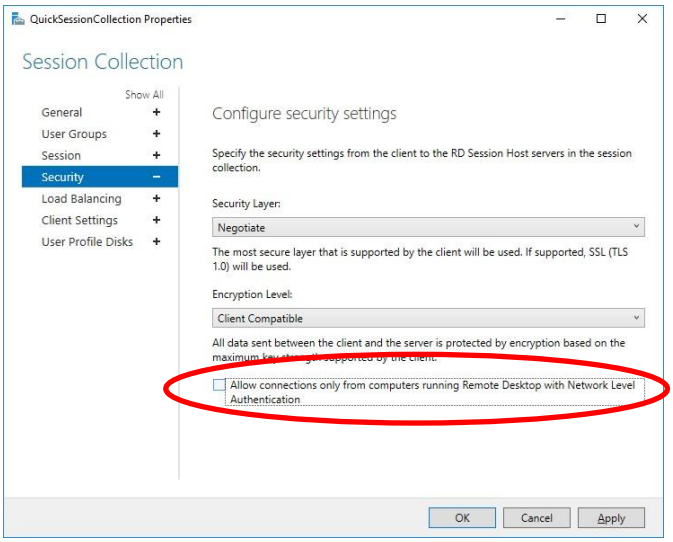
Disabling NLA on Windows Server 2016

The steps required to disable NLA on Windows server may vary depending on the OS version. On Windows Server 2016 can be done as follows:

(1) Open *Server Manager*.
(2) Select Remote Desktop Services.
(3) Select the active Session Collection.
(4) Click *TASKS* and select *Edit Properties*.



(5) Select *Security* from the list on the left.

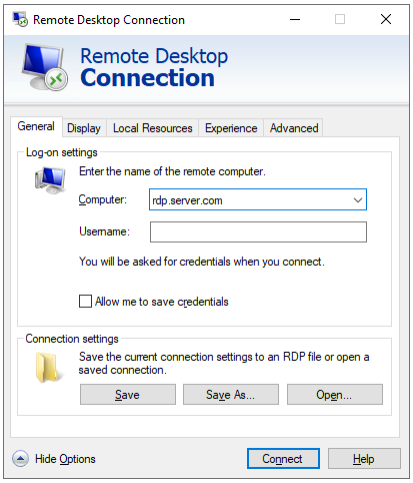


(6) Untick *Allow connections only from computers running Remote Desktop with Network Level Authentication*.
(7) Click *Ok* and close Server Manager.

Disabling NLA on the RDP client

> **Note**
> NLA must be disabled, or at least not required, on the server prior to disabling NLA on the client otherwise connections will be rejected.

(1) Create an RDP connection on a client with the required connection information.



(2) Click *Save As...* and save the RDP configuration to a file.
(3) Edit the RDP file in notepad and add the following line to the file:

```
enablecredsspsupport:i:0
```

(4) Save and close the RDP file in notepad.
(5) The new RDP configuration file can now be used to connect to the server without NLA.

Disabling NLA on the macOS client

> **Note**
> NLA must be disabled, or at least not required, on the server prior to disabling NLA on the client otherwise connections will be rejected.

macOS Remote Desktop clients prior to version 10.2.2 did not support NLA and therefore NLA is off by default.

Agent Architecture

The architecture of the Authlogics Windows Desktop Agent is made up of a few key components:

- An *Authlogics Windows Desktop Agent* Windows Service which caters for:
  - Password policy processing
  - Offline logons
  - Caching and syncing with AD when online
  - Deviceless OTP challenge generation
  - Processing AD Group Policy settings
- A Windows Credential Provider which plugs into the Windows logon screen and communicates with the *Authlogics Windows Desktop Agent* Service.
- An AES256 bit encrypted cache database.