Installation and Configuration Guide

MyID Multi-Factor Authentication and Password Security Management

Product Version: 5.0.6942.0

Publication date: March 2024

Call us on:	+44 (0)1455 558 111 (UK & EMEA) +1 408 706 2866 (US)
Email us:	info@intercede.com

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organisations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organisation, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

Intercede may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written licence agreement from Intercede, the furnishing of this document does not give you any licence to these patents, trademarks, copyrights, or other intellectual property.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

The information contained in this document represents the current view of Intercede on the issues discussed as of the date of publication. Because Intercede must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Intercede, and Intercede cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. INTERCEDE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS Document.

Table of Contents

Introduction

> **Note**
> MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly.
>
> The term 'Authlogics' may still appear in certain areas of the product.

MyID Authentication Server is a multi-factor authentication system which provides:

- Token and tokenless, device and deviceless Multi-Factor Authentication.
- Mobile Push Authentication.
- NIST 800-63B compliant Password Security Management solution.
- Self-service password reset and unlocking.
- Web Service API and RADIUS interfaces for connectivity.
- Multiple Authentication technologies:
  - Grid Pattern - Pattern Based Authentication
  - Phrase - Random Character Authentication
  - One Time Code - OATH (TOTP) Compliant Authentication
  - YubiKey – Yubico YubiKey hardware token support
  - FIDO2 / Passkey
  - Google / Microsoft Authenticators (OATH compliant)

Considerations

System Requirements

The supported operating systems for MyID Authentication Server are:

- Windows Server 2022 *
- Windows Server 2019
- Windows Server 2016

> **Note: * Windows Server 2022 Update Requirement**
> The MyID Reporting Dashboard requires the update from Microsoft KB5023705, or latest Windows Updates, on Windows Server 2022 due to a known OS issue listed by Microsoft as "This update addresses an issue that affects the Get-WinEvent cmdlet. It fails. The system throws InvalidOperationException".

Minimum .NET Framework version: 6

The hardware requirements for MyID Authentication Server are:

	Minimum	Recommended
CPU	Dual Core 1.2 GHz	Quad Core 2.5 GHz
RAM	4Gb RAM	8Gb RAM
Disk	Single Disk	Dual Disk

Rights and Permissions

Local administrator rights are required to perform the binary installation process of the MyID Authentication Server on Windows Server.

The Directory Configuration Wizard requires either:

- Enterprise Admin rights
  or
- Domain Admin rights on the domain of which the Authentication server is a member, and
- Domain Admin rights on each domain containing user accounts which will be used with MyID.

Once the Directory Configuration Wizard is complete an administrator will need to be a member of the MyID Administrators group and have local administration rights on the member server.

Password Breach Databases

Intercede has 3 versions of its Password Breach Database:

(1) Offline Password Breach Database (Min)
- Included with MyID Authentication Server containing the top 1 million breached passwords.
- Infrequently updated.

(2) Offline Password Breach Database (Full)
- A separate download containing over 8 billion breached passwords.
- Infrequently updated.

(3) Cloud Password Breach Database
- An Internet hosted database containing over 8 billion breached credentials.
- Regularly updated.

The MyID Authentication Server includes an Offline Password Breach Database of the top 1 million most often breached passwords. This can reduce the reliance on Cloud Password Breach lookups. If a password is not found in the Offline Password Breach Database then, unless disabled by policy, the MyID Cloud Password Breach Database will also be checked.

A full Offline Password Breach Database containing over 8 billion breached passwords is available as a separate addon download from https://www.intercede.com/support/downloads. When the full database is installed it may be possible to disable Cloud Password Breach Database lookups.

Note

The MyID Cloud Password Breach Database is regularly updated whereas the Offline Password Breach Database is not. Unless a fully offline solution is required Intercede still recommends leaving Cloud Password Breach Database lookups enabled to ensure that the most recent entries are being checked.

High Availability

MyID is designed for multiple deployment sizes, topologies and configurations.

High availability is achieved by ensuring that there are multiple instances of the user database and the authentication server.

To ensure the user database is highly available there must be multiple Domain Controllers in each domain. Active Directory automatically replicates the domain information to all DC's in the domain, including MyID data.

To ensure high availability of the MyID Authentication servers, simply install multiple instances on separate servers which are members of the same AD Forest. Each server will use standard Windows mechanisms to locate and work with the most appropriate Domain Controller, or DC's and GC's can be manually specified. Each server can be addressed separately as a Primary/Secondary configuration, e.g. RADIUS1 and RADIUS2, or they can be clustered via the built-in Windows Network Load Balancing and treated as a single entity.

Database Backup & Restore

All user metadata is stored in Active Directory and no data is stored on the local server. All MyID data is automatically backed up along with Active Directory when you perform a standard AD backup.

A server can be recovered simply by reinstalling from the ground up and the new installation will be re-attached to the existing data in the AD and will continue functioning as before. Exceptions to this include and custom changes to the web UI and NPS (RADIUS) policy changes.

Developers

For developer-specific information regarding the Web Services Application Programming Interface (REST) please see the MyID Authentication Server Developers Guide.

Language Requirements

MyID Authentication Server is compatible with multi-lingual versions of Windows Server; however, it is only available in English. Product support and documentation are also only available in English.

Elements of the Microsoft Management Console (MMC) will show in the language of the server, e.g. “Ok” buttons, however, MyID specific text is in English only.

Internet Connectivity

The MyID Authentication Server requires Internet Access for certain functionality. The majority of required connectivity is outbound to the Internet and all URL's are bound to the authlogics.com DNS domain for easier management. Not all access is required as this will depend on the chosen product functionality.

Mobile Push Authentication

When using Mobile Push authentication for MFA , the MyID Authentication Server will require outbound Internet access to the following destination (depending on the capabilities of the network firewall):

- Destination URL: `https://*.ccp.authlogics.com/api/*`
- Host: `*.ccp.authlogics.com` on port `443`

Note
Devices running the Authlogics Authenticator app will also require access to the above URL. While this would normally be available when they are connected to GSM / public networks, they may require explicit access when on corporate Wi-Fi.

Password Breach Database

When using Password Security Management and the MyID Cloud Password Breach Database lookups are enabled, the MyID Authentication Server will require outbound Internet access to the following destination (depending on the capabilities of the network firewall):

- Destination URL: `https://passwordsecurityapi.authlogics.com/api/*`
- Host: `passwordsecurityapi.authlogics.com` on port `443`

Note
Domain Controller Agents do not require direct access to the Internet as they perform lookups via the Authentication Server. However, there is a GPO setting to enable Internet access as a fallback, and if enabled, Internet access will be required.

Licencing

Unless an offline licence has been provided, the MyID Authentication Server will require outbound Internet access to the following destination (depending on the capabilities of the network firewall):

- Destination URL: `https:// licencing.authlogics.com/api/*`
- Host: `licencing.authlogics.com` on port `443`

Warning
If access to the licencing URL is not available the licence may fail and the Authentication Server may cease to function.

External Access Server (Windows Desktop Agent)

When using the Windows Desktop Agent (optional) configured with an External Access Server the MyID Authentication Server will require inbound access from the Internet to the External Access Server instance of the Authentication Server on port 14444 (by default):

External Access Server role is a separate IIS site on the MyID Authentication Server hosting a limited API set to support the Windows Desktop Agent and runs on a separate port to the rest of the server. It is recommended that the Windows Desktop Agents are configured to use port 443 to ensure good connectivity over the Internet. To facilitate this a reverse proxy / port translator should be used to redirect external 443 traffic to the internal port 14444. Alternatively, the External Access Server IIS instance can be configured within IIS Manager to use port 443 on a separate IP address.

Licensing

MyID MFA and PSM solutions are licensed on a per-user basis with each user requiring a licence. A licence must be installed onto each instance of a MyID Directory. Contact sales@intercede.com for any licencing enquires.

To install a MyID licence simply run the Licence Configuration Wizard within the MyID Authentication Server Management Console.

Licence functionality

The functionality available in the MyID Authentication Server will depend on the type of licence(s) that are installed. All solution features are broken down into two licence types:

- Password Security Management (PSM)
- Multi-Factor Authentication (MFA)

A product key or licence is issued for each licence type.

> **Note**
> For detailed information on the licence types please refer to the licence agreement document embedded within the installation package.

Evaluation licence

MyID is available for trial use for an unlimited number of users with a 30-day time-limit. An evaluation licence can be requested and installed instantly via the Licence Configuration Wizard.

Free licence

MyID MFA and PSM solutions are available free of charge for up to 10 users with no time limit. A free licence can be requested and installed instantly via the Licence Configuration Wizard.

Design and Deployment Scenarios

MyID Authentication Server is an enterprise-class solution scaling from stand-alone single instance installations to highly availability multi-master Active Directory-integrated deployments. A single MyID server can support multiple Active Directory Domains in a single forest and the server can be a member of any domain within the forest. User accounts can be AD user accounts or external accounts which do not have an AD user account.

A variety of authentication tokens can be used with the MyID Authentication Server including SMS/Text message, email, offline OTP (pattern or OATH), Mobile Push, biometrics, FIDO2, Passkey and YubiKey hardware tokens.

MyID Authentication Server has been designed to integrate with a multitude of remote access solutions and applications. The core of MyID is the Authentication Server which is an IdP Server and also provides REST APIs and a RADIUS interface. MyID also provides agents for various 3rd party systems to allow for direct integration, e.g. Windows Desktop, Remote Desktop Gateway, Exchange Server etc.

Any remote access concentrator or application that can interact with REST Services or RADIUS will be able to communicate with the Authentication Server. Integration guides and sample code are also provided for common deployments to assist with the integration into 3rd party systems.

MyID Authentication server is a Federated Identity Provider (IdP) capable of being used as an replacement for ADFS and supports standard protocols of SAML 2.0 and OpenID Connect.

MyID Authentication Server is also a complete NIST 800-63B compliant password policy and management solution for Active Directory. It can ensure that users are not using known breached or shared passwords in real-time, as well as with retrospective checking and automatic remediation.

The MyID Authentication Server Management console utilises Microsoft Management Console technology. Administration rights are granted via roles which are typically mapped to Active Directory groups.

For high-availability deployment scenarios with numerous users, user information can be stored across multiple domains in an Active Directory forest. Multiple MyID servers can be deployed within an Active Directory forest for multiple points of presence, or in the same location with built-in Network Load Balancing for full HA.

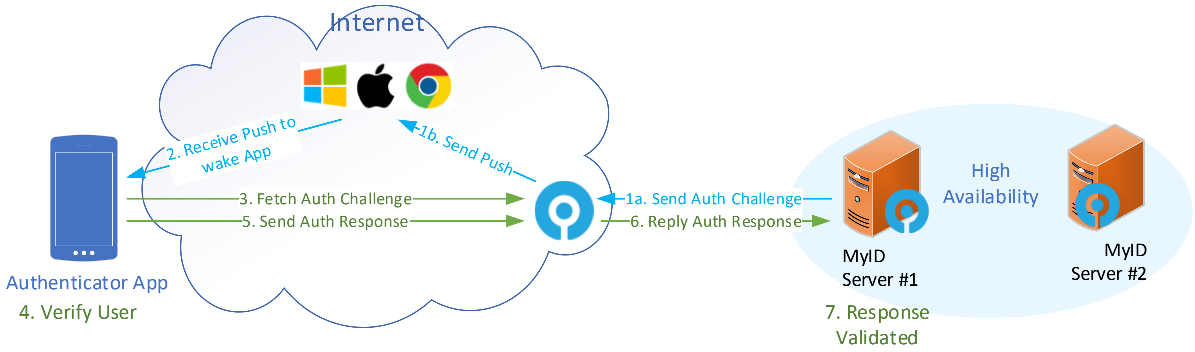
Mobile Push Authentication

Overview

MyID Mobile Push MFA has been designed to work seamlessly when online or offline, and does not rely on Microsoft, Apple & Google for timely delivery.

If the user is offline they can simply enter the short alpha-numeric OTP generated by the same Authlogics Authenticator App they use when they are online.

MyID MFA Mobile Push MFA Logon Process Flow



Public Push Networks

App notifications via Microsoft, Apple & Google Public Push Networks can be unreliable and they are not a guaranteed delivery service. MyID does not rely on Public Push Networks for core functionality and as such no authentication data or sensitive information is contained within the Public Push Networks notification.

If the Public Push Networks are functioning as expected it creates a better user experience, however, if not then the user can simply load the Authenticator App themselves and still login as normal.

Passwordless MFA

Mobile Push

Mobile Push MFA is most commonly deployed as a passwordless authentication solution, however, can also be used in conjunction with a password if required. This can be connected to applications via RADIUS, Web API or various agents including for Windows Desktop Agent.

Passwordless for Windows

The MyID Windows Desktop Agent allows users to logon to Windows without having to enter their Windows password. This form of passwordless logon is achieved by storing the AD Password in a Secure Password Vault which is seamlessly 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 Logon" functionality to remove the Active Directory password for logon group policy option on the Windows Desktop Agent.

For a detailed breakdown of the Passwordless process see the *Passwordless workflows* section later in this document.

The MyID Server Password Vault

The MyID Authentication Server uses Active Directory as a database, as such all of its data is physically stored on the Domain Controllers, including the Server Password Vault. The Password Vault is disabled by default and must be explicitly enabled before use.

During the Authentication Server installation, a unique certificate is generated with an RSA 2048bit key pair which is used to encrypt the password data. This certificate can be replaced at any time by running the Certificate Configuration Wizard on the server which will re-encrypt the data with the new certificate key pair. The MyID Password Vault information can only be decrypted if the certificate's private key is available.

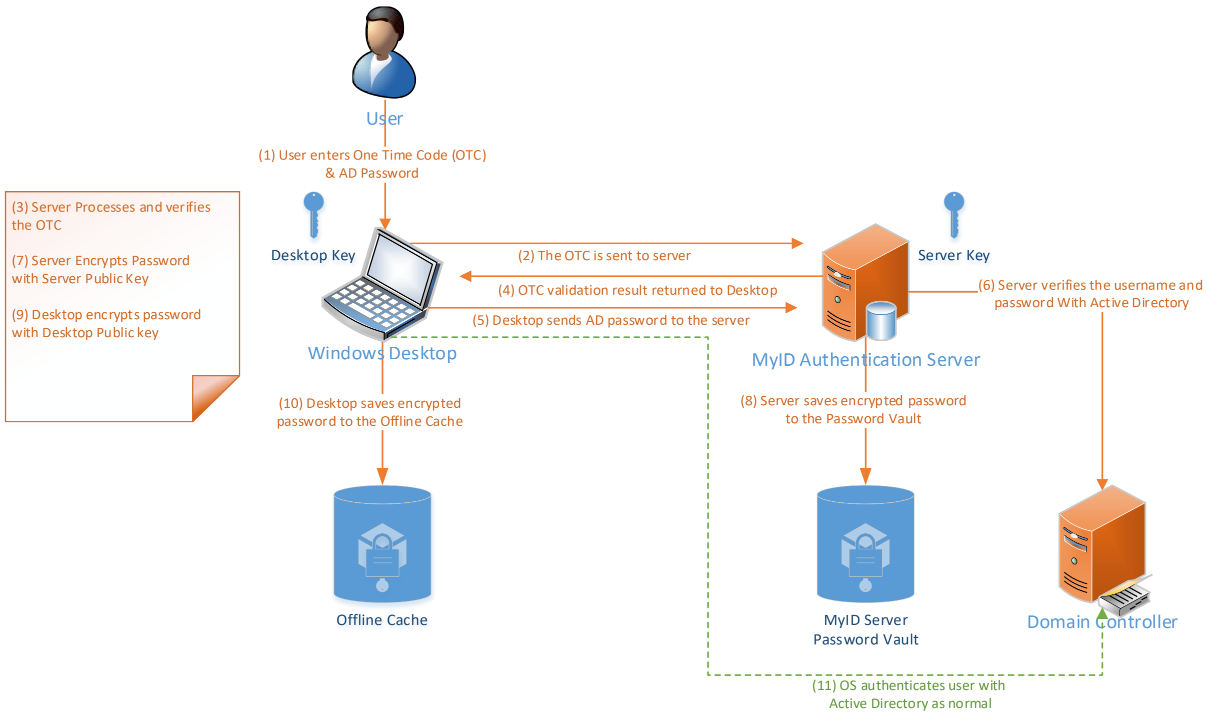
The Windows Desktop Agent

The Windows Desktop Agent is designed run on a Windows desktop/server machine to provide Multi-Factor Authentication security and Passwordless logons. The agent is fully managed and deployable via Active Directory group policy for easy and granular administration.

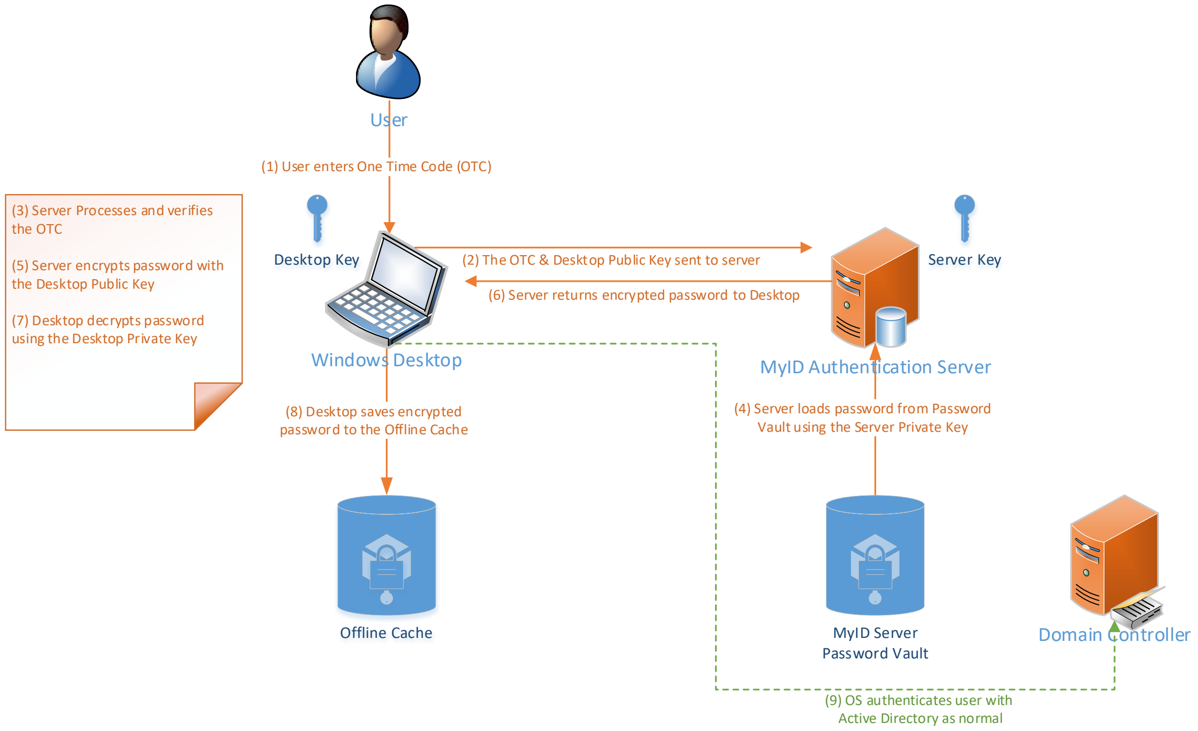
The agent can work in an offline scenario for when there is no connection available to the Authentication Server.

See the MyID Windows Desktop Agent Integration Guide for further information.

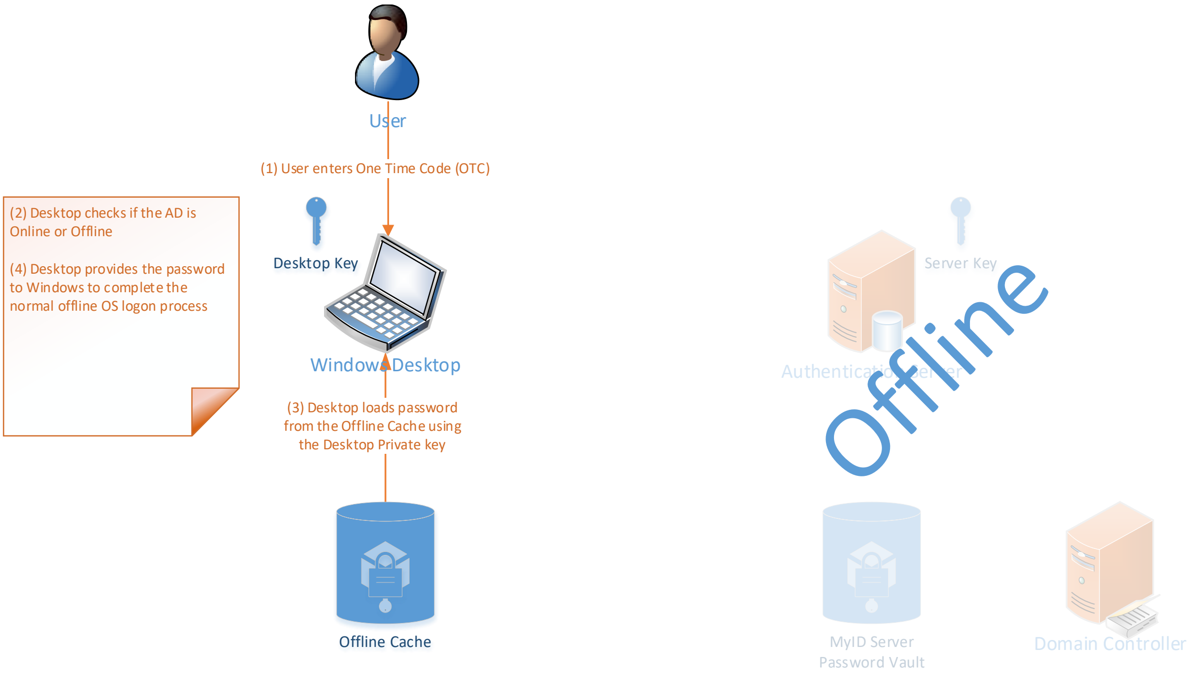
MyID MFA Windows Desktop Password-less logon process First Online Logon


User
(1) User enters One Time Code (OTC) & AD Password
(3) Server Processes and verifies the OTC
(7) Server Encrypts Password with Server Public Key
(9) Desktop encrypts password with Desktop Public key
Desktop Key
Windows Desktop
(2) The OTC is sent to server
(4) OTC validation result returned to Desktop
(5) Desktop sends AD password to the server
Server Key
MyID Authentication Server
(6) Server verifies the username and password With Active Directory
(10) Desktop saves encrypted password to the Offline Cache
(8) Server saves encrypted password to the Password Vault
Offline Cache
MyID Server Password Vault
Domain Controller
(11) OS authenticates user with Active Directory as normal

MyID MFA Windows Desktop Password-less logon process Regular Online Logon

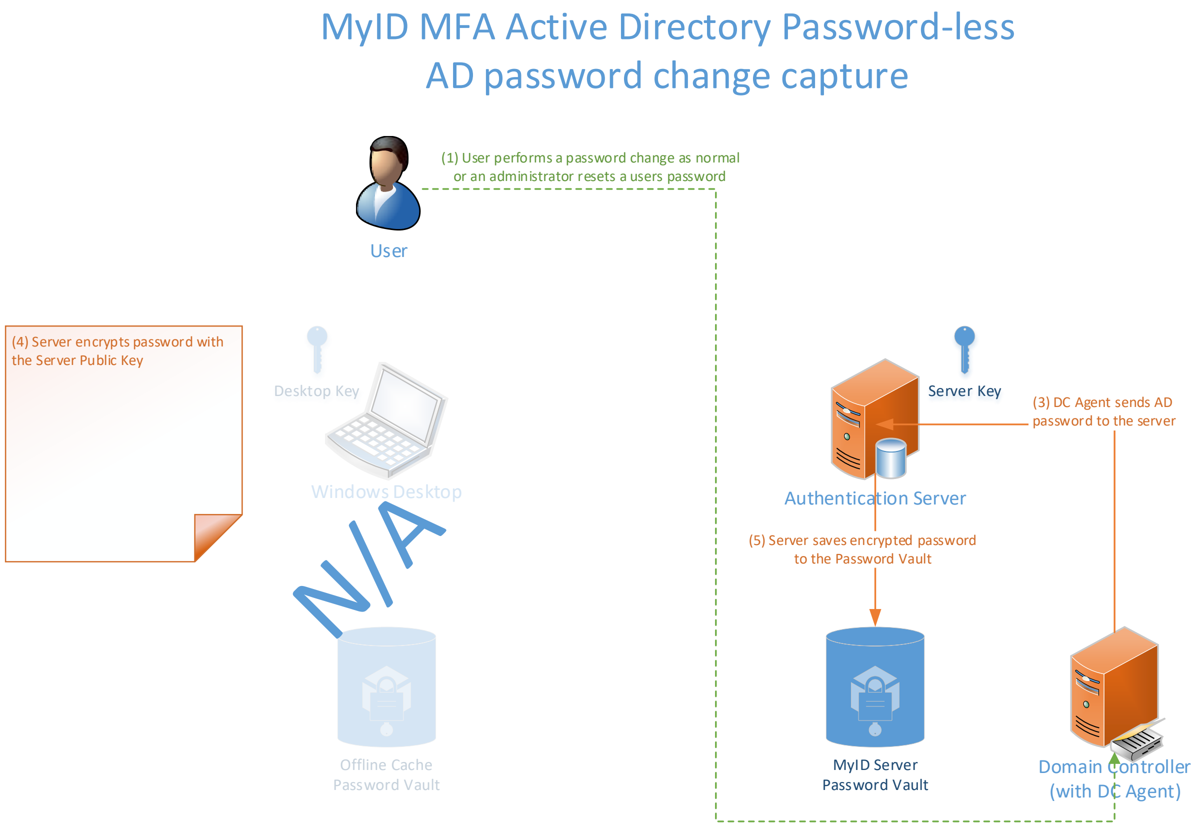

User
(1) User enters One Time Code (OTC)
(3) Server Processes and verifies the OTC
(5) Server encrypts password with the Desktop Public Key
(7) Desktop decrypts password using the Desktop Private Key
Desktop Key
Windows Desktop
(2) The OTC & Desktop Public Key sent to server
(6) Server returns encrypted password to Desktop
Server Key
MyID Authentication Server
(8) Desktop saves encrypted password to the Offline Cache
(4) Server loads password from Password Vault using the Server Private Key
Offline Cache
MyID Server Password Vault
Domain Controller
(9) OS authenticates user with Active Directory as normal

MyID MFA Windows Desktop Password-less logon process
Regular Offline logon


User
(1) User enters One Time Code (OTC)
(2) Desktop checks if the AD is Online or Offline
(4) Desktop provides the password to Windows to complete the normal offline OS logon process
Desktop Key
Windows Desktop
(3) Desktop loads password from the Offline Cache using the Desktop Private key
Offline Cache
Server Key
Authentication Server
Offline
MyID Server Password Vault
Domain Controller

The Domain Controller Agent

The Domain Controller Agent is a lightweight service designed to capture password changes made on the Windows Domain, process them against policy to see if they comply, and store them securely in the MyID Server Password Vault. This ensures that all new passwords comply with the latest NIST SP 800-63B guidance and it keeps the AD password database and the MyID Server Password Vault in sync at all times regardless of which mechanism is used to change/reset an AD password. Administrators can use DC Agent to ensure that passwords used within the environment are unique and prevent users from sharing passwords internally.


MyID MFA Active Directory Password-less
AD password change capture
User
(1) User performs a password change as normal or an administrator resets a users password
(4) Server encrypts password with the Server Public Key
Desktop Key
Windows Desktop
N/A
Offline Cache Password Vault
Server Key
Authentication Server
(3) DC Agent sends AD password to the server
(5) Server saves encrypted password to the Password Vault
MyID Server Password Vault
Domain Controller (with DC Agent)

Active Directory Permissions

The following groups will be created in the Windows Domain selected when first running the Directory Configuration Wizard. Members of the Enterprise Admins and Domain Admins group ALWAYS have full access to MyID independently of these groups. This behaviour cannot be changed due to the Active Directory security model whereby members of these groups always can take ownership of any object and change its permissions.

Group Name	Type	Members	Member Of	Provides access to...
MyID Authentication Server Administrators	Universal Group	{Installation user account}	Builtin Administrators	Full admin access to the MMC and Web Management Portal.
MyID Authentication Server Operators	Universal Group	{no members by default}	{no member of}	Limited admin access only via the Web Management Portal.
MyID Authentication Servers	Universal Group	{Authlogics server account}	Builtin Administrators	Full access to directory info.

When upgrading from V4.x Authentication Server deployments, the pre-existing Active Directory groups created originally will remain. These Active Directory security groups are:

Group Name	Type	Members	Member Of	Provides access to...
Authlogics Administrators	Universal Group	{Installation user account}	Builtin Administrators	Full admin access to the MMC and Web Management Portal.
Authlogics Operators	Universal Group	{no members by default}	{no member of}	Limited admin access only via the Web Management Portal.
Authlogics Servers	Universal Group	{Authlogics server account}	Builtin Administrators	Full access to directory info.

Note

The Built-in Administrators group has full administrator access on Domain Controllers and the Active Directory. Unlike the Domain Admins group, the Built-in Administrators group **does not** have administrator access to any member servers in the domain as it is a Domain Local security group.

For information regarding granular application of rights within AD please contact techsupport@intercede.com

For further information about AD groups and permissions see https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory

Integration with Intercede MyID CMS

Intercede MyID CMS can manage MyID Authentication Server user accounts. The integration is performed via the MyID WebAPI which must be configured prior to use.

MyID CMS must be configured to connect to the MyID Authentication Server. This enables MyID CMS to create MyID Authentication Server users, provision MFA technologies and change various account settings. Please see the MyID CMS documentation.

The MyID Authentication Server can also notify MyID CMS when an event occurs, such as a user completes setting up a new MFA device. To facilitate this configuration of MyID CMS information is required in the MyID Authentication Server.

> **Note**
>
> Intercede MyID CSM version 12.9 or higher is required for integration.

Required Information

The following information is required complete the integration.

- The MyID CMS Server URL
  - e.g. “https://myid/web.oauth2”.
- The MyID CMS Callback URL
  - e.g. “https://myid/MFABroker”.
- The MyID CMS Client ID used to authenticate
  - e.g. “myid.notifications”
- The MyID CMS Client Scope use to authenticate
  - e.g. “myid.notifications.basic”
- The MyID CMS Client Secret used to authenticate
  - e.g. “4116e8f9-92e2-48b1-8616-5fb3d130b91d”

See the Configuring MyID CMS Settings later in this document for details.

High Availability Integration

The MyID CMS settings only need to be configured on ONE MyID Authentication Server and the settings will be replicated to all the servers in the AD forest.

MyID Authentication Server works on a multi-master HA model, not Active-Passive, thus any MyID Authentication Server is able to update user account details. As such, all MyID Authentication Servers must be able to access the *MyID CMS OAuth2 Authentication Service* & *MyID CMS MFA Broker Service* URLs.

MyID CMS can be configured to use any MyID Authentication Server for configuration changes. Specifying more than one server, or using a load balanced address, is recommended.

Deployment Check List

#	Item	Check
1	A Physical or Virtual Machine to Operating System. *Recommended: Virtual Machine with 4 CPU cores and 8Gb RAM*	
2	A Windows Server 2016 or higher OS on which to install MyID Authentication Server. *Recommended: Windows Server 2019*	
3	Internet Connectivity (HTTPS) from MyID Server for licencing and activation. *Recommended: Allow the destination of https://*.authlogics.com*	
4	An administrative account with rights to install the software and configure the directory service on AD root domain. *Recommended: An Enterprise Admin or Domain Admin account*	
5	Server downtime authorisation to reboot the server post-installation.	
6	Email / SMTP server settings and credentials (if required) to allow the server to send email tokens and provisioning emails. *Recommended: Use an Exchange server with integrated authentication.*	
7	Plan the DNS name to use in the URL for the Self Service Portal which users will use to access their account. *Recommended: ssp.mycompany.com*	
8	PSM only: Plan the deployment of the password policy. Must apply to all DC's and MyID Authentication Servers. *Recommended: Use the policy defaults where possible.*	
9	Plan which MFA technology to provision users for. *Recommended: Grid Pattern Authentication as it suits the most use cases and is the most secure.*	
10	Plan if MFA devices are to be used or only deviceless authentication. *Recommended: Use MFA where high security or compliance is required, otherwise use deviceless for convenience while improving security over passwords.*	
11	Plan which MyID agents to deploy or how to integrate with 3rd party systems. *Recommended: Use industry-standard RADIUS for networking equipment and the WebAPI for application integration.*	
12	Plan which applications can use SSO / Federation (e.g. SAML 2.0, OpenID Connect, WS-Fed). *Recommended: Use MyID IdP services or Microsoft ADFS with the MyID ADFS Agent is still supported.*	

Multi-Factor Authentication Technology

Background

As the usage of Information Technology has increased exponentially, the need for security of these systems has increased proportionately. Traditionally, authenticating users was solely performed by the user providing a valid username and password. This is known as single-factor authentication as the user “knows” all parts of the authentication process. Passwords have proven to be unsecure and therefore additional authentication factors have become a requirement.

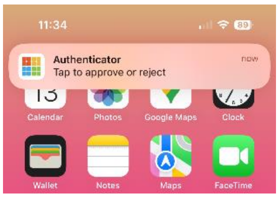
The increase of security provided by multi-factor (typically 2-factor) is that users must now “have something” and “know something” in the authentication process. The “have something” usually takes the form of a physical hardware device, like a key fob, which generates a specific unique One Time Pin (OTP). This OTP must also be entered as part of the authentication process.

Although these hardware token devices have improved security significantly, they do have certain limitations and incur a costing overhead in both their implementation as well as on-going maintenance. Furthermore, they typically still need to be used together with a password and don’t provide a path towards Passwordless logons.

Intercede provides a multitude of hardware and software-based authentication technologies and delivery mechanisms to suit many scenarios, all while keeping down the logistical overhead of hardware tokens down.

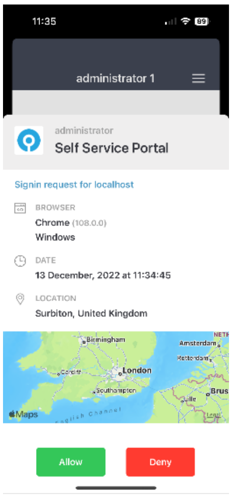
Mobile Push Authentication Technology

MyID Mobile Push is designed to simply send a notification to a user’s phone to authenticate. Once the notification is tapped the Authlogics Authenticator app loads and the user may be required to authenticate with biometrics.



11:34

Authenticator
Tap to approve or reject
now



11:35

administrator 1

administrator
Self Service Portal

Signin request for localhost

BROWSER
Chrome (108.0.0)
Windows

DATE
13 December, 2022 at 11:34:45

LOCATION
Surbiton, United Kingdom

The user is presented with information about the logon and can choose to Allow or Deny the request.

If the user taps Allow then the application they were trying to access will complete its logon process.

However, if the user taps Deny they will be asked why which is recorded on the MyID Authentication Server. If they stated they did not make this logon request then the server will track future logon attempts and automatically throttle sending new Push requests to prevent “MFA fatigue”.

MyID Mobile Push helps to mitigate typical Push vulnerabilities:

- MFA fatigue protection:
  - Require an initial offline logon for untrusted browser connections.
  - Dynamic throttling for legacy (e.g. RADIUS) / none-browser channels when a Denied logon is recorded by the user.
- Does not send any OTP or secret information via Apple or Google servers, thus it cannot be tampered with in transit.
- Authlogics App will respond to a logon request when open even if a network “Push” is not received via Apple or Google to prevent denial of service attacks or network delays.

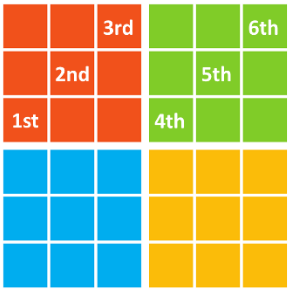
Grid Pattern Technology

Grid Pattern authentication technology (formerly known as PINgrid) mitigates the security limitations of the traditional OTP tokens by generating a One Time Code derived from a grid of numbers. These grids are specific to each user and change every minute reflecting different numbers. The additional security of Grid Pattern is that the user also needs to know a unique pattern to extrapolate an OTP.

To thwart automated brute force attacks, MyID includes “Account Lockout” functionality where a user’s account is locked out either indefinitely or for a pre-configured period when a passcode is entered incorrectly after several times. Grid Pattern authentication even mitigates the threat of keylogging, screen scraping and shoulder surfing attacks.

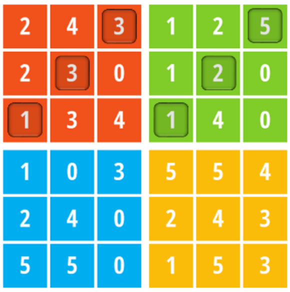
Grid Pattern authentication is available in 1, 2 and 3-Factor Authentication methodologies. Grids can be views within an app, on a web page, sent via TEXT/SMS or email, or used offline via the Authlogics Authenticator in the App Store.

How it works?



		3rd			6th
	2nd			5th	
1st			4th		

User pattern



2	4	3	1	2	5
2	3	0	1	2	0
1	3	4	1	4	0
1	0	3	5	5	4
2	4	0	2	4	3
5	5	0	1	5	3

Pattern on a challenge grid

One Time Code is: *133125*

In a ‘Prove it!’ situation the pattern is used with a challenge grid

- A One Time Password (OTP) is hidden in the grid
- Only the person who knows the secret pattern can ‘see’ the OTP

Finally, Grid Pattern authentication technology is truly a One Time Pin authentication solution as all valid passcodes entered can be used only once, even if the authentication attempt occurs within the same period from the same device.

Phrase Technology

Phrase authentication (formerly known as PINphrase) uses a few authentication methods which have become a de facto standard in the banking industry to provide a simple to use but efficient and cost-effective solution.

Phrase authentication is based upon a passphrase question and answer system which prompts the user to enter random characters from the answer to a randomly chosen question. Unlike passwords, the answers to the questions are typically things that the user is not likely to forget which reduces helpdesk calls, limits resets and further cuts costs. Since the user is only ever entering part of the answer, e.g. letters 2, 5 and second last character. During each login the user is asked to enter different letters, and from different answers, making the response a One Time Code. The full answer is not revealed during the login, this makes Phrase authentication ideal for both a deviceless and Multi-Factor Authentication. Phrase authentication can also be configured to randomly select letters from different questions to further enhance security.

An administrator can configure multiple common questions for things users will generally know an answer for and can then specify how many of the questions a user must provide an answer for, e.g. the user must provide answers for at least 4 of the 10 supplied questions. By default, a user is assigned a Codeword which is a randomly chosen dictionary word which can be used for first login.

Scenarios

A new user called Bob Jones is enabled and his mobile phone details are recorded. He then provides answers to at least 6 questions from a pool, he chooses the following:

Place of birth?	Seattle
Pets name?	Tigger
Memorable place?	Springfield
Mother's maiden name?	Watson
Memorable date and time (YYYYMMDDHHMM)	201101021937
First school?	Winchester

Authentication Scenario #1 - Deviceless Authentication

Bob wants to logon to an Internet banking site. He types in his Username and is then presented with a question from the answered pool and is asked to enter specific characters from the answer.

```
Please provide the 1st, 3rd, 4th and the last characters from your
memorable place.
```

To authenticate, Bob will enter `S R I D`.

Authentication Scenario #2 – Multi-Factor Authentication

This requires a physical device on which Bob will receive the question and random positions, i.e. the soft token. Typically, this device is a mobile phone as the mobile phone number is unique to the user.

Bob accesses the logon page of his internet banking site and types in his username. Once Bob enters his Username, the Phrase authentication server detects that the logon process for Bob has started. A challenge will be generated and sent as an SMS/Text message to Bob's mobile device as follows:

```
Phrase: Please provide the 2nd, 3rd, 5th and penultimate characters
from your place of birth.
```

To authenticate, Bob will enter `A L S R`.

A key part of MyID Phrase authentication is that both the deviceless and Multi-Factor methods have an identical look and feel to the user with the only difference being where the challenge message is displayed.

In cases where mobile phone reception cannot be guaranteed and instant message retrieval may not always be possible, Phrase authentication can Pre-send tokens. Pre-sending tokens ensure that the user always has a token on his/her device prior to the authentication attempt. As soon as the token is used, then the next token is sent to the user's mobile device ready to be used for the next login.

One Time Code Technology

MyID One Time Code (formerly known as PINpass) is an OATH RFC compliant 2-factor authentication solution which utilises soft tokens to reduce the costs associated with hardware key fobs. One Time Code OTPs are delivered to mobile phones via SMS text messages or as an email for even more flexibility and cost savings.

One Time Code gives administrators the ability to pre-send one or more OTP's so that the user always has an OTP on their mobile device before logging on. As soon as the last OTP is used, then a new set of OTPs are sent to the user ready for future logon attempts. Alternatively, One Time Code can be used offline via the Authlogics Authenticator in the App Store.

To increase security and convenience, administrators can configure users to provide an Active Directory password or static PIN with the One Time Pin. A static pin can be entered, before, after or even in the middle of the OTP code making it more difficult for a key logger to differentiate between the OTC code and the user's static PIN.

When a user is configured with a real-time token and attempts to login, they enter their unique login name and One Time Code sends a 6 to 8 digit OTP to their mobile phone via SMS or email address. The user then enters the OTC along with either their AD password or a static PIN, depending on the configuration.

The login process is similar for a user who is configured with a pre-send token except that a code is not sent to the user after they enter their username as they will already have a code on their phone. Instead, a new code is only sent after they login for use during the next login.

Standard OATH TOTP

MyID MFA supports standard software OATH tokens such as the Microsoft and Google Authenticator apps. With this, users will no longer be required to download the MyID Authenticator App (Authlogics Authenticator app) and can add MyID MFA to their Microsoft and Google Authenticator app profile.

As with the MyID OTC solution, standard OATH authenticators utilises soft tokens to reduce the costs associated with hardware key fobs. One Time Code OTPs are generated on the mobile phones out-of-band without the need for the mobile device to have signal or sufficient data.

As with other MyID MFA technologies, Standard OATH support extends to offline logins for our MyID Authentication agents.

YubiKey OTP

If hardware tokens are required, MyID supports YubiKey OTP tokens from Yubico. YubiKey OTP tokens are USB devices that do not have a battery, do not expire and work with any OS.

To increase security and convenience, administrators can configure users to provide an Active Directory password or static PIN with the YubiKey token. A static pin can be entered, before generating the YubiKey OTP code to ensure that the multi-factor requirements are satisfied with the “something I have” (YubiKey token) and “something I know” (static PIN).

FIDO Passkeys for the Enterprise

Passkeys are based on the FIDO standard and enable cryptography-based phishing-resistant authentication. By combining high security with a passwordless user experience Passkeys are revolutionising the consumer authentication experience.

However, it has been difficult for enterprises to gain the benefits Passkey-based authentication brings, as by design they do not enable the level of management and integration enterprises require.

By bringing enterprise managed FIDO passkeys into the MyID MFA product, organisations can now easily FIDO-enable multiple applications and deploy passkeys to end users enhancing security and improving the user experience

MyID MFA acts as both a FIDO authentication server and a passkey issuance solution. End users authenticate to MyID MFA with their passkey, and by support for standard federated identity protocols, MyID MFA provides authentication services to multiple applications including cloud, on-premise and Windows desktop logon.

There are two type of Passkeys, both of which are supported by MyID MFA, enabling customers to choose the best balance of security and costs that fits their particular needs:

Synch-able Passkeys: use an existing mobile phone to protect the private key used in the authentication process. Able to communicate over the FIDO protocol built into multiple devices and web browsers, the phone simply acts as the user's security token and the user accesses the protected private key via fingerprint, face ID or PIN, delivering secure, passwordless authentication with a simple user experience.

Synch-able passkeys can be backed up and restored using the mobile operating system's built in mechanisms such as iCloud. This effectively deals with lost or replacements devices without having to reissue credentials.

Device Bound Passkeys: for organisations wanting higher levels of security and control over where passkeys are, MyID MFA also support device-bound passkeys such as those stored on a USB authenticator like a YubiKey. Device-bound passkeys never leave the device, resulting in the highest levels of phishing resistance.

MyID MFA supports the innovative YubiKey Bio device, enabling users to replace a PIN with a simple match of a fingerprint, delivering a seamless authentication experience while maintaining the highest level of security

Authentication Technology vs Factor type

Technology	Knowledge	Possession	Inherent
Password (NIST)	X		
Grid Authentication	X	X	X
Phrase Authentication	X	X	
One Time Code	X	X	X
Push		X	X
Standard OATH		X	
YubiKey OTP	X	X	
Passkey/FIDO2		X	X

Automatic MFA Determination and SSO Assurance Levels

MyID MFA allows for users to be provisioned for multiple MFA technologies at once. Applications Logon Technology can be set to ***Automatic*** MFA which determines the most appropriate technology that the user is capable to authenticate with.

Coupled to this, MyID MFA also provides Single Sign On (SSO) capabilities across applications. This means that a user can authenticate to one application and will not be required to re-authenticate to other applications. As each application can be configured with its own MFA assurance level, it is feasible that users will authenticate to an application with a lower-level assurance level than another application. MyID MFA provides conditional SSO where SSO is allowed provided the application being accessed has the same or lower assurance level than the application a user original authenticated to. If an application has a higher-level of assurance than the original authenticated to, then the user will need to authenticate to this application with the higher-level assurance MFA technology.

The following table details the MyID MFA automatic logon technology and assurance levels hierarchy:

Hierarchy
FIDO / Passkey
Grid Multi-Factor Authentication
Push
YubiKey One Time PIN
One Time Code
Phrase Multi-Factor Authentication
Grid Deviceless
Phrase Deviceless
AD Password (Not applicable to Realm users)

Federation Server

Federation brings the ability to share identity and authentication information between systems in a managed way. By supporting standards-based protocols such as OpenID Connect and SAML, MyID MFA can easily add stronger authentication to a range of applications be they cloud based or on-premises.

By supporting the widest range of authentication options from OTP over SMS, through pass phrases, OTP generation via App, push-notifications and FIDP passkeys, organisations can introduce a single means of strong authentication to project multiple applications or mix and match technologies as best fits their security needs and deployment scenario.

Building Identity provider capabilities into the MFA solution, not only supports federation, but also delivers a unified authentication experience across the entire application suite, including authentication to application, logging on to the windows desktop, accessing the self-service portal and resetting credentials such as passwords. A simplified and consistent authentication process improves the user experiences and reduces the likelihood of a call to the help desk.

ADFS replacement

Microsoft ADFS (Active Directory Federation Services) has been the mainstay of many organisations looking to add secure authentication to multiple applications in a Microsoft-centric environment. With the move to Microsoft Entra based solutions a number of organisations are finding themselves looking for an alternative that is simpler to deploy and provides support for both cloud and legacy on-premises applications as well as securing the Windows Desktop logon and Microsoft 365.

The federated identity provider (IDP) capabilities MyID MFA delivers, provides a modern and easy to alternative to ADFS. By supporting a wide range of authenticators, include FIDO passkeys, and standard protocols such as OpenID Connect and SAML 2.0, MyID MFA is a natural successor to ADFS.

Deployment

The following deployment overview walks through the installation process for deploying an MyID Authentication Server.

Overview

To fully deploy the MyID Authentication Server:

(1) Install the Authentication Server on a Windows Server.

(2) Provision users in the MyID Directory.

(3) Install Plug-ins, configure 3rd party integrations or setup RADIUS clients. MyID plug-ins have separate Integration guides which should be followed.

(4) Create Applications for Federated App support

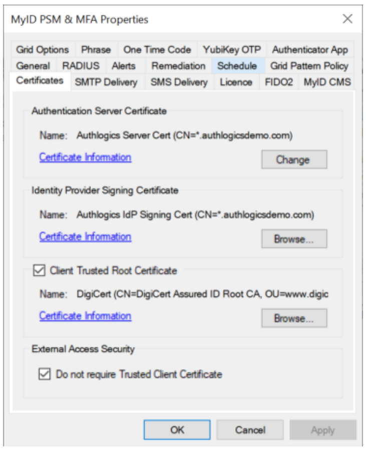
(5) Optional: Deploy additional Authentication Servers for High Availability.

High Availability and Certificates

The Authentication Server installer will automatically generate an MyID Server Certificate which is used for encrypting data sorted in the directory. In addition, the installer will create a MyID SSL Certificate which is used by IIS for encrypting web traffic in transit.

Prior to installing an additional MyID Authentication Server, the MyID Server Certificate must be exported from the primary MyID Authentication Server with its private key and imported onto the additional server. Until this is done, the additional Authentication Server will not be able to access encrypted data stored in the directory.

To verify which certificate is being used on an existing Authentication Server and Identity Provider Signing certificates check the certificates tab in the MyID Management Console:



Authentication Server Certificate

Name: Authlogics Server Cert (CN=*.authlogicsdemo.com)

Identity Provider Signing Certificate

Name: Authlogics IdP Signing Cert (CN=*.authlogicsdemo.com)

☑ Client Trusted Root Certificate

Name: DigiCert (CN=DigiCert Assured ID Root CA, OU=www.digic

External Access Security

☑ Do not require Trusted Client Certificate

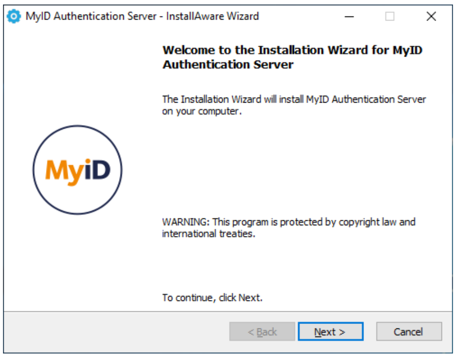
Follow the Certificate Export and Import section later in this guide for setup by step details.

Installing MyID Authentication Server

The MyID Authentication Server is responsible for processing logon requests and other core activities. This MyID Authentication Server should be set up before any other component.

> **Note**
>
> This section of the installation process requires Local Administrator rights on the server. Domain rights are not required at this stage.

1. To start the MyID Authentication Server installation, run the *MyID Authentication Server xxxxx.exe* installer. Click *Next* to automatically uninstall the previous version.



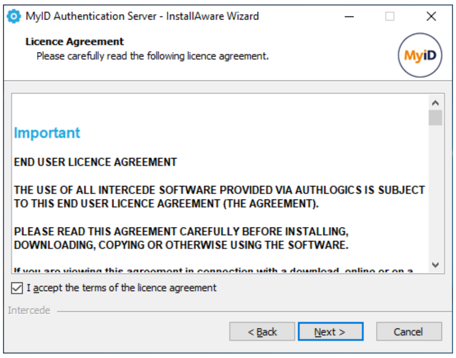
Welcome to the Installation Wizard for MyID Authentication Server

The Installation Wizard will install MyID Authentication Server on your computer.

WARNING: This program is protected by copyright law and international treaties.

To continue, click Next.

2. Click *Next* to continue.



Licence Agreement

Please carefully read the following licence agreement.

Important

END USER LICENCE AGREEMENT

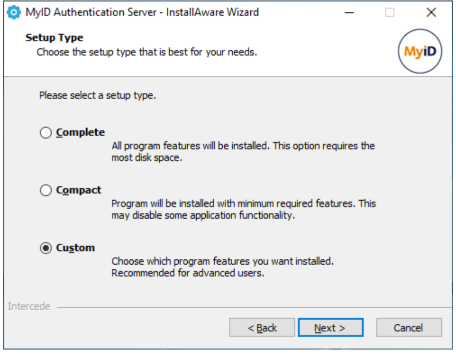
THE USE OF ALL INTERCEDE SOFTWARE PROVIDED VIA AUTHLOGICS IS SUBJECT TO THIS END USER LICENCE AGREEMENT (THE AGREEMENT).

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE SOFTWARE.

If you are viewing this agreement in connection with a download, online or on a

☑ I accept the terms of the licence agreement

After **reading** the licence agreement click *I accept the terms in the terms in the Licence Agreement* if you agree to the terms, then click *Next* to continue.



Setup Type

Choose the setup type that is best for your needs.

Please select a setup type.

○ **Complete**

All program features will be installed. This option requires the most disk space.

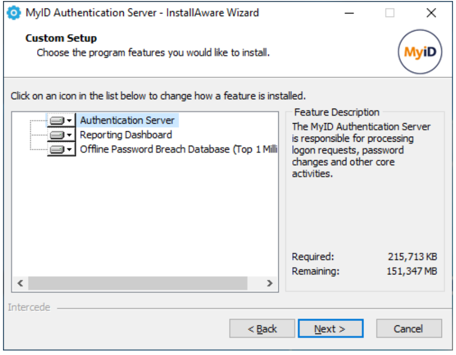
○ **Compact**

Program will be installed with minimum required features. This may disable some application functionality.

● **Custom**

Choose which program features you want installed. Recommended for advanced users.

Select the *Custom* setup type and select *Next* to continue.



Custom Setup

Choose the program features you would like to install.

Click on an icon in the list below to change how a feature is installed.

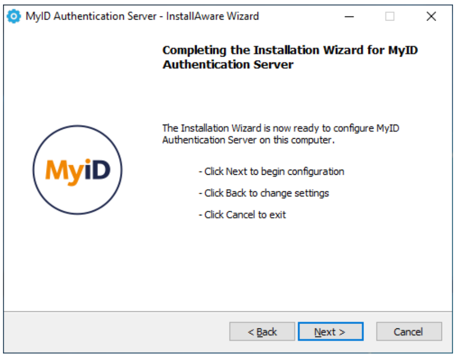
- Authentication Server
- Reporting Dashboard
- Offline Password Breach Database (Top 1 Milli

Feature Description

The MyID Authentication Server is responsible for processing logon requests, password changes and other core activities.

Required:	215,713 KB
Remaining:	151,347 MB

3. As a minimum ensure to select the *Authentication Server core* and the *Authentication Server Management Console* features for installation. Click *Next* to continue.


MyID Authentication Server - InstallAware Wizard

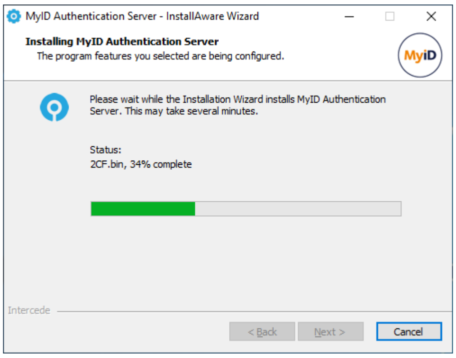
Completing the Installation Wizard for MyID Authentication Server

The Installation Wizard is now ready to configure MyID Authentication Server on this computer.

- Click Next to begin configuration
- Click Back to change settings
- Click Cancel to exit

4. Click *Next* to continue.

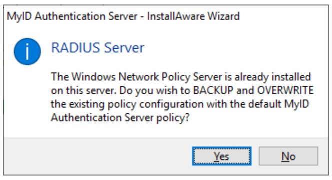
The installation is being performed.


MyID Authentication Server - InstallAware Wizard

Installing MyID Authentication Server
The program features you selected are being configured.

Please wait while the Installation Wizard installs MyID Authentication Server. This may take several minutes.

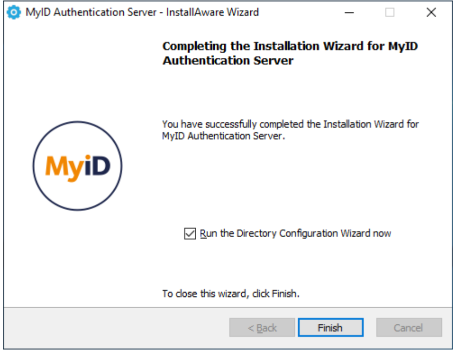
Status:
2CF.bin, 34% complete


MyID Authentication Server - InstallAware Wizard

RADIUS Server

The Windows Network Policy Server is already installed on this server. Do you wish to BACKUP and OVERWRITE the existing policy configuration with the default MyID Authentication Server policy?

If prompted to overwrite the existing NPS policy click *Yes*.


MyID Authentication Server - InstallAware Wizard

Completing the Installation Wizard for MyID Authentication Server

You have successfully completed the Installation Wizard for MyID Authentication Server.

☑ Run the Directory Configuration Wizard now

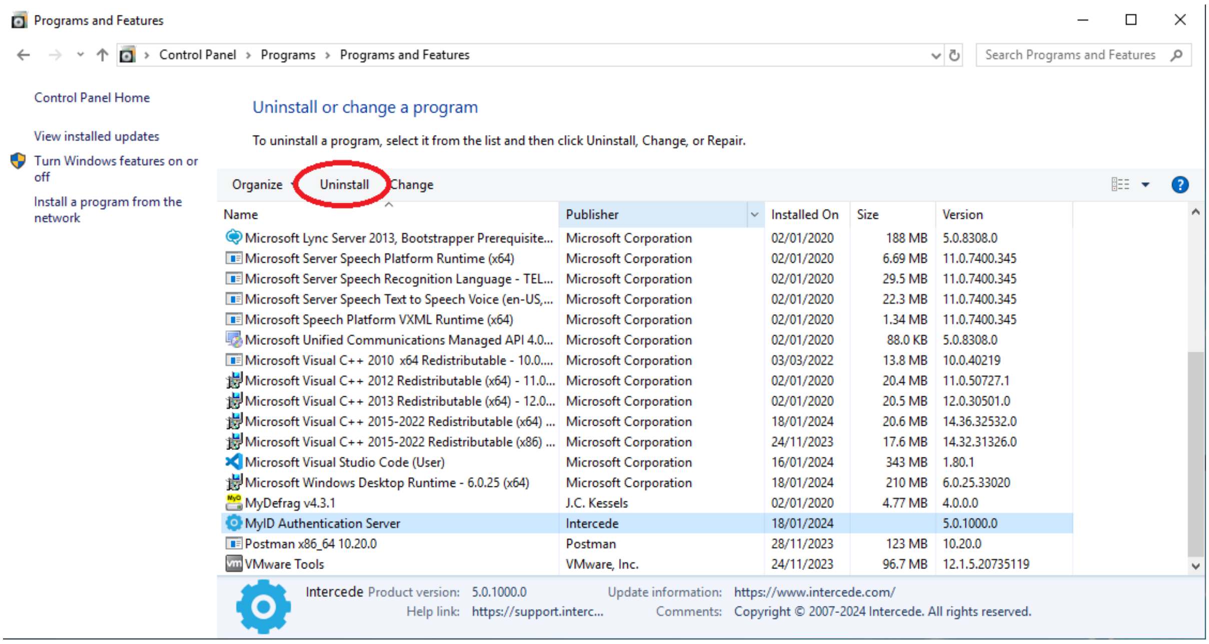
To close this wizard, click Finish.

5. All necessary MyID Authentication Server files have been installed on your server. Select *Run the Directory Configuration Wizard now* if you wish to set up the directory immediately.

   Click *Finish* to complete the installation process.

Uninstalling MyID Authentication Server

If you no longer require MyID Authentication Server on a server, you can remove it by performing an uninstall from Control Panel > Programs > Programs and Features:


Programs and Features
Control Panel > Programs > Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize
Uninstall
Change

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Installed On	Size	Version
Microsoft Lync Server 2013, Bootstrapper Prerequisite...	Microsoft Corporation	02/01/2020	188 MB	5.0.8308.0
Microsoft Server Speech Platform Runtime (x64)	Microsoft Corporation	02/01/2020	6.69 MB	11.0.7400.345
Microsoft Server Speech Recognition Language - TEL...	Microsoft Corporation	02/01/2020	29.5 MB	11.0.7400.345
Microsoft Server Speech Text to Speech Voice (en-US,...	Microsoft Corporation	02/01/2020	22.3 MB	11.0.7400.345
Microsoft Speech Platform VXML Runtime (x64)	Microsoft Corporation	02/01/2020	1.34 MB	11.0.7400.345
Microsoft Unified Communications Managed API 4.0...	Microsoft Corporation	02/01/2020	88.0 KB	5.0.8308.0
Microsoft Visual C++ 2010 x64 Redistributable - 10.0....	Microsoft Corporation	03/03/2022	13.8 MB	10.0.40219
Microsoft Visual C++ 2012 Redistributable (x64) - 11.0...	Microsoft Corporation	02/01/2020	20.4 MB	11.0.50727.1
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0...	Microsoft Corporation	02/01/2020	20.5 MB	12.0.30501.0
Microsoft Visual C++ 2015-2022 Redistributable (x64) ...	Microsoft Corporation	18/01/2024	20.6 MB	14.36.32532.0
Microsoft Visual C++ 2015-2022 Redistributable (x86) ...	Microsoft Corporation	24/11/2023	17.6 MB	14.32.31326.0
Microsoft Visual Studio Code (User)	Microsoft Corporation	16/01/2024	343 MB	1.80.1
Microsoft Windows Desktop Runtime - 6.0.25 (x64)	Microsoft Corporation	18/01/2024	210 MB	6.0.25.33020
MyDefrag v4.3.1	J.C. Kessels	02/01/2020	4.77 MB	4.0.0.0
MyID Authentication Server	Intercede	18/01/2024		5.0.1000.0
Postman x86_64 10.20.0	Postman	28/11/2023	123 MB	10.20.0
VMware Tools	VMware, Inc.	24/11/2023	96.7 MB	12.1.5.20735119

Intercede Product version: 5.0.1000.0 Update information: https://www.intercede.com/
Help link: https://support.interc... Comments: Copyright © 2007-2024 Intercede. All rights reserved.

Active Directory metadata

Uninstalling MyID does NOT remove the metadata from user accounts in the Active Directory. If you are planning to completely remove MyID from your environment you should delete all user accounts via the MMC prior to uninstalling – this does NOT delete the actual AD user account, it simply removes all MyID information from it.

For detailed information about MyID AD metadata see Authlogics KB207256965 (https://support.authlogics.com/hc/en-us/articles/207256965).

Installing a new version of MyID Authentication Server

Updates vs Upgrades

A product Update is a minor new version designed to fix specific known issues in the product and introduce some new features. Updates are typically low risk to deploy and are designed to be a simple in-place update. Updates are released regularly and may be skipped if changes in the update are not required. Check the readme.txt for the update to see the changelog.

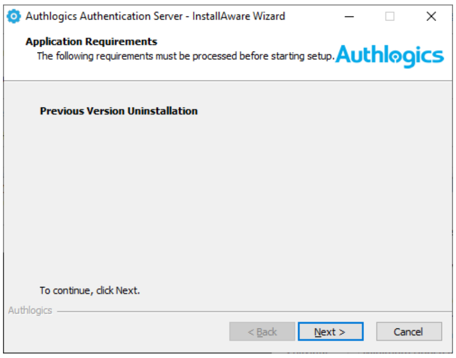
A product Upgrade is a major new version which will include fixes but is mainly designed to deliver new features and functionality. Upgrades are not released regularly. Upgrades may require additional planning before they are installed. Always review the Installation and Configuration Guide of the new version before upgrading.

Installing an Update

The installation program of an Update can be used for a full clean install, or to perform an in-place update of an existing installation.

The installation process is almost identical to performing a new installation. Once installed, the Directory Configuration Wizard must be run for the server to be used after the update. For PSM deployments, ensure that the Password Security Management wizard is rerun after an upgrade. All directory settings, registry settings and supported web portal customisations are retained during an update.

1. To start the MyID Authentication Server installation, run the *MyID Authentication Server xxxxx.exe* installer.



Authlogics Authentication Server - InstallAware Wizard

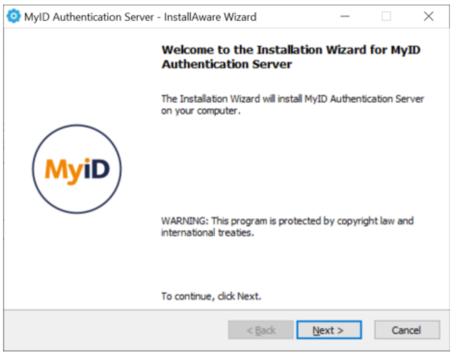
Application Requirements

The following requirements must be processed before starting setup.

Previous Version Uninstallation

To continue, click Next.

2. Click *Next* to automatically uninstall the previous version.



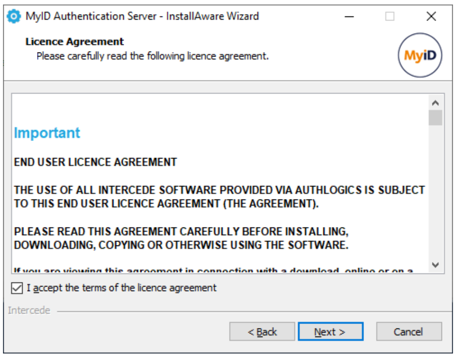
Welcome to the Installation Wizard for MyID Authentication Server

The Installation Wizard will install MyID Authentication Server on your computer.

WARNING: This program is protected by copyright law and international treaties.

To continue, click Next.

3. Click *Next* to continue.



Licence Agreement

Please carefully read the following licence agreement.

Important

END USER LICENCE AGREEMENT

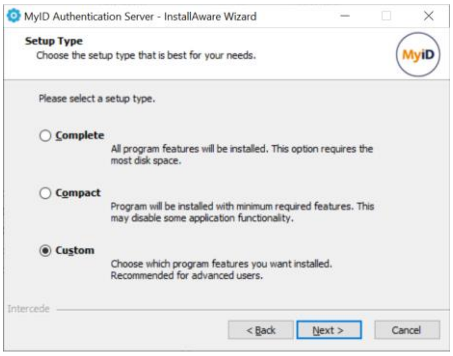
THE USE OF ALL INTERCEDE SOFTWARE PROVIDED VIA AUTHLOGICS IS SUBJECT TO THIS END USER LICENCE AGREEMENT (THE AGREEMENT).

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE INSTALLING, DOWNLOADING, COPYING OR OTHERWISE USING THE SOFTWARE.

If you are viewing this agreement in connection with a download, online or on a

☑ I accept the terms of the licence agreement

4. After **reading** the licence agreement click *I accept the terms in the terms in the Licence Agreement* if you agree to the terms, then click *Next* to continue.



Setup Type

Choose the setup type that is best for your needs.

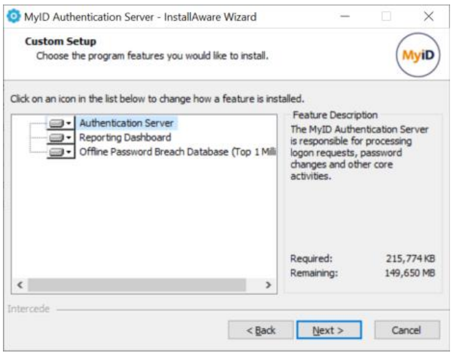
Please select a setup type.

○ Complete
All program features will be installed. This option requires the most disk space.

○ Compact
Program will be installed with minimum required features. This may disable some application functionality.

● Custom
Choose which program features you want installed. Recommended for advanced users.

5. Select the *Custom* setup type and select *Next* to continue.



Custom Setup

Choose the program features you would like to install.

Click on an icon in the list below to change how a feature is installed.

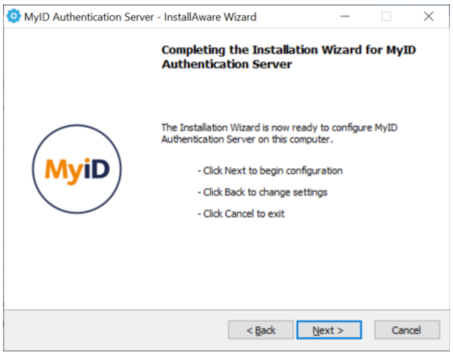
- Authentication Server
- Reporting Dashboard
- Offline Password Breach Database (Top 1 Milli

Feature Description

The MyID Authentication Server is responsible for processing logon requests, password changes and other core activities.

Required:	215,774 KB
Remaining:	149,650 MB

6. As a minimum ensure to select the *Authentication Server core* and the *Authentication Server Management Console* features for installation. Click *Next* to continue.



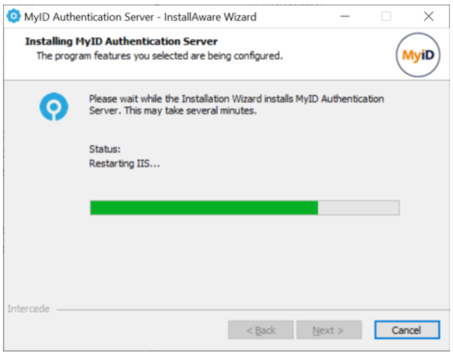
Completing the Installation Wizard for MyID Authentication Server

The Installation Wizard is now ready to configure MyID Authentication Server on this computer.

- Click Next to begin configuration
- Click Back to change settings
- Click Cancel to exit

7. Click *Next* to continue.

The installation is being performed.

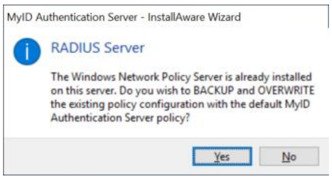


Installing MyID Authentication Server

The program features you selected are being configured.

Please wait while the Installation Wizard installs MyID Authentication Server. This may take several minutes.

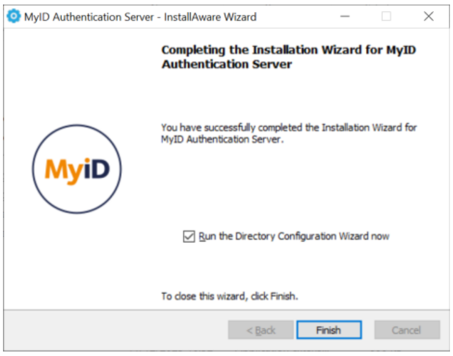
Status:
Restarting IIS...



RADIUS Server

The Windows Network Policy Server is already installed on this server. Do you wish to BACKUP and OVERWRITE the existing policy configuration with the default MyID Authentication Server policy?

8. When prompted to overwrite the existing NPS policy click *No*.



Completing the Installation Wizard for MyID Authentication Server

You have successfully completed the Installation Wizard for MyID Authentication Server.

☑ Run the Directory Configuration Wizard now

To close this wizard, click Finish.

9. All necessary MyID Authentication Server files have been installed on your server. Select *Run the Directory Configuration Wizard now* if you wish to set up the directory immediately.

   Click *Finish* to complete the installation process.

Upgrading from Version 4.2

MyID Authentication Server 5.0 supports upgrading from version 4.0 and higher. To upgrade from 3.x you must first upgrade to 4.1 (not 4.2), and then to 5.0, there is no direct upgrade path.

> **Important –Windows Desktop Agent**
>
> If the Authlogics Desktop Logon Agent version 4.x is deployed the **Windows Desktop Agent MUST be upgraded to version 5.0 before the MyID Authentication Server is upgraded**. The Windows Desktop Agent 5.0 is backwards compatible with version 4.x Authentication servers. See the Authlogics Windows Desktop Agent Integration Guide for further details.

Process overview:

(1) If multiple MyID Authentication Servers running 4.2 are deployed then all but one server must be uninstalled.

(2) On the last remaining MyID Authentication Server run the setup for version 5 to in-place upgrade the server. This will automatically remove version 4.2.

(3) Complete the Directory Configuration Wizard to upgrade the version 4.2 user metadata.

(4) For PSM upgrades, complete the Password Security Management wizard to upgrade version 4.2 PSM metadata.

(5) Review the MyID Authentication Server settings, noting new features which may be required.

(6) Test user logons and general functionality post upgrade.

(7) Deploy additional MyID Authentication Servers if needed.

   a. Review the *Certificate Export and Import* section of this document prior to installing additional MyID Authentication Servers.

Certificate Export and Import

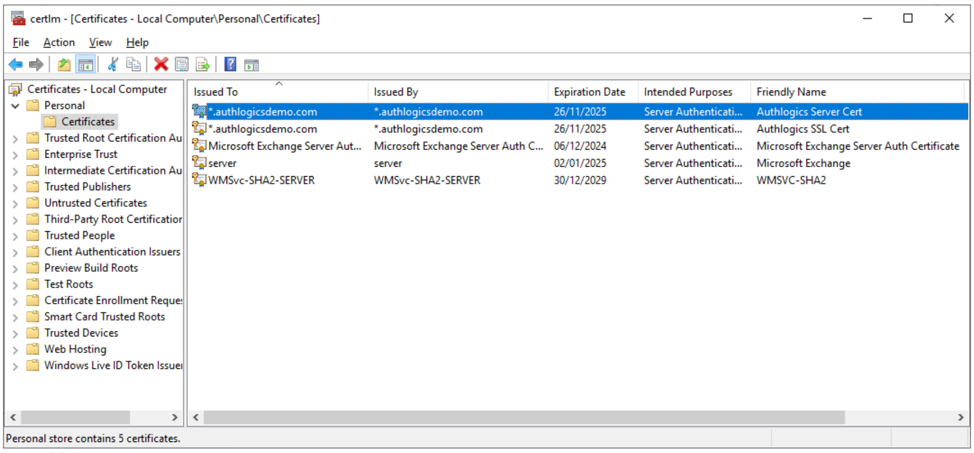
This section details the process of exporting the MyID Authentication Server directory encryption and Identity Provider certificates to a file so it can be imported onto another server where the MyID Authentication Server software will be installed.

Export the IdP Signing Cert

The following documents the process to export the directory encryption certificate; this process must be repeated for the IdP Signing certificate.

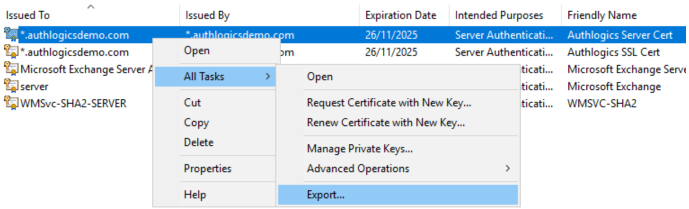
Export Certificate from existing MyID Authentication Server

1. To start the Certificate MMC, run *certlm.msc*.

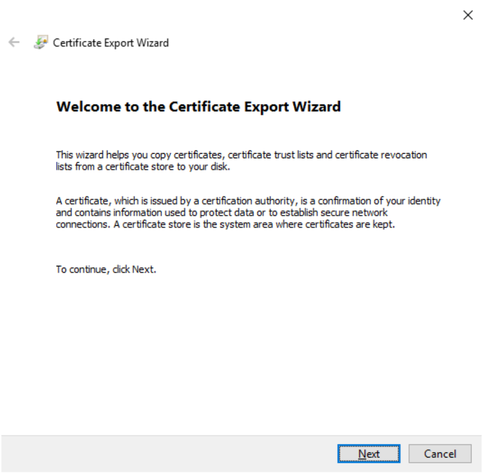

certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
*.authlogicsdemo.com	*.authlogicsdemo.com	26/11/2025	Server Authenticati...	Authlogics Server Cert
*.authlogicsdemo.com	*.authlogicsdemo.com	26/11/2025	Server Authenticati...	Authlogics SSL Cert
Microsoft Exchange Server Aut...	Microsoft Exchange Server Auth C...	06/12/2024	Server Authenticati...	Microsoft Exchange Server Auth Certificate
server	server	02/01/2025	Server Authenticati...	Microsoft Exchange
WMSvc-SHA2-SERVER	WMSvc-SHA2-SERVER	30/12/2029	Server Authenticati...	WMSVC-SHA2

Personal store contains 5 certificates.



2. Right-click the MyID Server Certificate (or IdP Signing Certificate) being used, select *All Tasks*, *Export...*



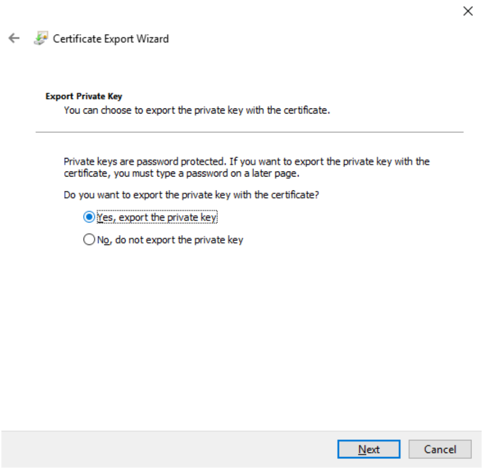
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

3. Click *Next* to continue.



Export Private Key
You can choose to export the private key with the certificate.

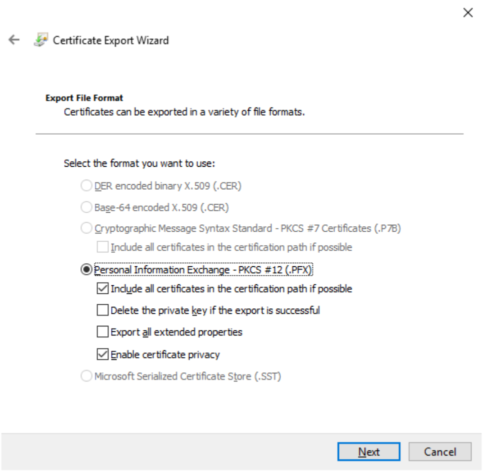
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

4. Select *Yes, export the private key* and click *Next* to continue.



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

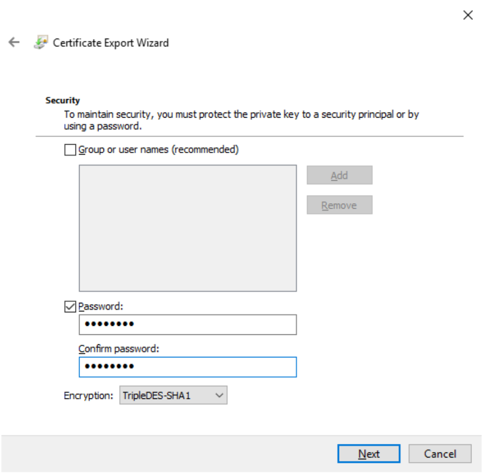
- □ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

- ☑ Include all certificates in the certification path if possible
- □ Delete the private key if the export is successful
- □ Export all extended properties
- ☑ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

5. Click *Next* to continue.



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

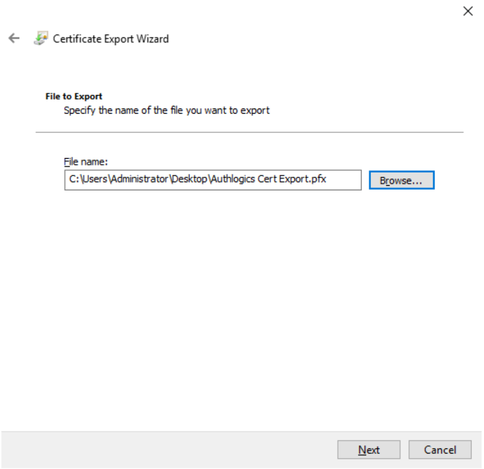
☐ Group or user names (recommended)

☑ Password:
••••••••

Confirm password:
••••••••

Encryption: TripleDES-SHA1

6. Select *Password* and enter a password twice to confirm. Click *Next* to continue.



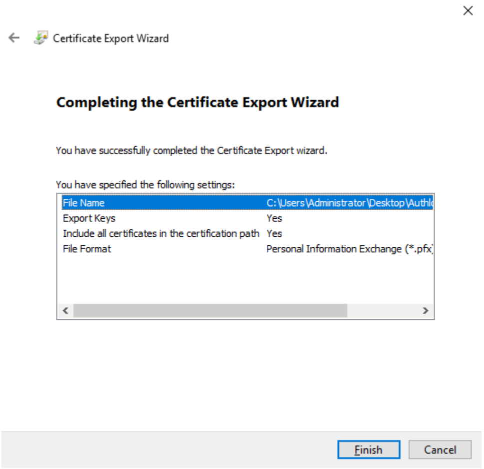
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:
C:\Users\Administrator\Desktop\Authlogics Cert Export.pfx

7. Enter a file name to export to. Click *Next* to continue.



Certificate Export Wizard

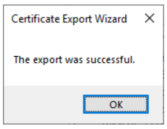
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Desktop\Authl
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx

8. Click *Finish*.



Certificate Export Wizard

The export was successful.

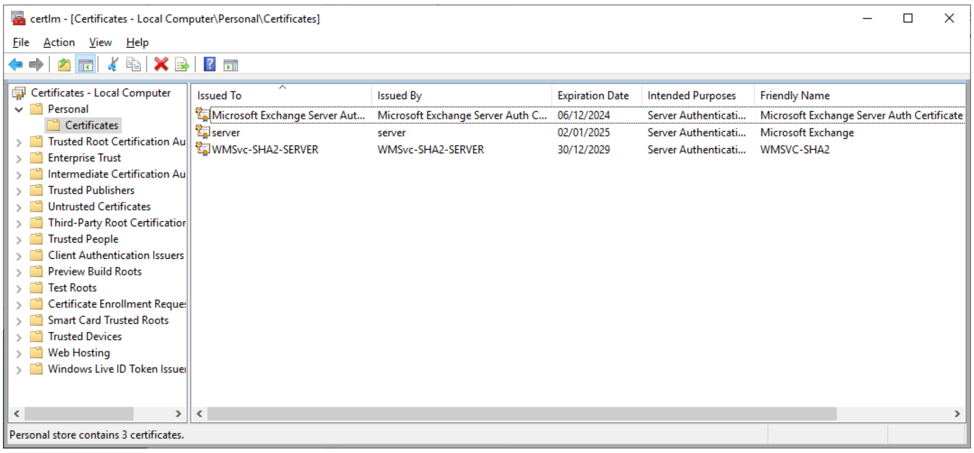
9. Click *Ok* to close the wizard.

Import Certificate to new MyID Authentication Server

Importing the IdP Signing Cert

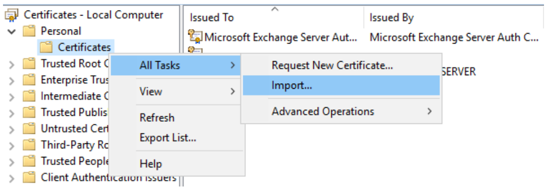
As with the export of the certificates, this process will need to be followed for both the Authenticate Server encryption and IdP Signing certificates.

1. To start the Certificate MMC, run *certlm.msc*.

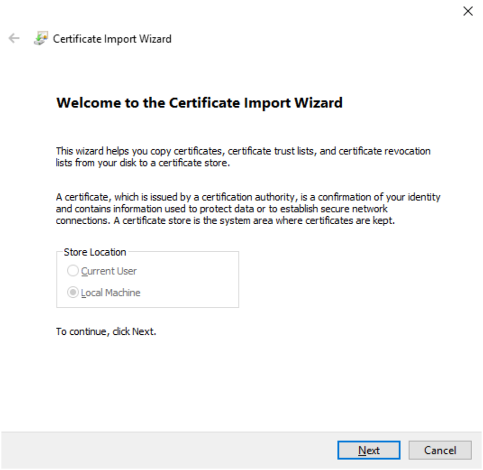

certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Certificate Enrollment Reque
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
Microsoft Exchange Server Aut...	Microsoft Exchange Server Auth C...	06/12/2024	Server Authenticati...	Microsoft Exchange Server Auth Certificate
server	server	02/01/2025	Server Authenticati...	Microsoft Exchange
WMSvc-SHA2-SERVER	WMSvc-SHA2-SERVER	30/12/2029	Server Authenticati...	WMSVC-SHA2

Personal store contains 3 certificates.



2. Right-click *Certificates* in the *Personal* store, select *All Tasks*, *Import...*



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

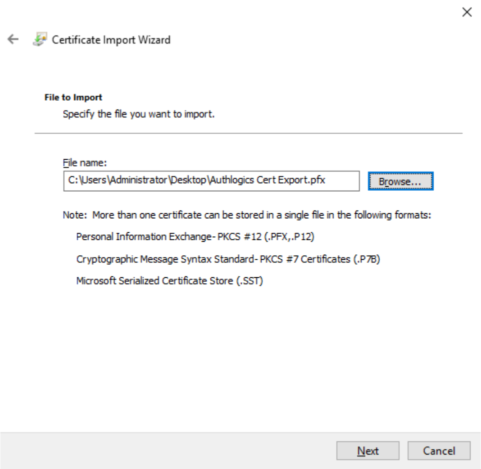
Store Location

○ Current User

● Local Machine

To continue, click Next.

3. Click *Next* to continue.


Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\Administrator\Desktop\Authlogics Cert Export.pfx

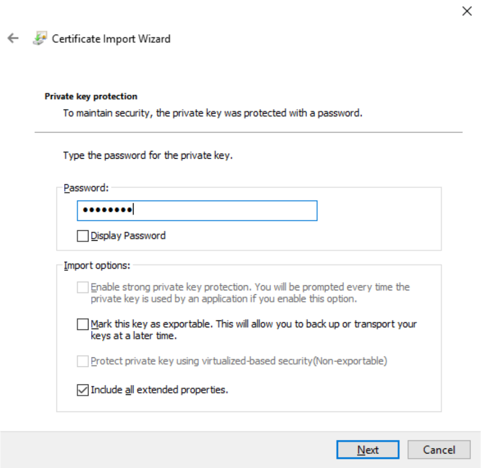
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

4. Enter the path to the file previously exported. Click *Next* to continue.


Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

••••••••

□ Display Password

Import options:

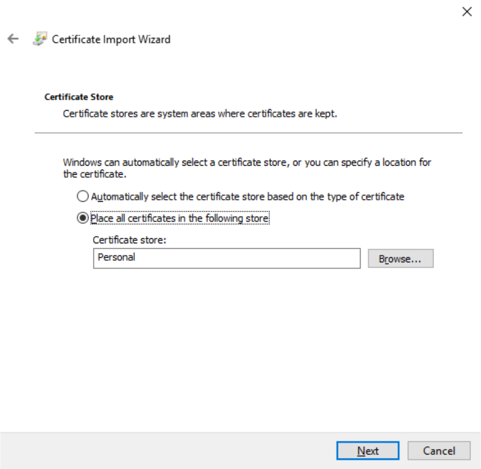
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

□ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

□ Protect private key using virtualized-based security(Non-exportable)

☑ Include all extended properties.

5. Enter the password used when exporting the certificate. Click *Next* to continue.


Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

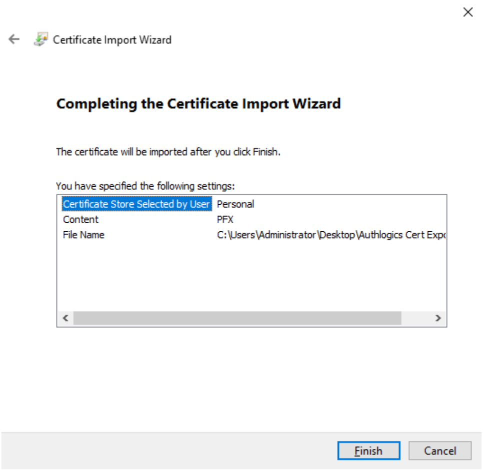
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Personal

6. Click *Next* to continue.



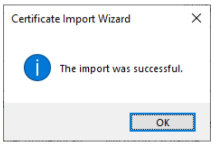
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Personal
Content	PFX
File Name	C:\Users\Administrator\Desktop\Authlogics Cert Expo

7. Click *Finish*.



The import was successful.

8. Click *Ok* to close the wizard.

MyID Authentication Server Directory Configuration

MyID Authentication Server Directory must be configured before users can be provisioned for Multi-Factor Authentication or password policies created.

Directory Configuration Wizard

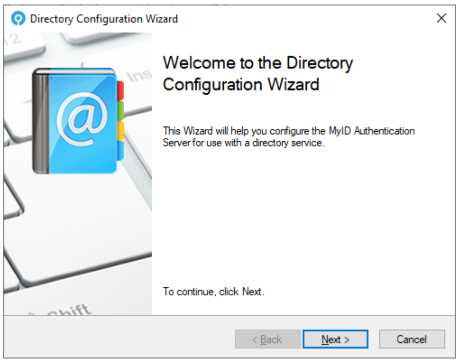
This section should be performed on the server running the MyID Authentication Server.

> **Note**
>
> This section of the installation process requires the logged-on user to have **Domain Admin** rights in the domain containing MyID Users and the domain containing the Authentication Server. Alternatively, an **Enterprise Admin** account can be used.

1. Start the MyID Directory Configuration Wizard from the Windows Start menu:

```
Start – All Programs – MyID Authentication Server – MyID Management Console
```

> **Note**
>
> Ensure that you are logged on with domain administrator account and not a local administrator account.

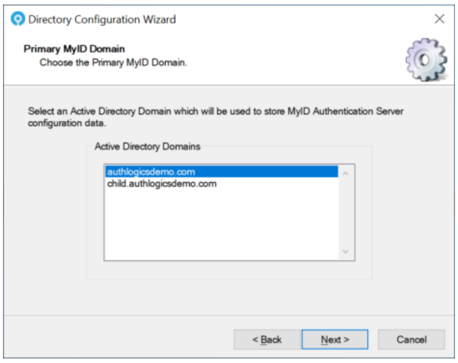


Welcome to the Directory Configuration Wizard

This Wizard will help you configure the MyID Authentication Server for use with a directory service.

To continue, click Next.

2. Click *Next* to start the MyID Authentication Server Configuration Wizard.

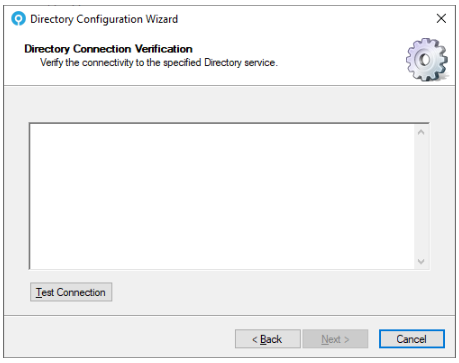


Primary MyID Domain
Choose the Primary MyID Domain.

Select an Active Directory Domain which will be used to store MyID Authentication Server configuration data.

authlogicsdemo.com
child.authlogicsdemo.com

3. If the AD forest contains more than 1 domain and this is the first time the directory is being configured, choose which AD Domain you want to use to store MyID configuration data in and click *Next*.

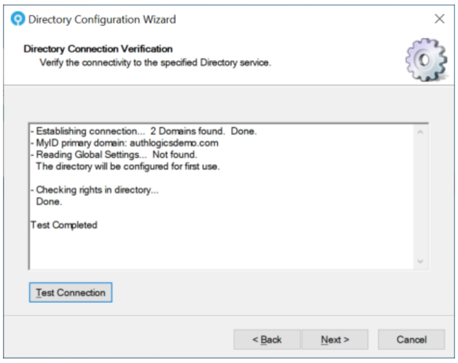


Directory Configuration Wizard

Directory Connection Verification

Verify the connectivity to the specified Directory service.

4. To ensure that the MyID Authentication Server can access the specified directory click the *Test Connection* button.



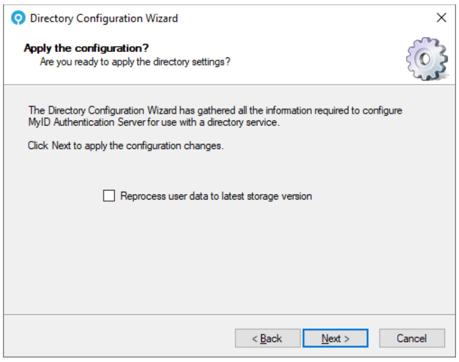
Directory Configuration Wizard

Directory Connection Verification

Verify the connectivity to the specified Directory service.

```
- Establishing connection...  2 Domains found.  Done.
- MyID primary domain: authlogicsdemo.com
- Reading Global Settings...  Not found.
  The directory will be configured for first use.

- Checking rights in directory...
  Done.

Test Completed
```

5. If the test is successful and all the necessary information has been collected, click *Next* to continue, otherwise correct the issue and try again.



Directory Configuration Wizard

Apply the configuration?

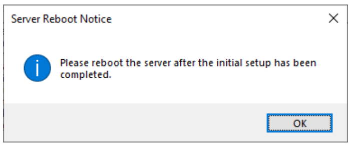
Are you ready to apply the directory settings?

The Directory Configuration Wizard has gathered all the information required to configure MyID Authentication Server for use with a directory service.

Click Next to apply the configuration changes.

☐ Reprocess user data to latest storage version

6. Click the “*Reprocess user data to latest storage version*” to upgrade the user information from a version 4 schema to the latest schema. For clean installations or native MyID version 5 deployment, this option can be left unchecked. Click *Next* to apply the configuration changes.



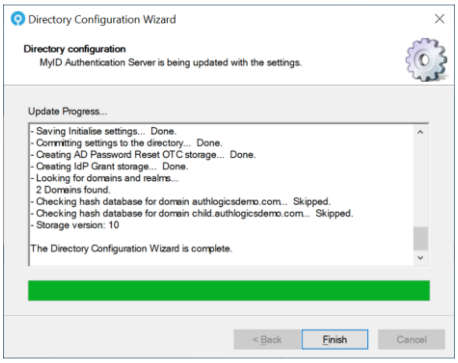
Server Reboot Notice

Please reboot the server after the initial setup has been completed.

7. Click *OK* to acknowledge the reboot requirement.

Important!

After configuring the MyID Authentication server for use with Active Directory you **MUST reboot the server** otherwise authentication services **will fail**. These failures will be reflected in the Windows Events – Application logs.



Directory Configuration Wizard

Directory configuration

MyID Authentication Server is being updated with the settings.

Update Progress...

```
- Saving Initialise settings...  Done.
- Committing settings to the directory...  Done.
- Creating AD Password Reset OTC storage...  Done.
- Creating IdP Grant storage...  Done.
- Looking for domains and realms...
  2 Domains found.
- Checking hash database for domain authlogicsdemo.com...  Skipped.
- Checking hash database for domain child.authlogicsdemo.com...  Skipped.
- Storage version: 10

The Directory Configuration Wizard is complete.
```

8. Examine the update progress information for any unexpected errors which may have occurred during the AD configuration. This information is also logged in the Windows Application Event Log with Information Event ID 1719.

   Click *Finish* when done.

Add users to the MyID Administrators Group

The MyID Directory Configuration wizard will automatically add the currently logged in user account to the MyID Administrators Active Directory security group. User accounts for the administrators of MyID must also be manually added to the MyID Administrators Active Directory security group.

MyID Licence Configuration

The Licence Configuration Wizard is responsible for adding all licence types to the Authentication Server.

Intercede will supply a unique Licence Key for each product (PSM & MFA) specific to each Active Directory. The Licence Key is entered in the Licence Configuration Wizard via the MMC. The licence will require product activation and the server will periodically update Intercede with licence usage information - **this requires Internet connectivity to https://licencing.authlogics.com/* which must be maintained for the server to continue functioning**.

In certain circumstances, Intercede may supply an offline licence file. These digitally signed licence files do not require product activation or any Internet connectivity. They must not be modified or tampered with or they will be rendered inoperable. Contact sales@intercede.com for further information.

Getting a free 10 user licence or a 30-day trial licence

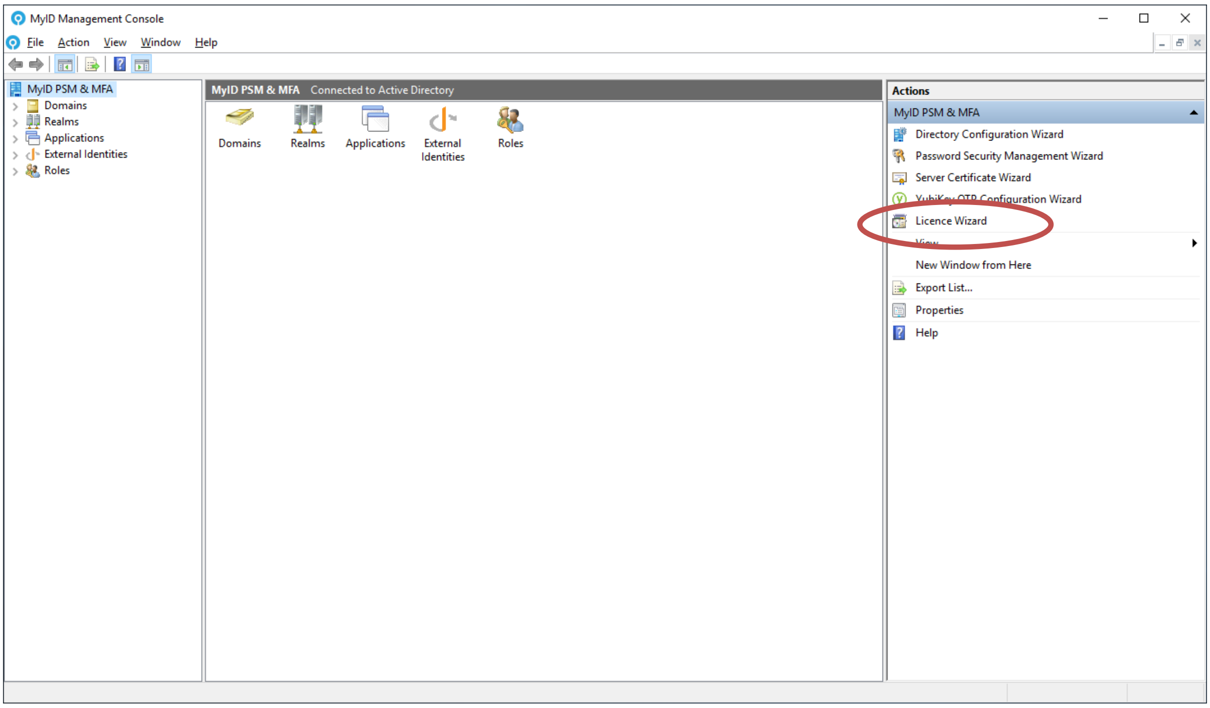
Intercede provides a free licence for up to 10 users. The free licence does not include our standard product support and assistance and we will only be able to provide email assistance on a best-effort basis. However, access to our knowledge base and community site is freely available: https://support.authlogics.com/. If you require additional users in the future we can easily upgrade your existing licence.

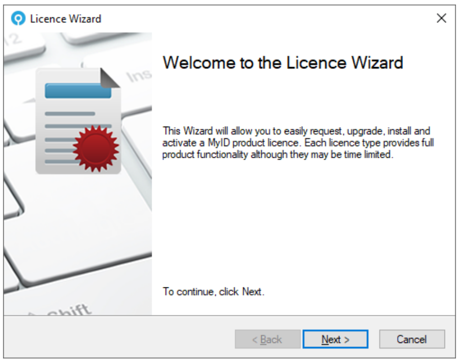
Testing MyID Authentication Server before you buy is simple. Get a free 30-day trial at any time, and when you decide MyID is for you we will simply update your licence to a full one when you purchase, no reinstall is required.

A free or trial licence is installed instantly so you can evaluate at your own pace, however, it does require Internet connectivity (HTTPS) to install and will be activated. If Internet connectivity is not available on the authentication server please contact Intercede for support.

Licence Configuration Wizard

1. The Licence Wizard will start automatically when the MyID Management Console is first loaded. The wizard can also be started from the MMC as follows:



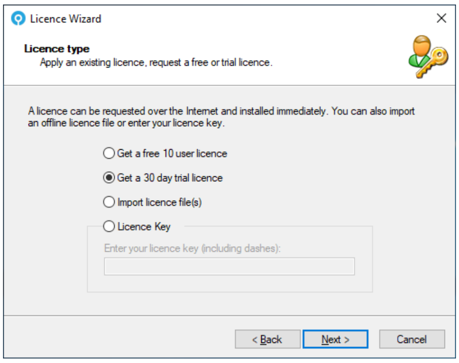


Welcome to the Licence Wizard

This Wizard will allow you to easily request, upgrade, install and activate a MyID product licence. Each licence type provides full product functionality although they may be time limited.

To continue, click Next.

2. Click *Next* to start the MyID Licence Configuration Wizard.



Licence type

Apply an existing licence, request a free or trial licence.

A licence can be requested over the Internet and installed immediately. You can also import an offline licence file or enter your licence key.

○ Get a free 10 user licence

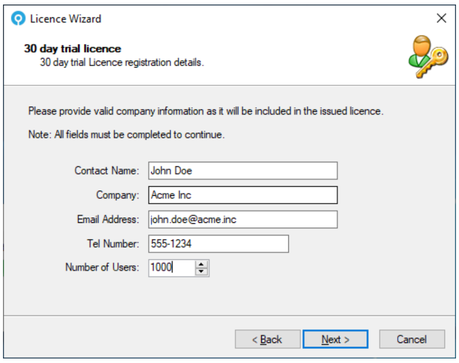
● Get a 30 day trial licence

○ Import licence file(s)

○ Licence Key

Enter your licence key (including dashes):

3. Select Get a free 10 user licence or Get a 30-day trial licence. Click Next to continue.



Licence Wizard

30 day trial licence

30 day trial Licence registration details.

Please provide valid company information as it will be included in the issued licence.

Note: All fields must be completed to continue.

Contact Name: John Doe

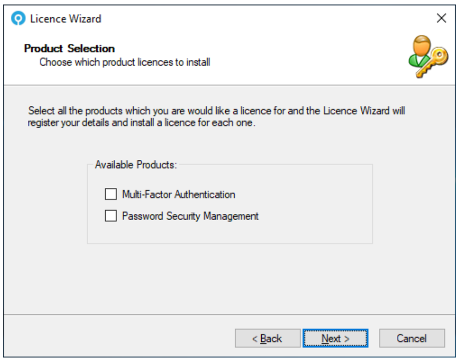
Company: Acme Inc

Email Address: john.doe@acme.inc

Tel Number: 555-1234

Number of Users: 1000

4. Complete your details and click *Next* to continue.



Licence Wizard

Product Selection

Choose which product licences to install

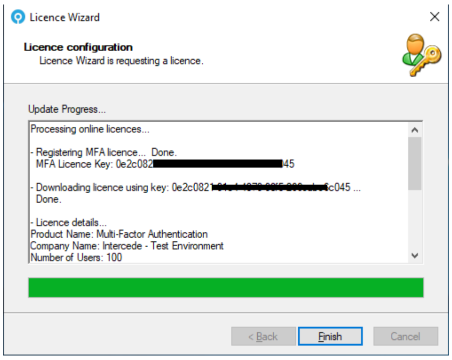
Select all the products which you are would like a licence for and the Licence Wizard will register your details and install a licence for each one.

Available Products:

☐ Multi-Factor Authentication

☐ Password Security Management

5. Select which product you would like licences for and click *Next* to continue.



Licence Wizard

Licence configuration

Licence Wizard is requesting a licence.

Update Progress...

```
Processing online licences...

- Registering MFA licence...  Done.
  MFA Licence Key: 0e2c082[redacted]45

- Downloading licence using key: 0e2c0821[redacted]c045 ...
  Done.

- Licence details...
Product Name: Multi-Factor Authentication
Company Name: Intercede - Test Environment
Number of Users: 100
```

6. The licences will be requested over the Internet and will be activated.

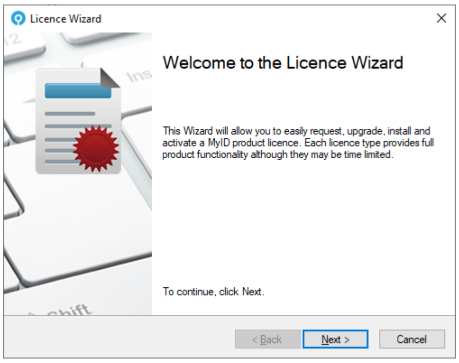
   Click *Finish* when done.

Importing an offline licence file

An offline licence file may be issued by Intercede in certain circumstances. Please contact sales@intercede.com for eligibility. These licences **DO NOT** require Internet connectivity or Activation.

If you have multiple licences files they need to be added one at a time. Simply run the wizard again to add the second licence file.

1. Start the Licence Configuration Wizard



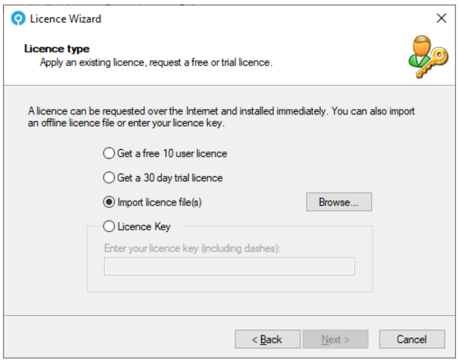
Licence Wizard

Welcome to the Licence Wizard

This Wizard will allow you to easily request, upgrade, install and activate a MyID product licence. Each licence type provides full product functionality although they may be time limited.

To continue, click Next.

2. Click *Next* to start the MyID Licence Configuration Wizard.



Licence Wizard

Licence type

Apply an existing licence, request a free or trial licence.

A licence can be requested over the Internet and installed immediately. You can also import an offline licence file or enter your licence key.

○ Get a free 10 user licence

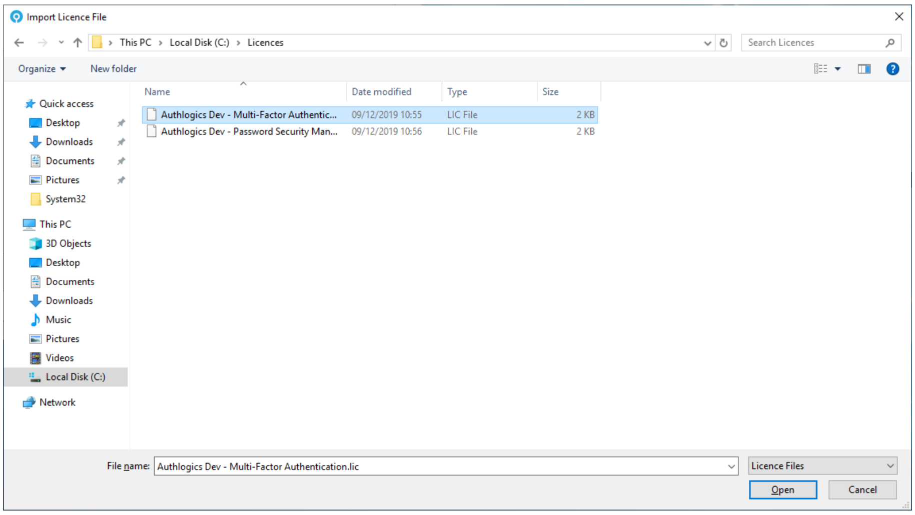
○ Get a 30 day trial licence

● Import licence file(s)

○ Licence Key

Enter your licence key (including dashes):

3. Select Import licence file(s) and click Browse…

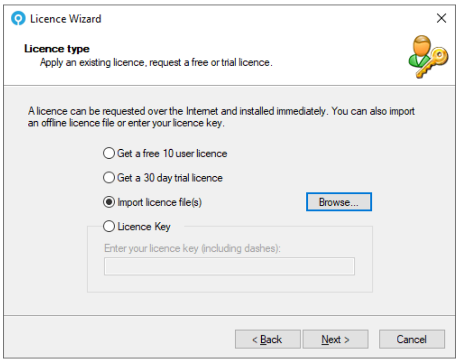


Name	Date modified	Type	Size
Authlogics Dev - Multi-Factor Authentic...	09/12/2019 10:55	LIC File	2 KB
Authlogics Dev - Password Security Man...	09/12/2019 10:56	LIC File	2 KB

File name: Authlogics Dev - Multi-Factor Authentication.lic

Licence Files

4. Select one or more of your licence file (ending in .LIC) and click *Open*.



Licence type

Apply an existing licence, request a free or trial licence.

A licence can be requested over the Internet and installed immediately. You can also import an offline licence file or enter your licence key.

○ Get a free 10 user licence

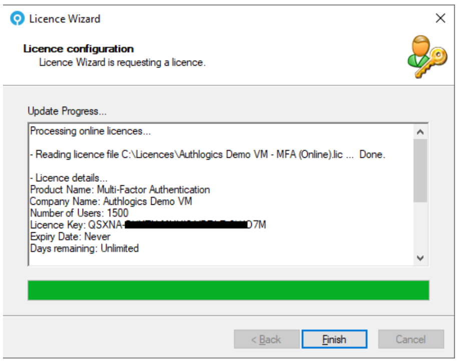
○ Get a 30 day trial licence

● Import licence file(s)

○ Licence Key

Enter your licence key (including dashes):

5. Click *Next* to continue.



Licence configuration

Licence Wizard is requesting a licence.

Update Progress...

```
Processing online licences...

- Reading licence file C:\Licences\Authlogics Demo VM - MFA (Online).lic ...  Done.

- Licence details...
Product Name: Multi-Factor Authentication
Company Name: Authlogics Demo VM
Number of Users: 1500
Licence Key: QSXNA-[redacted]D7M
Expiry Date: Never
Days remaining: Unlimited
```

6. The licence(s) will be installed and activation skipped.

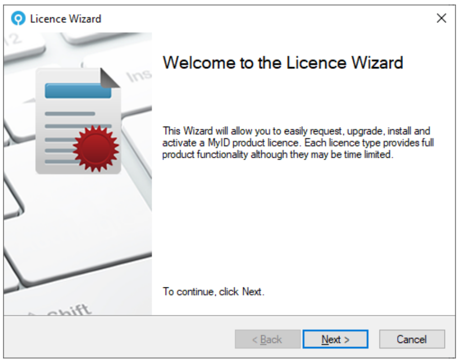
   Click *Finish* when done.

Entering an existing licence key

A licence key is issued by Intercede at the point of purchase. Licences keys **do require** Internet connectivity for installation, activation and ongoing licence reporting metrics. No private or confidential information is reported back to Intercede.

If you have multiple licences keys they need to be added one at a time. Simply run the wizard again to add the second licence key.

1. Start the Licence Configuration Wizard



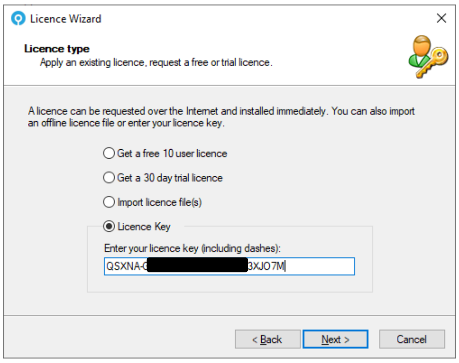
Licence Wizard

Welcome to the Licence Wizard

This Wizard will allow you to easily request, upgrade, install and activate a MyID product licence. Each licence type provides full product functionality although they may be time limited.

To continue, click Next.

2. Click *Next* to start the MyID Licence Configuration Wizard.



Licence Wizard

Licence type
Apply an existing licence, request a free or trial licence.

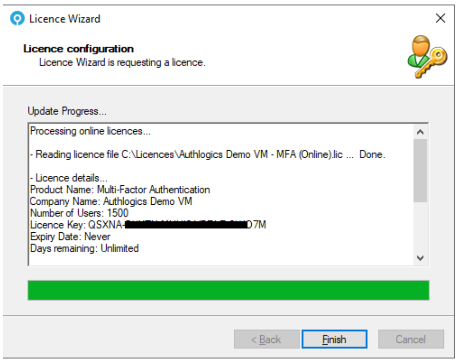
A licence can be requested over the Internet and installed immediately. You can also import an offline licence file or enter your licence key.

○ Get a free 10 user licence
○ Get a 30 day trial licence
○ Import licence file(s)
● Licence Key

Enter your licence key (including dashes): QSXNA-[redacted]3XJO7M

3. Select *Licence Key* and enter the licence key which was sent to you by Intercede.

   Click *Next* to continue.



Licence Wizard

Licence configuration
Licence Wizard is requesting a licence.

Update Progress...

```
Processing online licences...

- Reading licence file C:\Licences\Authlogics Demo VM - MFA (Online).lic ...  Done.

- Licence details...
Product Name: Multi-Factor Authentication
Company Name: Authlogics Demo VM
Number of Users: 1500
Licence Key: QSXNA-[redacted]7M
Expiry Date: Never
Days remaining: Unlimited
```

4. The licence will be installed and activated.

   Click *Finish* when done.

MyID Password Security Management Wizard

The Password Security Management Wizard (PSM) is responsible for configuring domains in the Active Directory Forest for real-time and retrospective protection against known breached and shared passwords, as well as dormant accounts. This includes:

- Analyse existing password hashes in AD
- Set a remediation protection schedule
- Set the account remediation policy
- Set the alerting actions and recipients

Retrospective Protection: The MyID Authentication Server is responsible for doing all retrospective protection, remediation and alerting work required by the scheduled.

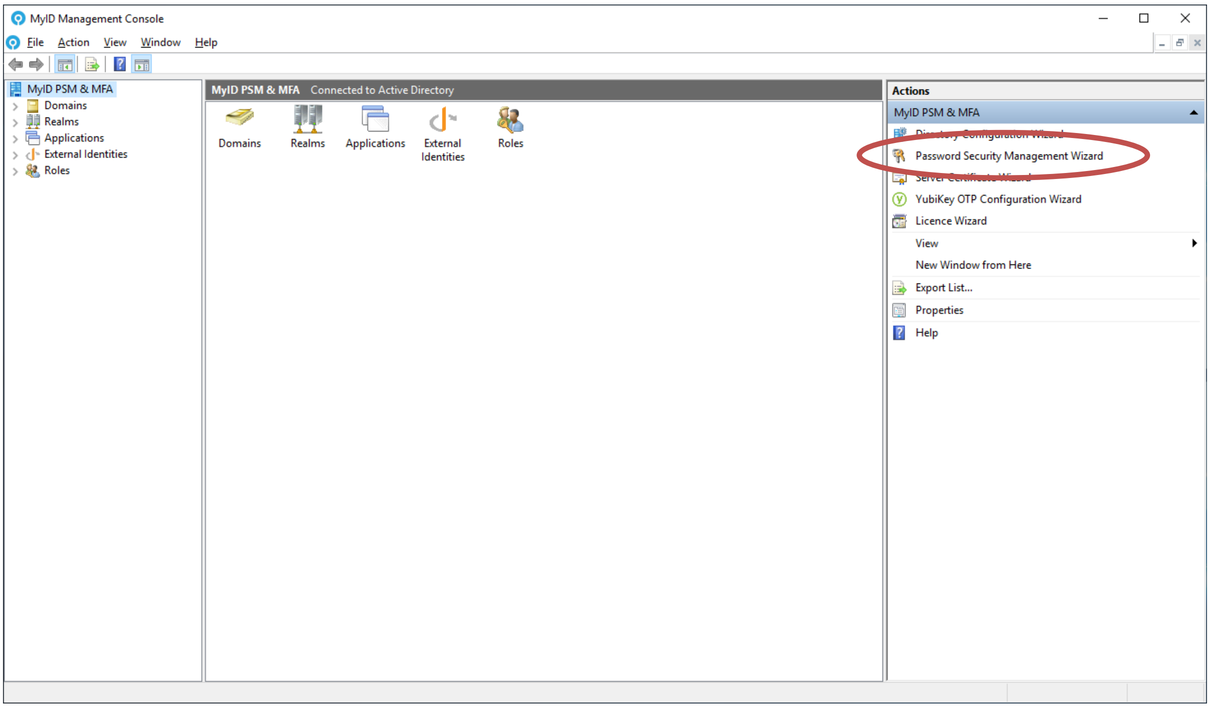
Real-Time Protection: The MyID Authentication Server works in conjunction with MyID Domain Controller Agent (DCA) to provide real-time protection of Active Directory passwords. The Domain Controller Agent will intercept password changes at the DC as they happen and query the MyID Authentication Server to check if the password should be accepted.

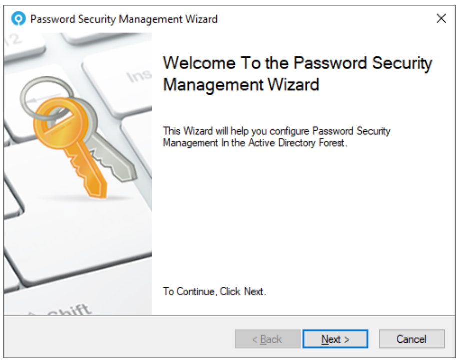
> **Note**
>
> A PSM Password Policy must be configured, enabled and applied via Group Policy to the Domain Controllers as well as the MyID Authentication Servers for the policy to take effect.
>
> See the *Configuring the* MyID *Password Policy* Settings section for further information.

The MyID Authentication Server requires Internet access to query the MyID Password Breach Database in the Cloud. See the *Internet Access for breach password lookups* section for further information. A fully offline copy of the MyID Password Breach Database can be installed on the MyID Authentication Server which can be downloaded here: https://www.intercede.com/support/downloads

Starting the Password Security Management Wizard

1. The wizard can be started from the MMC as follows:



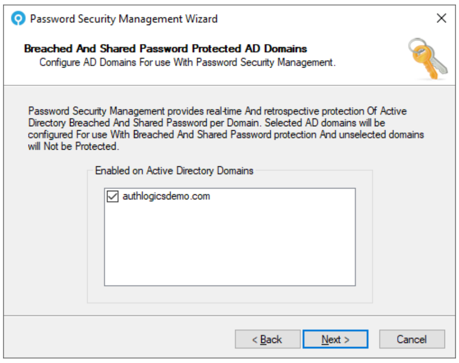


Welcome To the Password Security Management Wizard

This Wizard will help you configure Password Security Management In the Active Directory Forest.

To Continue, Click Next.

2. Click *Next* to start the MyID Password Security Management Wizard.



Breached And Shared Password Protected AD Domains

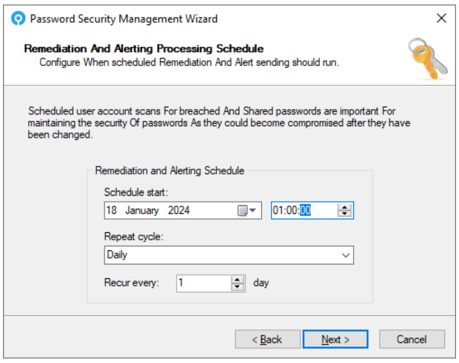
Configure AD Domains For use With Password Security Management.

Password Security Management provides real-time And retrospective protection Of Active Directory Breached And Shared Password per Domain. Selected AD domains will be configured For use With Breached And Shared Password protection And unselected domains will Not be Protected.

Enabled on Active Directory Domains

☑ authlogicsdemo.com

3. Select the domain or domains to which you wish to enable PSM password protection on. Click *Next* to continue.



Password Security Management Wizard

Remediation And Alerting Processing Schedule
Configure When scheduled Remediation And Alert sending should run.

Scheduled user account scans For breached And Shared passwords are important For maintaining the security Of passwords As they could become compromised after they have been changed.

Remediation and Alerting Schedule

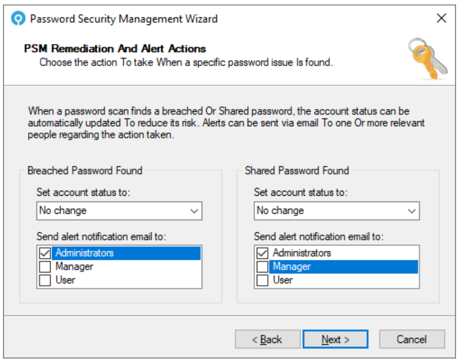
Schedule start: 18 January 2024 01:00:00

Repeat cycle: Daily

Recur every: 1 day

4. MyID Authentication Server provides the ability to run Password Security Management remediation and alerting on a scheduled basis.
5. Select the Schedule start date and time.
6. Select the Repeat cycle and recurrence cycle. Options available are:
7. Run Once
8. Hourly
9. Daily
10. Weekly
11. Monthly

Click *Next* to continue.



Password Security Management Wizard

PSM Remediation And Alert Actions
Choose the action To take When a specific password issue Is found.

When a password scan finds a breached Or Shared password, the account status can be automatically updated To reduce its risk. Alerts can be sent via email To one Or more relevant people regarding the action taken.

Breached Password Found

Set account status to: No change

Send alert notification email to:
☑ Administrators
□ Manager
□ User

Shared Password Found

Set account status to: No change

Send alert notification email to:
☑ Administrators
□ Manager
□ User

12. Password Security Management can alert Administrators, Managers or Users for newly detected breached or shared passwords.

    PSM also includes auto-remediation functionality where accounts can be disabled or users can be forced to change their password at next logon for breached or shared passwords.

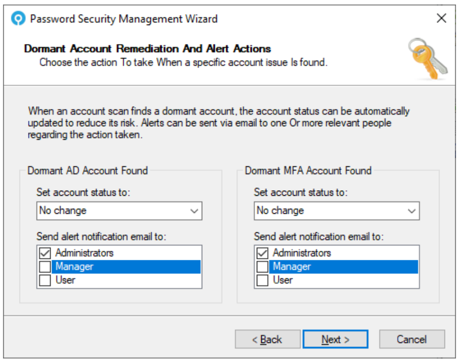
    Set account status for detected Breached Passwords and Shared Passwords to:

    - No change
    - Must change password at next logon
    - Account is disabled

    Select alert notifications for detected Breached Passwords and Shared Passwords to:

    - Administrators
    - Managers
    - Users

Click *Next* to continue.



Password Security Management Wizard

Dormant Account Remediation And Alert Actions
Choose the action To take When a specific account issue Is found.

When an account scan finds a dormant account, the account status can be automatically updated to reduce its risk. Alerts can be sent via email to one Or more relevant people regarding the action taken.

Dormant AD Account Found

Set account status to: No change

Send alert notification email to:
☑ Administrators
☐ Manager
☐ User

Dormant MFA Account Found

Set account status to: No change

Send alert notification email to:
☑ Administrators
☐ Manager
☐ User

13. Password Security Management can alert Administrators, Managers or Users for newly detected dormant AD or MFA accounts.

    PSM also includes auto-remediation functionality where accounts can be disabled or users can be forced to change their password at next logon for breached or shared passwords.

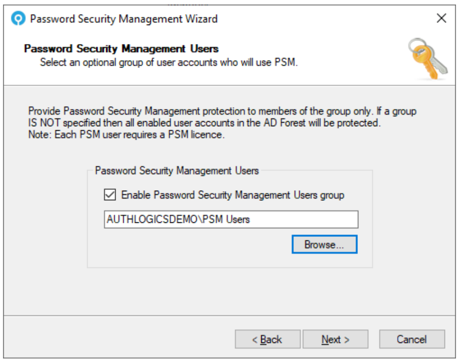
    Set account status for detected dormant AD or MFA accounts to:

    - No change
    - Must change password at next logon
    - Account is disabled

    Select alert notifications for detected dormant AD or MFA accounts to:

    - Administrators
    - Managers
    - Users

    Click *Next* to continue.



Password Security Management Wizard

Password Security Management Users
Select an optional group of user accounts who will use PSM.

Provide Password Security Management protection to members of the group only. If a group IS NOT specified then all enabled user accounts in the AD Forest will be protected.
Note: Each PSM user requires a PSM licence.

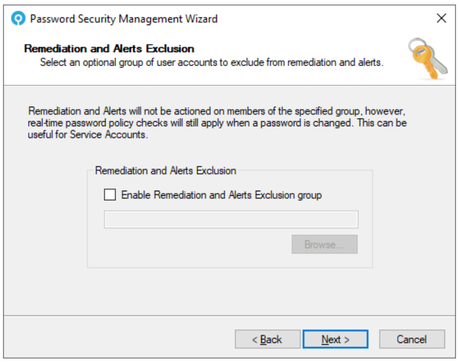
Password Security Management Users

☑ Enable Password Security Management Users group

AUTHLOGICSDEMO\PSM Users

14. To limit which users will use PSM (and thus require a licence) check *Enable Password Security Management Users group* and then click *Browse...* to select an AD Group containing the user accounts to include.

    Click *Next* to continue.



Password Security Management Wizard

Remediation and Alerts Exclusion

Select an optional group of user accounts to exclude from remediation and alerts.

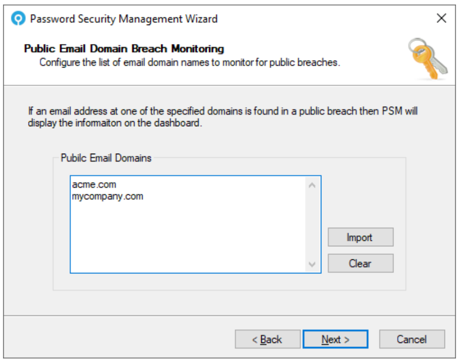
Remediation and Alerts will not be actioned on members of the specified group, however, real-time password policy checks will still apply when a password is changed. This can be useful for Service Accounts.

Remediation and Alerts Exclusion

☐ Enable Remediation and Alerts Exclusion group

15. To exclude users from PSM remediation and alerting check *Enable Remediation and Alerts Exclusion group* and then click *Browse...* to select an AD Group containing the user accounts to exclude.

    Click *Next* to continue.



Password Security Management Wizard

Public Email Domain Breach Monitoring

Configure the list of email domain names to monitor for public breaches.

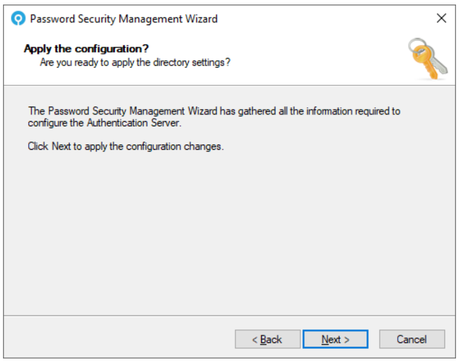
If an email address at one of the specified domains is found in a public breach then PSM will display the informaiton on the dashboard.

Public Email Domains

acme.com
mycompany.com

16. To monitor and display data breaches based on email addresses for your organisation on the Web Management Portal Dashboard enter all public email domain names. MyID will auto detect any email domain names configured within Microsoft Exchange.

    Click *Next* to continue.



Password Security Management Wizard

Apply the configuration?

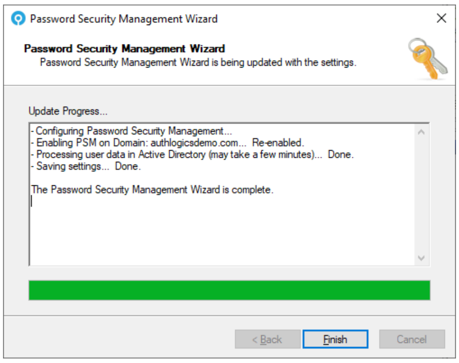
Are you ready to apply the directory settings?

The Password Security Management Wizard has gathered all the information required to configure the Authentication Server.

Click Next to apply the configuration changes.

17. Click *Next* to continue.

Password Security Management will be configured.



Password Security Management Wizard
Password Security Management Wizard
Password Security Management Wizard is being updated with the settings.
Update Progress...
< Back
Finish
Cancel

```
- Configuring Password Security Management...
- Enabling PSM on Domain: authlogicsdemo.com...  Re-enabled.
- Processing user data in Active Directory (may take a few minutes)...  Done.
- Saving settings...  Done.

The Password Security Management Wizard is complete.
```

18. Click *Finish* when done.

YubiKey OTP Configuration Wizard

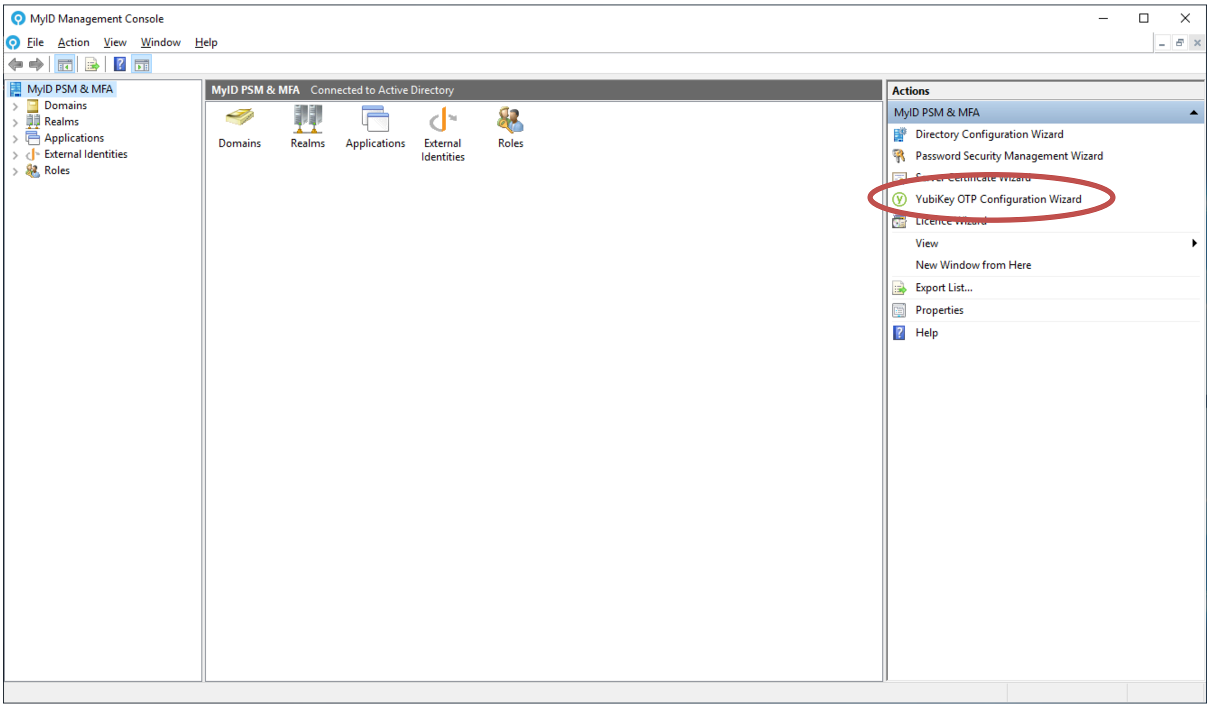
The YubiKey OTP Configuration Wizard is responsible for managing reprogrammed YubiKey tokens so that YubiKey OTPs are processed by the MyID Authentication Server and access to the Internet-based YubiKey servers is not required for validation.

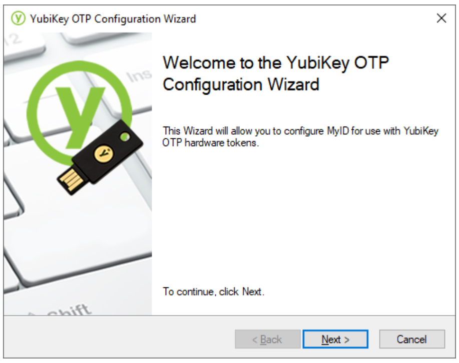
Should you wish to still validate YubiKey OTPs using the Internet-based YubiKey servers for tokens that have not been reprogrammed then the MyID Authentication Server still requires Internet access.

To reprogram YubiKey tokens and create a YubiKey Personalization CSV file see the MyID *Authentication Server YubiKey Reprogramming Guide*.

Starting the YubiKey OTP Configuration Wizard

1. The wizard can be started from the MMC as follows:



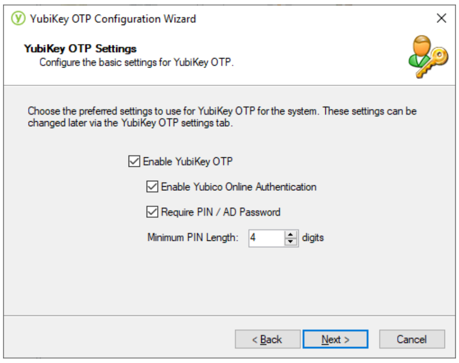


Welcome to the YubiKey OTP Configuration Wizard

This Wizard will allow you to configure MyID for use with YubiKey OTP hardware tokens.

To continue, click Next.

2. Click *Next* to start the MyID YubiKey Configuration Wizard.



YubiKey OTP Settings
Configure the basic settings for YubiKey OTP.

Choose the preferred settings to use for YubiKey OTP for the system. These settings can be changed later via the YubiKey OTP settings tab.

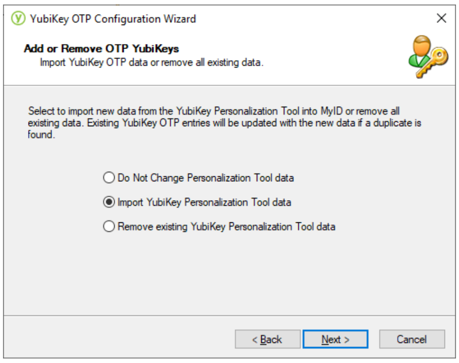
☑ Enable YubiKey OTP

☑ Enable Yubico Online Authentication

☑ Require PIN / AD Password

Minimum PIN Length: 4 digits

3. Configure YubiKey OTP options.
   Select *Enable Yubico Online Authentication* to send YubiKey OTPs to Yubico's servers to verify the validity of the YubiKey token. The user's AD password can be used instead of a PIN or the user can select a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation.
   Click Next



Add or Remove OTP YubiKeys
Import YubiKey OTP data or remove all existing data.

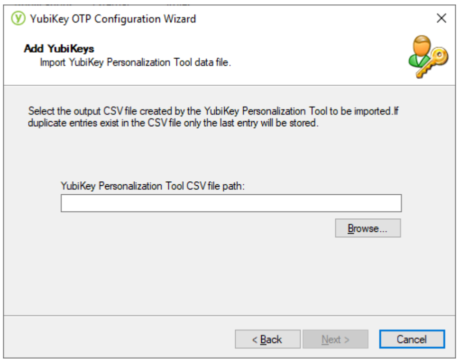
Select to import new data from the YubiKey Personalization Tool into MyID or remove all existing data. Existing YubiKey OTP entries will be updated with the new data if a duplicate is found.

○ Do Not Change Personalization Tool data

● Import YubiKey Personalization Tool data

○ Remove existing YubiKey Personalization Tool data

4. Select Import YubiKey Personalisation Tool data. Click *Next* to continue.

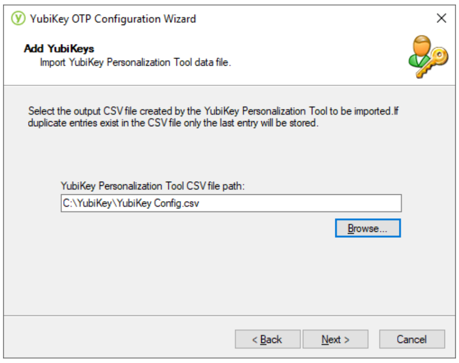


Add YubiKeys
Import YubiKey Personalization Tool data file.

Select the output CSV file created by the YubiKey Personalization Tool to be imported.If duplicate entries exist in the CSV file only the last entry will be stored.

YubiKey Personalization Tool CSV file path:

5. Select *Browse* to select the YubiKey Personalisation Tool generated CSV file.



YubiKey OTP Configuration Wizard

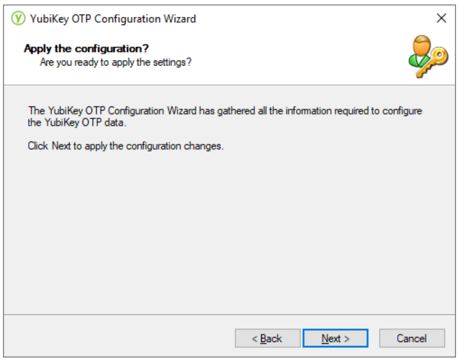
Add YubiKeys

Import YubiKey Personalization Tool data file.

Select the output CSV file created by the YubiKey Personalization Tool to be imported.If duplicate entries exist in the CSV file only the last entry will be stored.

YubiKey Personalization Tool CSV file path: C:\YubiKey\YubiKey Config.csv

6. Click *Next* to continue.



YubiKey OTP Configuration Wizard

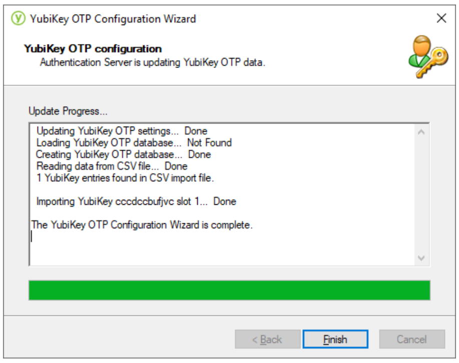
Apply the configuration?

Are you ready to apply the settings?

The YubiKey OTP Configuration Wizard has gathered all the information required to configure the YubiKey OTP data.

Click Next to apply the configuration changes.

7. Click *Next* to Apply the configuration and continue.



YubiKey OTP Configuration Wizard

YubiKey OTP configuration

Authentication Server is updating YubiKey OTP data.

Update Progress...

```
 Updating YubiKey OTP settings...  Done
 Loading YubiKey OTP database...  Not Found
 Creating YubiKey OTP database...  Done
 Reading data from CSV file...  Done
 1 YubiKey entries found in CSV import file.

 Importing YubiKey cccdccbufjvc slot 1...  Done

The YubiKey OTP Configuration Wizard is complete.
```

8. The YubiKey database has been imported.

   Click *Finish* when done.

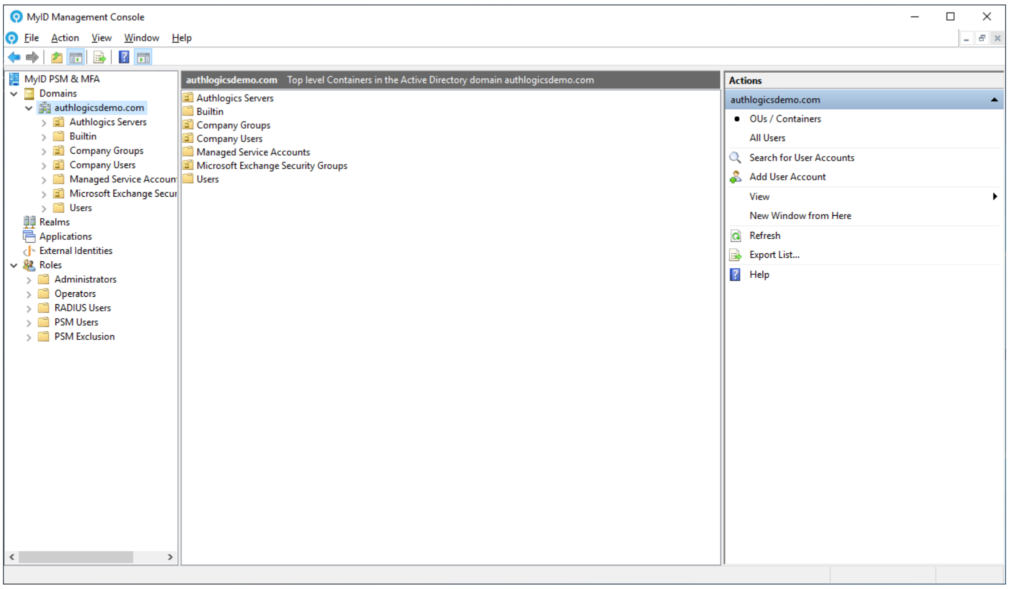
Administering MyID Authentication Server

The MyID Management Console

The MyID Management Console provides administrators with the ability to configure MyID settings and administer users. Functionality and options may differ depending on the product licence installed.

The MyID Management Console provides Administrators with the ability to manage the following:

- Directory Configuration
- MyID Global Settings
- MyID Users in Domains or Realms
- Applications
- External Identities
- User Roles



authlogicsdemo.com Top level Containers in the Active Directory domain authlogicsdemo.com

MyID Management Console Views

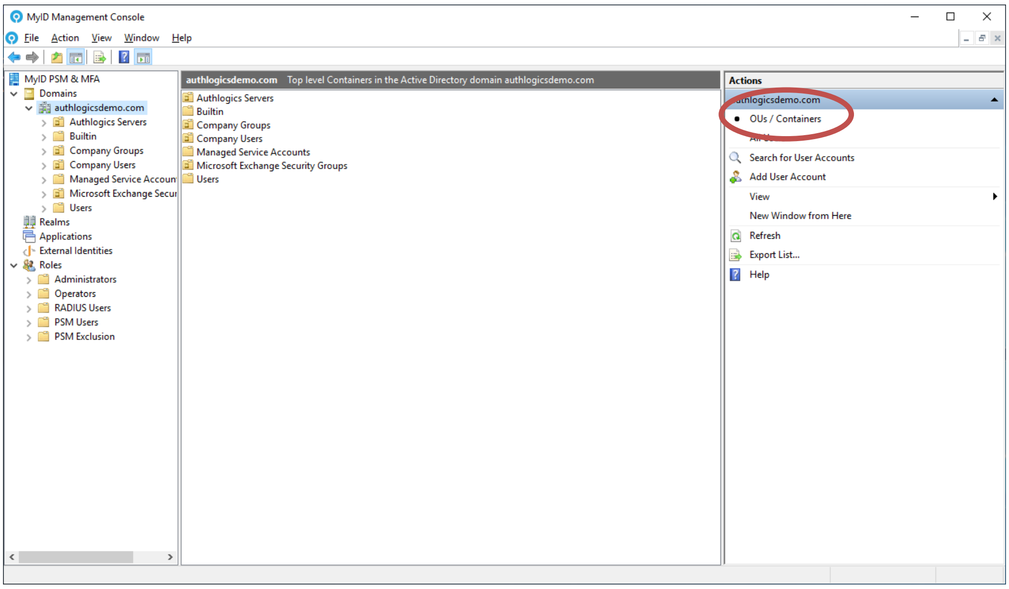
The MyID Management Console displays both the MFA and PSM users.

PSM user only icon:

MFA user icon:

The MyID Management Console is suited to small deployments and also scales to very large Active Directory environments. This is achieved by utilising the “OUs / Containers” and the “All Users” view for Active Directory Domains, and a Realms view for External users.

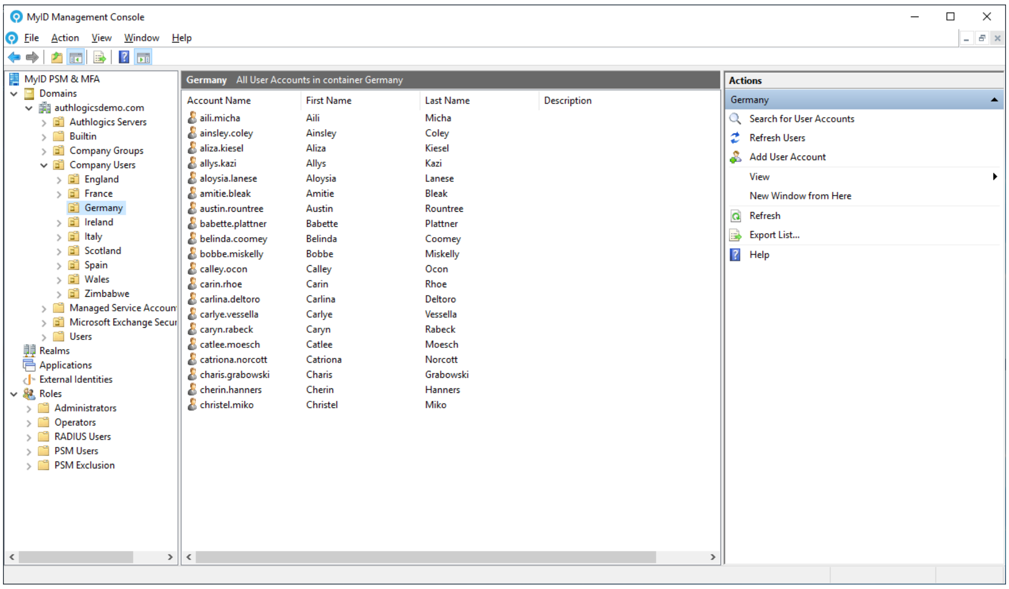
The Active Directory view can be chosen by selecting the domain and toggling between the two options.



Top level Containers in the Active Directory domain authlogicsdemo.com

OUs / Containers View

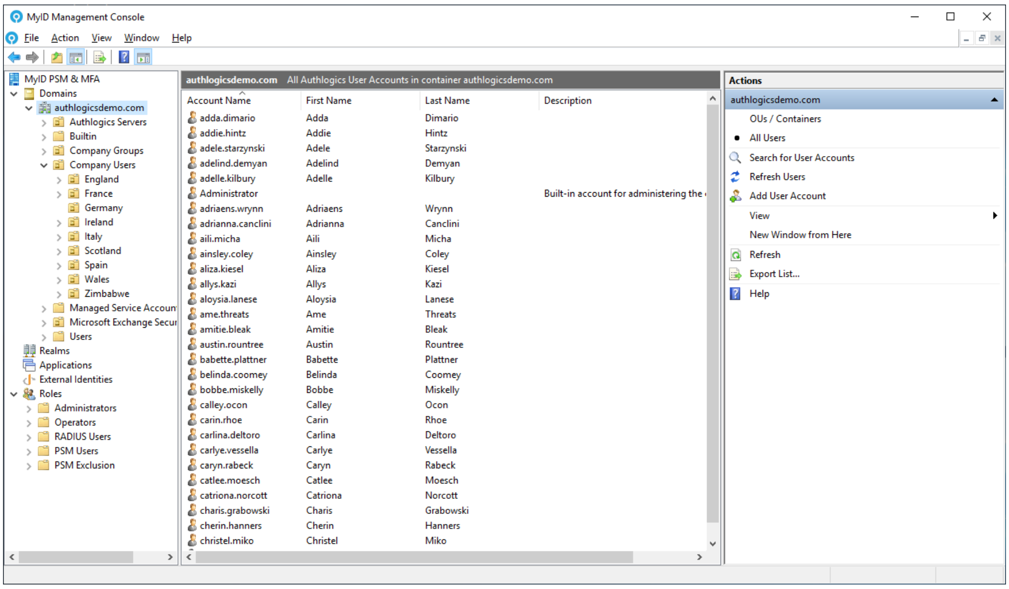
The OUs / Containers view is the default view which allows the AD OU structure to be traversed. Searches for user accounts can be done from the domain level or an OU or Container. All users in an OU tree can be found for by searching for the wildcard “*”.



Account Name	First Name	Last Name	Description
aili.micha	Aili	Micha	
ainsley.coley	Ainsley	Coley	
aliza.kiesel	Aliza	Kiesel	
allys.kazi	Allys	Kazi	
aloysia.lanese	Aloysia	Lanese	
amitie.bleak	Amitie	Bleak	
austin.rountree	Austin	Rountree	
babette.plattner	Babette	Plattner	
belinda.coomey	Belinda	Coomey	
bobbe.miskelly	Bobbe	Miskelly	
calley.ocon	Calley	Ocon	
carin.rhoe	Carin	Rhoe	
carlina.deltoro	Carlina	Deltoro	
carlye.vessella	Carlye	Vessella	
caryn.rabeck	Caryn	Rabeck	
catlee.moesch	Catlee	Moesch	
catriona.norcott	Catriona	Norcott	
charis.grabowski	Charis	Grabowski	
cherin.hanners	Cherin	Hanners	
christel.miko	Christel	Miko	

All Users View

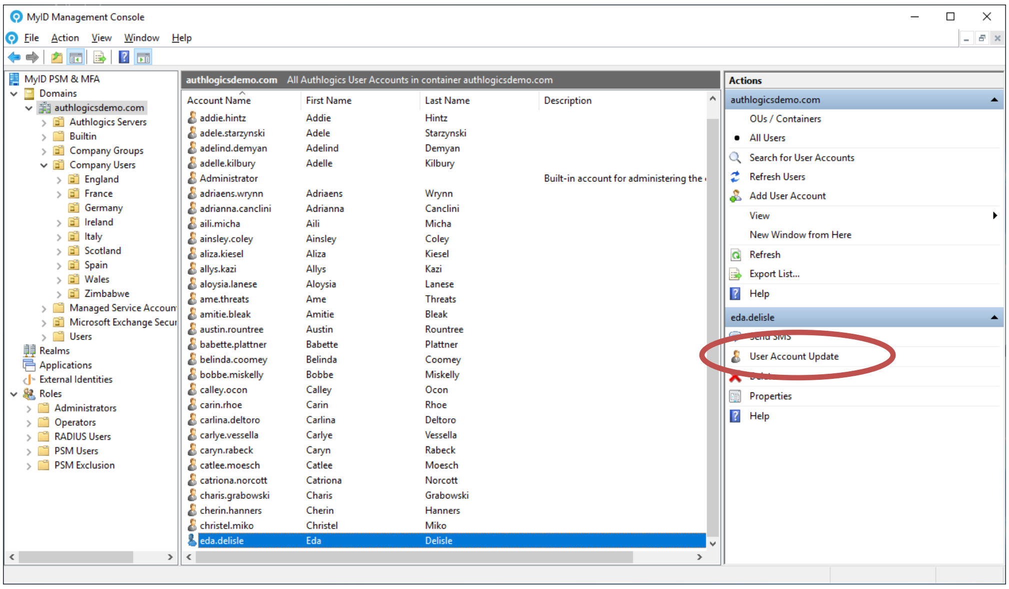
The All Users view lists all users in a single view for the entire domain. Since all users are loaded for the domain at once this view may be slower to load on large domains.



Account Name	First Name	Last Name	Description
adda.dimario	Adda	Dimario	
addie.hintz	Addie	Hintz	
adele.starzynski	Adele	Starzynski	
adelind.demyan	Adelind	Demyan	
adelle.kilbury	Adelle	Kilbury	
Administrator			Built-in account for administering the
adriaens.wrynn	Adriaens	Wrynn	
adrianna.canclini	Adrianna	Canclini	
aili.micha	Aili	Micha	
ainsley.coley	Ainsley	Coley	
aliza.kiesel	Aliza	Kiesel	
allys.kazi	Allys	Kazi	
aloysia.lanese	Aloysia	Lanese	
ame.threats	Ame	Threats	
amitie.bleak	Amitie	Bleak	
austin.rountree	Austin	Rountree	
babette.plattner	Babette	Plattner	
belinda.coomey	Belinda	Coomey	
bobbe.miskelly	Bobbe	Miskelly	
calley.ocon	Calley	Ocon	
carin.rhoe	Carin	Rhoe	
carlina.deltoro	Carlina	Deltoro	
carlye.vessella	Carlye	Vessella	
caryn.rabeck	Caryn	Rabeck	
catlee.moesch	Catlee	Moesch	
catriona.norcott	Catriona	Norcott	
charis.grabowski	Charis	Grabowski	
cherin.hanners	Cherin	Hanners	
christel.miko	Christel	Miko	

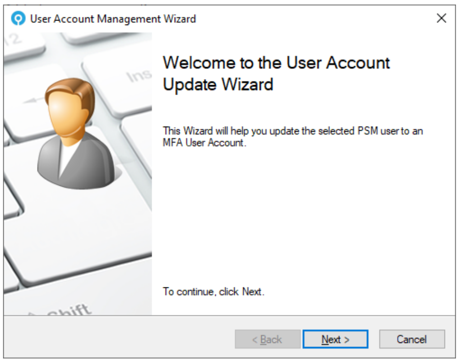
Updating PSM Users

PSM users are automatically added to the MyID Management Console when the user interacts with MyID either via an AD password change or Self-service portal login. These users can be made into MFA users (provided a valid MFA licence exists) by running the Update User Account.



authlogicsdemo.com All Authlogics User Accounts in container authlogicsdemo.com

Account Name	First Name	Last Name	Description
addie.hintz	Addie	Hintz	
adele.starzynski	Adele	Starzynski	
adelind.demyan	Adelind	Demyan	
adelle.kilbury	Adelle	Kilbury	
Administrator			Built-in account for administering the
adriaens.wrynn	Adriaens	Wrynn	
adrianna.canclini	Adrianna	Canclini	
aili.micha	Aili	Micha	
ainsley.coley	Ainsley	Coley	
aliza.kiesel	Aliza	Kiesel	
allys.kazi	Allys	Kazi	
aloysia.lanese	Aloysia	Lanese	
ame.threats	Ame	Threats	
amitie.bleak	Amitie	Bleak	
austin.rountree	Austin	Rountree	
babette.plattner	Babette	Plattner	
belinda.coomey	Belinda	Coomey	
bobbe.miskelly	Bobbe	Miskelly	
calley.ocon	Calley	Ocon	
carin.rhoe	Carin	Rhoe	
carlina.deltoro	Carlina	Deltoro	
carlye.vessella	Carlye	Vessella	
caryn.rabeck	Caryn	Rabeck	
catlee.moesch	Catlee	Moesch	
catriona.norcott	Catriona	Norcott	
charis.grabowski	Charis	Grabowski	
cherin.hanners	Cherin	Hanners	
christel.miko	Christel	Miko	
eda.delisle	Eda	Delisle	

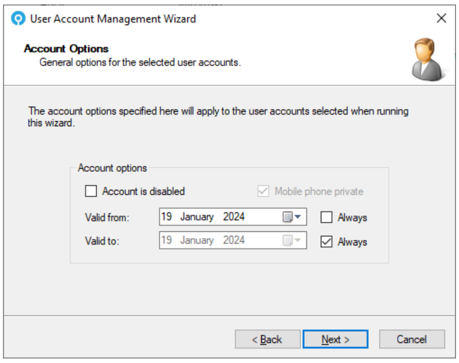


Welcome to the User Account Update Wizard

This Wizard will help you update the selected PSM user to an MFA User Account.

To continue, click Next.

1. Click *Next* to start the User Account Update Wizard.



Account Options
General options for the selected user accounts.

The account options specified here will apply to the user accounts selected when running this wizard.

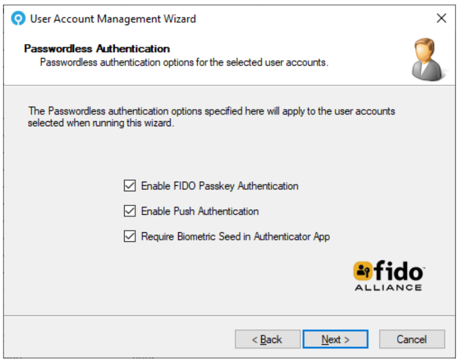
Account options

☐ Account is disabled ☑ Mobile phone private

Valid from: 19 January 2024 ☐ Always

Valid to: 19 January 2024 ☑ Always

2. Account options determine the user's initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use. The mobile phone privacy setting can also be specified. Make any required changes and click Next to continue.



User Account Management Wizard

Passwordless Authentication

Passwordless authentication options for the selected user accounts.

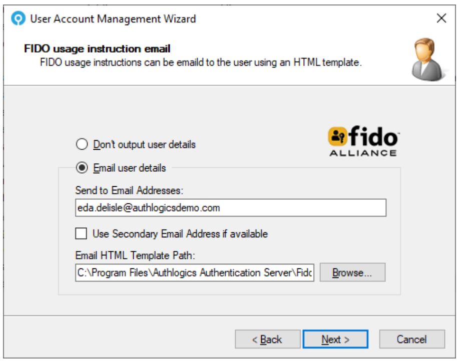
The Passwordless authentication options specified here will apply to the user accounts selected when running this wizard.

☑ Enable FIDO Passkey Authentication

☑ Enable Push Authentication

☑ Require Biometric Seed in Authenticator App

3. Select *Enable FIDO Passkey Authentication* and *Enable Push Authentication* to enable the FIDO Passkey and/or Push authentication for the user. Select *Require Biometric Seed in Authenticator App* to ensure that user is required to provide valid biometrics when accessing the Authenticator App.
   Click Next to continue.



User Account Management Wizard

FIDO usage instruction email

FIDO usage instructions can be emaild to the user using an HTML template.

○ Don't output user details

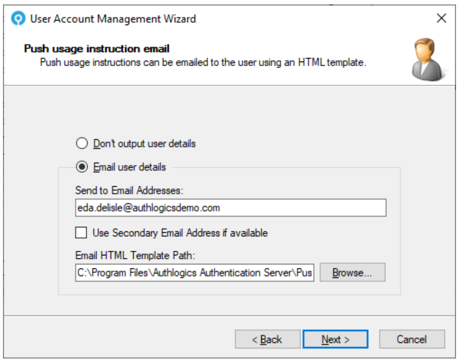
● Email user details

Send to Email Addresses: eda.delisle@authlogicsdemo.com

□ Use Secondary Email Address if available

Email HTML Template Path: C:\Program Files\Authlogics Authentication Server\Fidc

4. If the *Enable FIDO Passkey Authentication* was selected for the user above, then the FIDO instruction letter can be emailed to the user. If a secondary email address is configured, the email can be sent to this alternate address. Click Next to continue.



User Account Management Wizard

Push usage instruction email

Push usage instructions can be emailed to the user using an HTML template.

○ Don't output user details

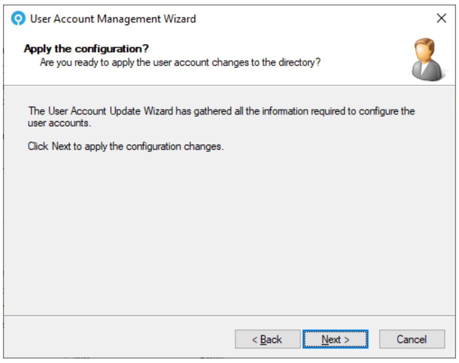
● Email user details

Send to Email Addresses: eda.delisle@authlogicsdemo.com

□ Use Secondary Email Address if available

Email HTML Template Path: C:\Program Files\Authlogics Authentication Server\Pus

5. If the Enable Push Authentication option was selected for the user above then a PUSH instruction letter can be emailed to the user. If a secondary email address is configured, the email can be sent to this alternate address. Click Next to continue.



User Account Management Wizard

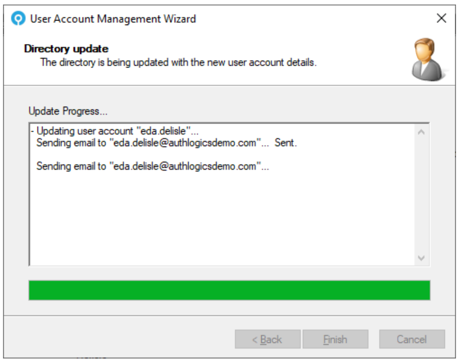
Apply the configuration?

Are you ready to apply the user account changes to the directory?

The User Account Update Wizard has gathered all the information required to configure the user accounts.

Click Next to apply the configuration changes.

6. Click Next to Apply the configuration changes.



User Account Management Wizard

Directory update

The directory is being updated with the new user account details.

Update Progress...

```
- Updating user account "eda.delisle"...
  Sending email to "eda.delisle@authlogicsdemo.com"...  Sent.

  Sending email to "eda.delisle@authlogicsdemo.com"...
```

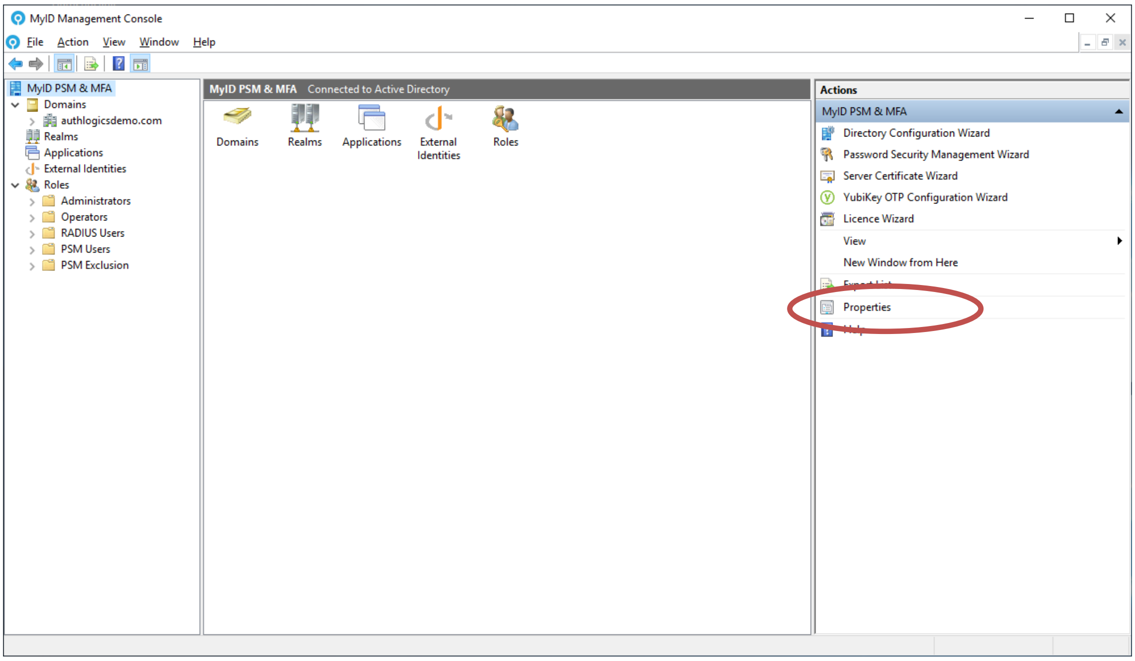
7. The User Account has been updated.
   Click *Finish* when done.

Global Settings walkthrough

The MyID global settings are a group of directory configuration options that apply to all MyID servers in the forest, they are not per-user settings.

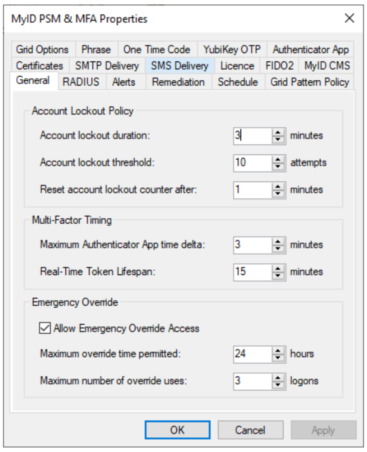
1. Open the MyID Authentication Server Management Console.
2. Highlight the high-level **MyID** node. The node name will include the product name based on the installed licences, e.g. PSM and/or MFA).

   Click *Properties* in the Actions pane.


MyID Management Console
File Action View Window Help
MyID PSM & MFA
Domains
authlogicsdemo.com
Realms
Applications
External Identities
Roles
Administrators
Operators
RADIUS Users
PSM Users
PSM Exclusion
MyID PSM & MFA Connected to Active Directory
Domains
Realms
Applications
External Identities
Roles
Actions
MyID PSM & MFA
Directory Configuration Wizard
Password Security Management Wizard
Server Certificate Wizard
YubiKey OTP Configuration Wizard
Licence Wizard
View
New Window from Here
Export List
Properties
Help

General Tab

The General tab contains the Account Lockout Policy, Multi-Factor Factor Timing and Emergency Override options.



MyID PSM & MFA Properties

Account Lockout Policy

Account lockout duration: 3 minutes

Account lockout threshold: 10 attempts

Reset account lockout counter after: 1 minutes

Multi-Factor Timing

Maximum Authenticator App time delta: 3 minutes

Real-Time Token Lifespan: 15 minutes

Emergency Override

☑ Allow Emergency Override Access

Maximum override time permitted: 24 hours

Maximum number of override uses: 3 logons

Account Lockout Policy settings take effect when a user logs on incorrectly after the specified invalid logon attempts within the lockout counter period. Accounts that have registered invalid attempts within the period, will be locked out for the lockout duration.

Allowed soft token time delta allows you to configure how many minutes difference you will allow the clock of a 2-factor device to be compared to the MyID server.

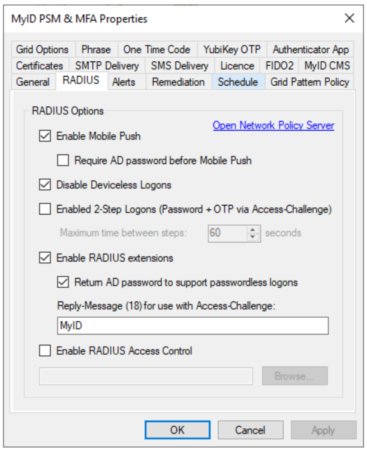
Real-time Token Lifespan provides the number in minutes that a Real-Time token can be used for before it expires. After this period has exceeded, the token will no longer be able to be used.

Emergency Override is a feature that allows a user to log in with a temporary PIN or password in an emergency. This is done by providing the user with a PIN or password and the usage of the password is limited by time, or by the number of uses. Unlike a standard password, the Emergency Override PIN or password is self-managed and will expire automatically.

The default time limit for Emergency Override use is *24 hours* and *3 logons*. Once these limits are reached, or the user logs on with either deviceless or Multi-Factor Authentication, the emergency is over and the user's emergency access is automatically removed.

RADIUS Tab

The RADIUS tab allows you to configure RADIUS options that are not available within Microsoft NPS.



RADIUS Options

☑ Enable Mobile Push

☐ Require AD password before Mobile Push

☑ Disable Deviceless Logons

☐ Enabled 2-Step Logons (Password + OTP via Access-Challenge)

Maximum time between steps: 60 seconds

☑ Enable RADIUS extensions

☑ Return AD password to support passwordless logons

Reply-Message (18) for use with Access-Challenge: MyID

☐ Enable RADIUS Access Control

MyID RADIUS supports Mobile Push authentication over RADIUS which can be enabled or disabled as required.

Enable *Require AD password Before Mobile Push* if you only want a Push to be sent after a password has been successfully verified. This is performed in a single RADIUS request. When disabled, a Push will be sent to the user with only a username being received over RADIUS.

Disable Deviceless Logons, when enabled, prevents users from using Grid Pattern and Phrase OTPs generated in deviceless mode and forces users to use a 2-factor generated OTP for RADIUS connections.

A 2-step logon process can be configured using the RADIUS Access-Challenge attribute buy setting the *Enable 2-Step Logons* option. When enabled, the first step is to validate the username and AD password, if successful an Access-Challenge is returned to the RADIUS client. The second step is to validate the username and OTP after which an Access-Accept will be returned to the RADIUS client.

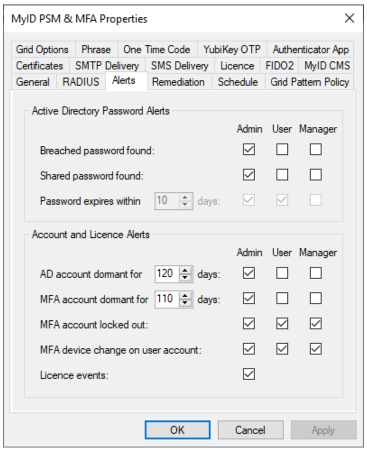
> **Step 1:** If the AD password is valid then Access-Challenge will be returned to tell the RADIUS client to request an OTP. If the AD password is invalid then an Access-Reject will be returned.
>
> **Step 2:** If the OTP is received within the allowed time (60 seconds by default) and it is valid an Access-Accept will be returned. If the OTP is invalid another Access-Challenge will be returned to prompt the RADIUS client to request a new OTP. An Access-Reject will be returned for any OTP received after the allowed time.

RADIUS extensions can be enabled to send additional metadata about the user to the RADIUS client. Additionally, the user's password can be returned to the RADIUS client to support Single Sign-On (e.g. on Citrix Access Gateways). The password is returned as clear text over RADIUS, however, it is encrypted in transit using the RADIUS shared secret. Returning the password requires the MyID Password Vault to be enabled on the Active Directory tab.

An optional RADIUS access control group can be configured on this tab, or via the Roles section of the MMC UI. This provides a level of access control over which users are allowed to use RADIUS authentication. Users who are not a member of the specified group will fail RADIUS logon request.

Alerts Tab

The Alerts tab allows you to configure multiple alerting options based on the type of event and the recipient.



Active Directory Password Alerts

	Admin	User	Manager
Breached password found:	☑	□	□
Shared password found:	☑	□	□
Password expires within 10 days:	☑	☑	□

Account and Licence Alerts

	Admin	User	Manager
AD account dormant for 120 days:	☑	□	□
MFA account dormant for 110 days:	☑	□	□
MFA account locked out:	☑	☑	☑
MFA device change on user account:	☑	☑	☑
Licence events:	☑		

Note

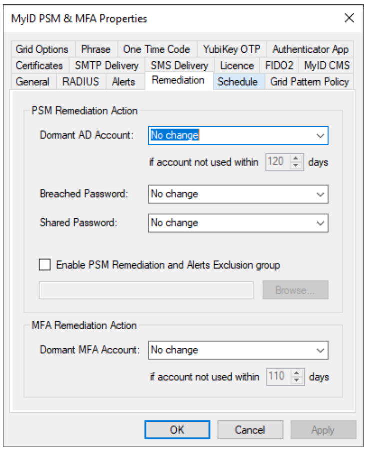
Alerts are sent via SMTP and cannot be configured unless an SMTP server is configured first. The options available are dependent on which licence types are installed and which PSM policies are configured.

Administrators will receive a summary email instead of individual emails per user whenever possible. Administrator emails are sent to the email address of all the accounts in the Authlogics Administrators role if any.

If a Manager is selected, an alert will be sent to the email address of the user account specified as the “Manager” for the user account within Active Directory. If no manager has been specified, then the alert will not be sent.

Remediation Tab

The Remediation tab allows you to configure an automatic resolution based on the type of condition found.



PSM Remediation Action

Dormant AD Account: No change

if account not used within 120 days

Breached Password: No change

Shared Password: No change

□ Enable PSM Remediation and Alerts Exclusion group

MFA Remediation Action

Dormant MFA Account: No change

if account not used within 110 days

Remediation provides an automated way to fix common user account issues to prevent security breaches. Automating these fixes is important as they are time-sensitive and often overlooked by manual processes.

If a breached, shared or dormant account is found then an account can be set to:

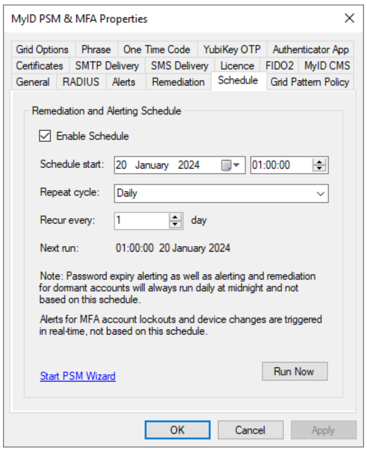
- No change
- Must change at next logon
- Account is disabled

“No change” is configured by default and it is recommended to analyse the administrator alerts prior to enabling remediation in order to assess the impact of initially enabling it.

It is recommended that dormant accounts and dormant MFA accounts are set to “Account is disabled” while breached and shared accounts be set to “Must change at next logon”.

Schedule Tab

The Schedule tab allows you to configure when *Breached and Shared* password remediation and alerting will take place.


MyID PSM & MFA Properties
Grid Options | Phrase | One Time Code | YubiKey OTP | Authenticator App
Certificates | SMTP Delivery | SMS Delivery | Licence | FIDO2 | MyID CMS
General | RADIUS | Alerts | Remediation | Schedule | Grid Pattern Policy
Start PSM Wizard
Run Now
OK
Cancel
Apply

Remediation and Alerting Schedule

☑ Enable Schedule

Schedule start: 20 January 2024 01:00:00

Repeat cycle: Daily

Recur every: 1 day

Next run: 01:00:00 20 January 2024

Note: Password expiry alerting as well as alerting and remediation for dormant accounts will always run daily at midnight and not based on this schedule.

Alerts for MFA account lockouts and device changes are triggered in real-time, not based on this schedule.

It is recommended to run the schedule daily out of hours, however, this can be customised as required. The processing work is ONLY performed on the primary MyID Server.

To run a check as soon as possible without waiting for the schedule click the Run Now button. This will begin the process within the next 15 mins.

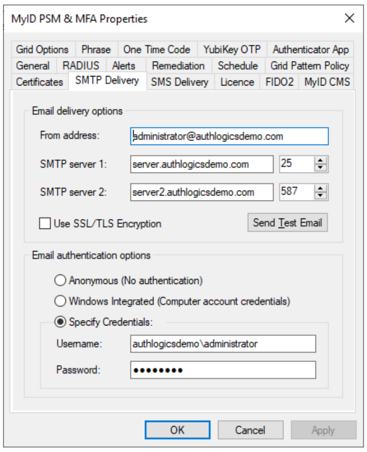
Note

Password expiry alerting as well as alerting and remediation for dormant accounts will always run daily at midnight and not based on this schedule.

Alerts for MFA account lockouts and device changes are triggered in real-time, not based on this schedule.

SMTP Delivery Tab

When users provisioned using the MyID Management Console they can receive an email with details of how to access the Self Service Portal, their initial pattern, PINs and other necessary logon information. Alerts will also be sent to administrators via email. The SMTP Delivery tab allows administrators to set the SMTP host and port for the email server for email message delivery.



Email delivery options

From address: administrator@authlogicsdemo.com

SMTP server 1: server.authlogicsdemo.com 25

SMTP server 2: server2.authlogicsdemo.com 587

☐ Use SSL/TLS Encryption

Email authentication options

○ Anonymous (No authentication)

○ Windows Integrated (Computer account credentials)

● Specify Credentials:

Username: authlogicsdemo\administrator

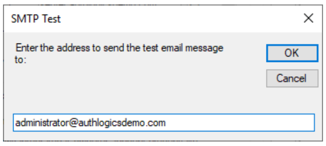
Password: ••••••••

The *From address* setting specifies the email address which delivered mail will be received from.

A primary SMTP must be specified to send an email. A secondary SMTP may be specified for redundancy purposes. The secondary server is only used if the sending fails via the primary server. Enter the *SMTP server 1* and *SMTP server 2* DNS names or IP addresses and corresponding port numbers. If the servers require an encrypted connection tick the *Use SSL/TLS Encryption* box.

If your email server requires authentication, select either *Use default Integrated credentials* or *Specify Credentials* and provide a username and password of an account with credentials to authenticate to the email server. These credentials are stored with 256bit AES asymmetric encryption.

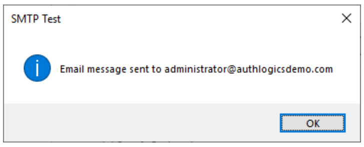
To ensure that the SMTP details are valid click *Send Test Email.*



Enter the address to send the test email message to:

administrator@authlogicsdemo.com

Enter a test email address and click OK.



Email message sent to administrator@authlogicsdemo.com

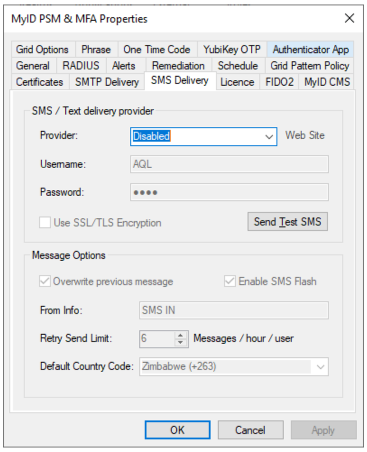
A confirmation that the message has been sent is displayed is the send was successful; if not an error stating the SMTP issue is displayed.

> **Note**
>
> When specifying email server details, ensure that the *From address* can deliver email to users through any anti-spam filters.

SMS Delivery Tab

The SMS Delivery tab allows administrators to set the SMS/Text delivery providers for SMS/Text message delivery and Message options. MyID can use SMS messages for delivery of 2-factor tokens to mobile devices without soft-tokens.

The administrator can also send notification or broadcast messages to one or many users via the MMC by right-clicking an account and selecting the *Send SMS* menu option.



SMS / Text delivery provider

Provider: Disabled

Username: AQL

Password: ••••

□ Use SSL/TLS Encryption

Message Options

☑ Overwrite previous message ☑ Enable SMS Flash

From Info: SMS IN

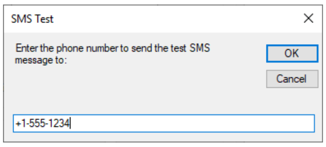
Retry Send Limit: 6 Messages / hour / user

Default Country Code: Zimbabwe (+263)

The provider list is pre-configured with some commonly used Internet-based SMS providers from around the globe. If you do not have an account with an SMS provider you can choose one from the list and click the "Web site" link to be taken directly to their signup page where you and typically signup for a free trial account.

Select your SMS provider and enter the Username and Password details for which they have provided.

To ensure that the SMS provider credentials are valid, click *Send Test SMS.*



Enter the phone number to send the test SMS message to:

+1-555-1234

Enter a test mobile number and click OK.

If you receive a Text message on the specified mobile device then the provider details are correct.

Some Providers allows messages to SMS messages from the same source to overwrite previous text messages. Select *Overwrite previous message.* For SMS messages to be delivered as a Flash SMS, select *Enable SMS Flash.*

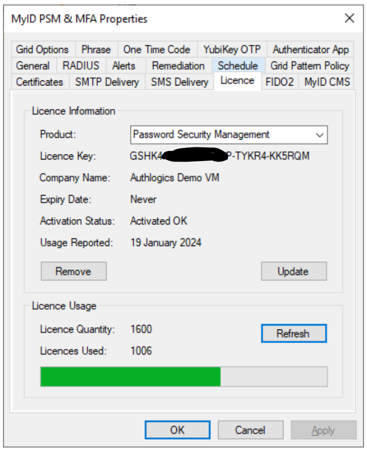
Enter the number that all messages will appear to be delivered from.

Retry Send Limit prevents more than the specified number of Text messages to be delivered to a specific user per hour.

The *Default Country Code* prefixes mobile phone numbers with the select dialling code for all mobile numbers that do not have an international dialling code.

Licence Tab

The Licence tab displays the loaded licence information.



Licence Information

Product: Password Security Management

Licence Key: GSHK4[redacted]P-TYKR4-KK5RQM

Company Name: Authlogics Demo VM

Expiry Date: Never

Activation Status: Activated OK

Usage Reported: 19 January 2024

Licence Usage

Licence Quantity: 1600

Licences Used: 1006

Details of the selected licence are displayed for your information, including the number of licences supported and the dates during which it is valid. Licence details of Multi-Factor Authentication and Password Security Management can be viewed and modified by selecting the Product from the drop-down list.

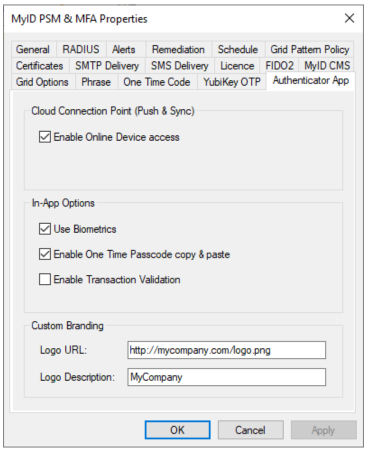
Licences can be removed by clicking the *Remove* button, which will be replaced by an *Add* button. Clicking the *Add* button starts the Licence Configuration Wizard.

The licence will be automatically refreshed periodically but MUST be updated at least every 60 days. If your licence details change, i.e. you renew your subscription or purchase more user licences, or you want to manually update the usage reporting simply click the *Update* button to get the latest licence version from Intercede.

The number of used licences will be updated periodically; however, it can be updated as needed by clicking the *Refresh* button.

Authenticator App Tab

The Authenticator App tab allows you to customise the appearance and functionality of the Authlogics Authenticator App which is installed on mobile devices from popular App Stores.



Cloud Connection Point (Push & Sync)

☑ Enable Online Device access

In-App Options

☑ Use Biometrics

☑ Enable One Time Passcode copy & paste

☐ Enable Transaction Validation

Custom Branding

Logo URL: http://mycompany.com/logo.png

Logo Description: MyCompany

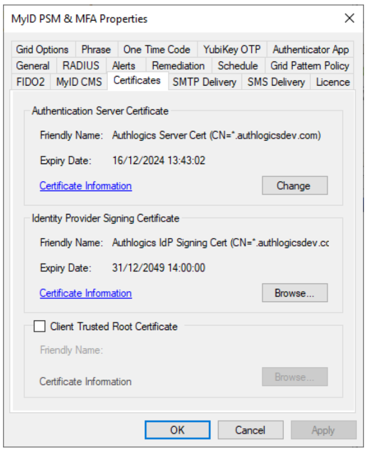
To allow the Authenticator App to perform an online pairing and Mobile Push authentication ensure the “Enable Online Device access” option is checked.

The in-app Authenticator App options can also be customised. Once these are set they cannot be changed by the user.

To show a custom logo at the top of the Authenticator App enter a Public URL to a graphic file that the mobile device can access. When provisioned, the Authenticator App will access the URL to download the graphic and store it within the Authenticator App. The graphic should be a 900 x 210 transparent PNG image. For accessibility purposes, it is also recommended to enter a description for the logo which may simply be the company name, for example.

Certificates Tab

The Certificates tab allows you to change the MyID Server and Identity Provider Signing certificates which are used to secure the MyID data stored in Active Directory and the Server Password Vault and sign Identity Provider requests. By default, the installation program will generate self-signed certificates. These are NOT the certificates used by IIS for HTTPS (SSL) connections to the server.



Authentication Server Certificate

Friendly Name: Authlogics Server Cert (CN=*.authlogicsdev.com)

Expiry Date: 16/12/2024 13:43:02

Certificate Information

Identity Provider Signing Certificate

Friendly Name: Authlogics IdP Signing Cert (CN=*.authlogicsdev.cc

Expiry Date: 31/12/2049 14:00:00

Certificate Information

□ Client Trusted Root Certificate

Friendly Name:

Certificate Information

The MyID Server Certificate contains the Public and Private keys used to asymmetrically encrypt and decrypt the stored data. An instance of the certificate, along with its Private Key, must be installed on each MyID Server in the Windows Computer certificate store. If the Private Key is not available the Authentication Server cannot operate.

Warning

If the Private Key is lost it is NOT possible to recover the MyID data stored in Active Directory.

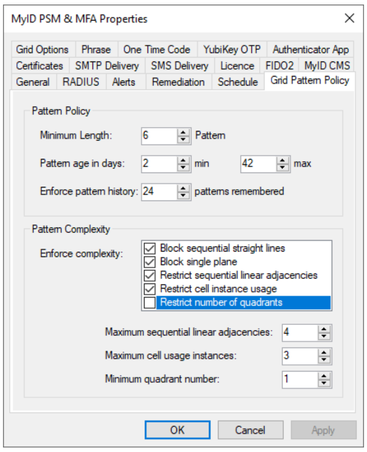
The MyID IdP Signing Certificate contains the Public and Private keys used to asymmetrically encrypt and decrypt Identity Provider Signing requests. An instance of the certificate, along with its Private Key, must be installed on each MyID Server in the Windows Computer certificate store. If the Private Key is not available the IdP services cannot operate.

If using Windows Desktop Agent, you can select an MyID *Server Certificate Trusted Root* certificate. If there is an enterprise CA available then a CA root certificate can be specified. This will require all MyID Desktop Agent machines to have a certificate installed on them which was issued from the specified root. If such a certificate is unavailable, some of the agent's features will not be available, e.g. offline and Passwordless logons. If an MyID *Server Certificate Trusted Root* certificate is not configured then the default Self Signed Certificates will be used.

Windows Desktop Agents connecting to the MyID Authentication Server using the External Access Server role must have a trusted certificate installed on it so that it have be validated by the MyID Authentication Server. If trusted certificates are not deployed on desktop PC's then check the *Disable External Access Trusted Certificate Checks* to allow untrusted External Access connections.

Grid Pattern Policy Tab

This tab configures the pattern policy and complexity settings.



Pattern Policy

Minimum Length: 6 Pattern

Pattern age in days: 2 min 42 max

Enforce pattern history: 24 patterns remembered

Pattern Complexity

Enforce complexity:

☑ Block sequential straight lines
☑ Block single plane
☑ Restrict sequential linear adjacencies
☑ Restrict cell instance usage
☐ Restrict number of quadrants

Maximum sequential linear adjacencies: 4

Maximum cell usage instances: 3

Minimum quadrant number: 1

The *Minimum length* settings determine the least number of characters allowed for a pattern. The larger the number, the more secure the patterns are but the more complex they are for users to manage.

The minimum and maximum *pattern age*, measured in days, prevents users from excessive changes of patterns within a short period and forces users to change their pattern regularly.

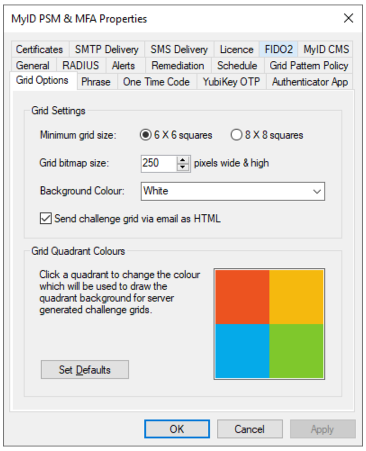
By enabling *enforce pattern history* an administrator can prevent users from re-using previously used patterns. Specify how many previous patterns are remembered.

Enforcing complexity ensures that users do not choose simple patterns which could be easily guessed. Administrators can enforce the following complexity checks:

- Block sequential straight lines
    - Block the use of a straight line in any direction in a contiguous chain and sequence.
- Block single plane
    - Block the usability to select all positions in a pattern that are on the same plane in any orientation, regardless of spacing or sequence. This would include a straight line.
- Restrict sequential linear adjacencies
    - Restrict the maximum number of allowed positions that are sequential and in a straight line before a gap and change of direction is required.
- Restrict cell instance usage
    - Restrict the number of times the same cell can be selected when choosing a pattern. For example, if the “Maximum cell usage instances” is 2 then a maximum of 2 cells, within the selected pattern, can be re-used.
- Restrict number of quadrants
    - Restrict the minimum number of quadrants a chosen pattern must use. For example, if the “Minimum quadrant number” is 2 then a pattern must use at least 2 of the 4 quadrants. While this encourages a user to choose a pattern that is well spread out it also limits the number of possible pattern combinations available.

Grid Options Tab

This tab configures generic and visual elements of MyID Grid authentication.



Grid Settings

Minimum grid size: ● 6 X 6 squares ○ 8 X 8 squares

Grid bitmap size: 250 pixels wide & high

Background Colour: White

☑ Send challenge grid via email as HTML

Grid Quadrant Colours

Click a quadrant to change the colour which will be used to draw the quadrant background for server generated challenge grids.

The *Minimum grid size* enforces the smallest size grids that users can have.

If the Authentication Server is used for deviceless logons then you can specify the dimensions of the PNG image that will be displayed on the client to suit the website/location you are displaying the image. You can also customise the background and grid colours used to display the squares in each quadrant of the grid.

Available Background Colours:

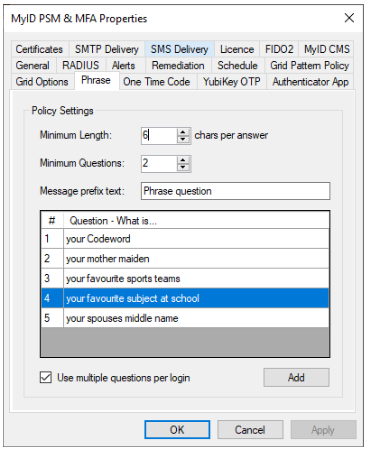
- Black
- Transparent
- White

When challenge grids are delivered via email, the *Send challenge grid via email as HTML* option sets whether challenge grids will be generated in plain text or as HTML.

To return the Quadrant Colours to the default colours, select the appropriate Background Theme and Click on the *Set Defaults* button.

Phrase Tab

This tab configures the standard Phrase policy settings.



Policy Settings

Minimum Length: 6 chars per answer

Minimum Questions: 2

Message prefix text: Phrase question

#	Question - What is...
1	your Codeword
2	your mother maiden
3	your favourite sports teams
4	your favourite subject at school
5	your spouses middle name

☑ Use multiple questions per login

The *Minimum Length* sets the minimum number of characters that a user must enter per answer.

The *Minimum Questions* setting allows an administrator to specify the minimum number of questions that a user must answer to be fully provisioned for phrase authentication. Phrase authentication allows administrators to create multiple questions and allow a user to select a subset of those questions to answer.

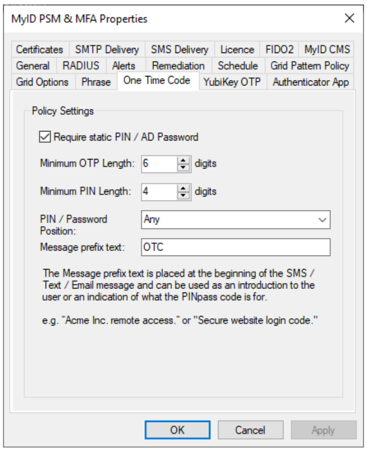
Set the *Message prefix text* that will precede all Phrase challenges which are sent to mobile devices.

By default, the only question is “your Codeword”, this is to cater for auto-provisioning whereby a user is provided with a random dictionary word to get them started. It is not recommended to change the first challenge question. To modify and add new Phrase challenge questions, Click *Add*.

Enable the *Use multiple questions per login* option to make Phrase randomly ask for letters from answers to multiple questions instead of picking random letters from a single answer. This option can increase security but may make it harder for users to login.

One Time Code Tab

This tab configures the standard One Time Code policy settings.



Policy Settings

☑ Require static PIN / AD Password

Minimum OTP Length: 6 digits

Minimum PIN Length: 4 digits

PIN / Password Position: Any

Message prefix text: OTC

The Message prefix text is placed at the beginning of the SMS / Text / Email message and can be used as an introduction to the user or an indication of what the PINpass code is for.

e.g. "Acme Inc. remote access." or "Secure website login code."

One Time Code (OTC) can be used as a single or Multi-Factor Authentication solution. To enforce Two Factor Authentication with OTC check the *Require PIN / AD Password* box so the user must enter a PIN code or Password along with an One Time PIN (OTP) when authenticating. This option is typically disabled when OTC is only being used to validate OTPs and static data such as a password is being verified elsewhere, or not at all.

The *Minimum OTP Length* sets the minimum number of digits allowed for an OTP code generated. The actual number of digits is set on a per-user basis but cannot be lower than this number.

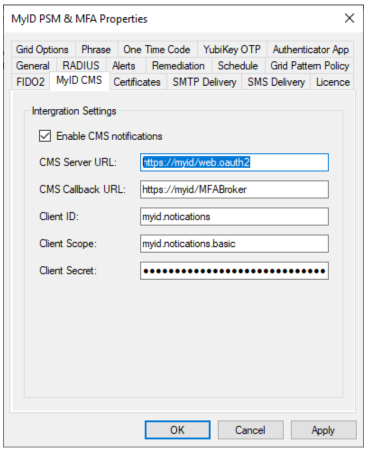
The *Minimum PIN Length* setting allows an administrator to specify the minimum number of digits in a user's static PIN code. This length is ignored when using Active Directory passwords in place of a PIN code.

The *PIN / Password position* dictates where users must enter the static PIN / Password in relation to the OTP. The default setting is *Any*.

Set the *Message prefix text* that will precede all OTC token challenges.

MyID CMS Tab

This tab configures the MyID CMS settings to allow for integration between the MyID MFA/PSM Server and the MyID CMS Server.



Intergration Settings

☑ Enable CMS notifications

CMS Server URL: https://myid/web.oauth2

CMS Callback URL: https://myid/MFABroker

Client ID: myid.notications

Client Scope: myid.notications.basic

Client Secret: ••••••••••••••••••••••••••••••

The following information is required to complete the configuration:

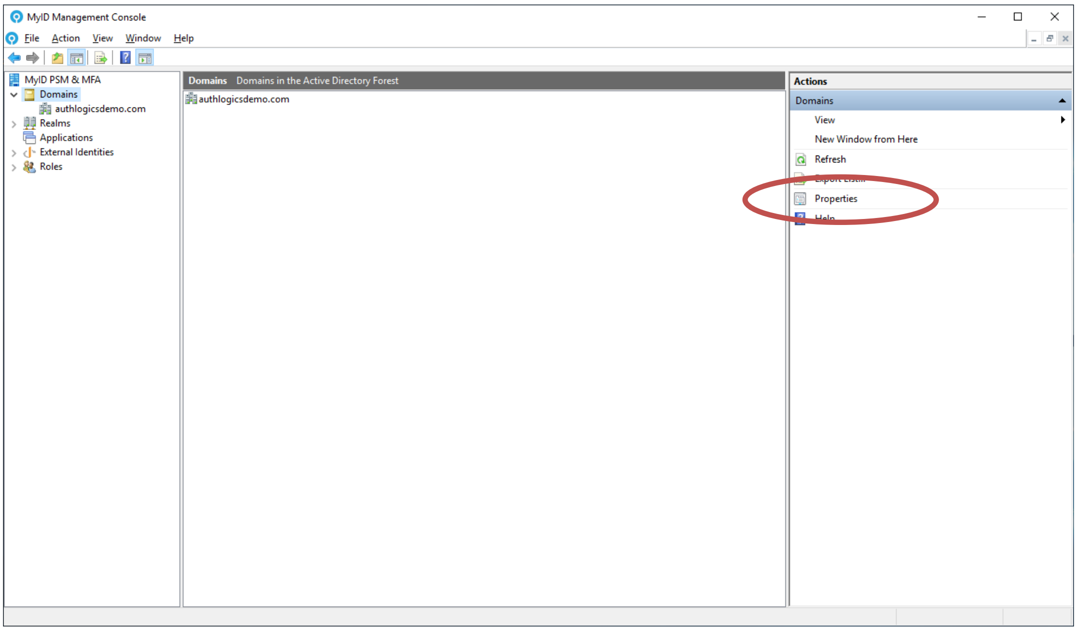
- The MyID CMS OAuth2 Authentication Service URL
  - e.g. **“https://myid/web.oauth2”**
- The MyID CMS MFA Broker Service URL
  - e.g. **“https://myid/MFABroker”.**
- The MyID CMS Client ID used to authenticate
  - e.g. “myid.notifications”
- The MyID CMS Client Scope use to authenticate
  - e.g. “myid.notifications.basic”
- The MyID CMS Client Secret used to authenticate
  - e.g. “4116e8f9-92e2-48b1-8616-5fb3d130b91d”

Domain Settings

The MyID Domain settings is a set of domain specific configuration options that apply to all MyID servers in the forest and are not per-user settings.

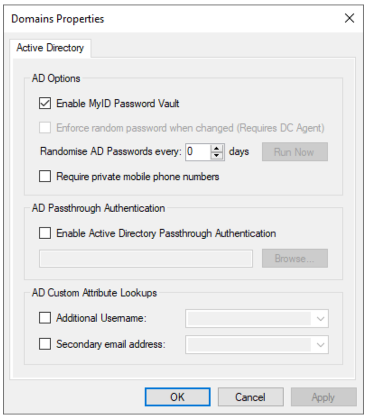
1. Open the MyID Authentication Server Management Console.
2. Highlight the **Domains** node.

   Click *Properties* in the Actions pane.



Domain Properties Tab

The Domain Properties tab allows administrators to control various Active Directory specific options.


Domains Properties

Active Directory

AD Options

☑ Enable MyID Password Vault

□ Enforce random password when changed (Requires DC Agent)

Randomise AD Passwords every: 0 days

□ Require private mobile phone numbers

AD Passthrough Authentication

□ Enable Active Directory Passthrough Authentication

AD Custom Attribute Lookups

□ Additional Username:

□ Secondary email address:

The *MyID Password Vault* is a secure storage location protected with AES 256-bit asymmetric encryption with certificates. The Vault is used to store user passwords to allow for Passwordless logons to Windows and other applications. This feature can be used in conjunction with the Windows Desktop Agent with Passwordless logons enabled. The Password Vault is disabled by default and must be explicitly enabled.

Randomise AD Password enables the MyID Server to automatically manage user passwords by setting them to a highly secure random value regularly. They are kept secure because the users never know what they are and they constantly change. This feature must be used in conjunction with MyID Agents which support Passwordless logons such as the Windows Desktop Agent with Passwordless logons enabled.

To enable this feature, specify how many days until the passwords must be randomly changed. Setting it to 0 disables the feature. You can also enable *Enforce random AD Password when changed* which will prevent a user's password from being reset/changed to a non-random password. If it is not enforced then the password reset will be allowed and the new password can be used until the next randomisation schedule. The block is done directly at the Domain Controller by the Domain Controller Agent which must be installed separately on all Domain Controllers.

To force password randomisation of all accounts click the "Run Now" button. This will cause the Password Policy Agent to run the password randomisation task within the next 15 mins.

To ensure that all user mobile phone numbers are kept private select "Require private mobile phone numbers". This setting ensures that mobile numbers are encrypted instead of using the clear text default mobile phone AD field.

AD Passthrough Authentication allows logon attempts to be passed directly to Active Directory for logon processing if a user has not been provisioned for MFA. AD Passthrough Authentication is only permitted for user accounts which are a member of a specified AD group and is disabled by default. To enable AD Passthrough Authentication, check the *Enable Active Directory Passthrough Authentication* box. Click *Browse…* and select an Active Directory group which contains the user accounts which are permitted to use AD Passthrough Authentication.

AD Custom Attribute Lookups enables MyID to use a custom LDAP attributes on a user account when looking up a user account name or secondary email address.

The *Additional Username* option may be useful to locate a user account via an employee number instead of an AD account name. If the employee number is stored in "extensionAttribute1" in AD then you can configure MyID to also look in the specified attribute. The custom field is used as a secondary addition to the standard Username or UPN, if an account match is found using the standard Username then the custom LDAP field will not be searched.

The *Secondary email address* option can be used to locate a secondary email address for a user account. The secondary email address can be used in the authentication provisioning wizards for sending welcome emails to.

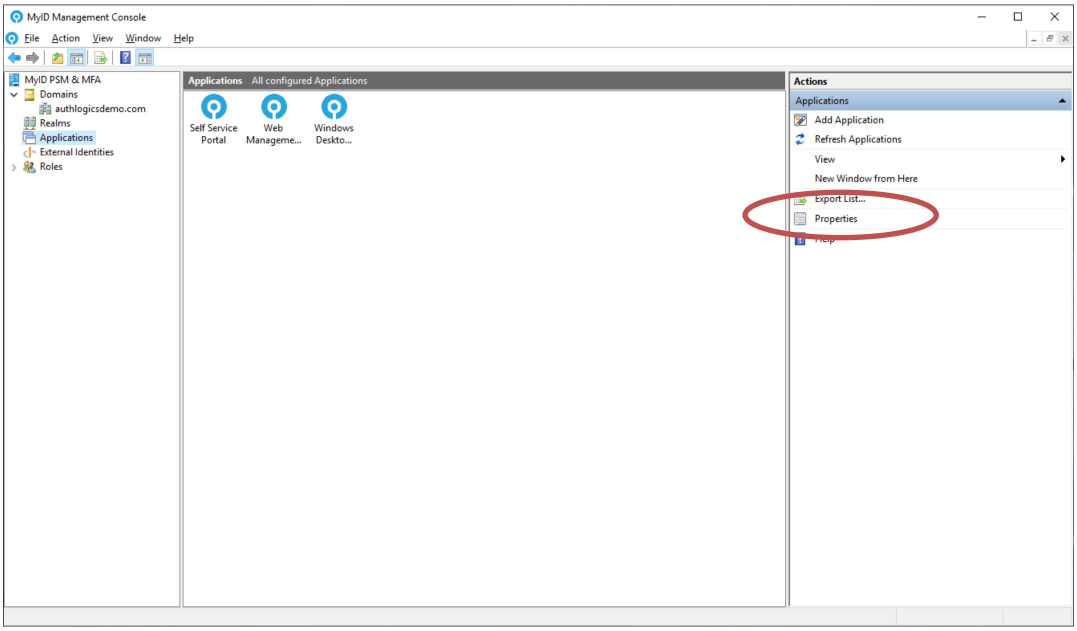
To enable a custom attribute lookup, check the box and select an LDAP attribute from the list which MyID should search.

Applications

Applications are all IdP published services and websites which require authentication. MyID includes 3 pre-configured applications; Self Service Portal, Web Admin Portal and Windows Desktop agent service.

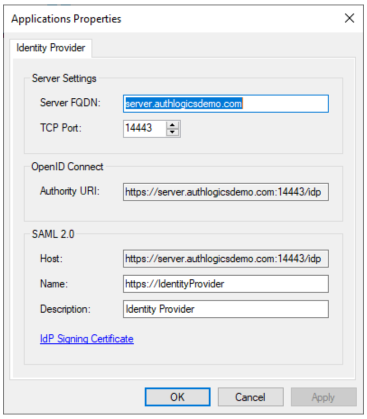
1. Open the MyID Authentication Server Management Console.
2. Highlight the **Applications** node.

   Click *Properties* in the Actions pane.



Applications Properties

The Applications Properties tab allows administrators to control the Identity Provider Server options. These properties apply to all MyID IdP servers in the forest and are not per-user settings.



Server Settings

Server FQDN: server.authlogicsdemo.com

TCP Port: 14443

OpenID Connect

Authority URI: https://server.authlogicsdemo.com:14443/idp

SAML 2.0

Host: https://server.authlogicsdemo.com:14443/idp

Name: https://IdentityProvider

Description: Identity Provider

The Server FQDN is the Fully-qualified Domain Name of the MyID IdP Server. The IdP Server operates on the HTTPs protocol and is bound to the Port specified within the TCP Port option. By default, the TCP Port is 14443.

The OpenID Connect Authority URI is dynamically built based on the Server FQDN and TCP Port settings.

For SAML 2.0 settings, the Host address is dynamically built based on the Server FQDN and TCP Port settings.

Enter your server NAME and Description for your MyID IdP Server. The active IdP signing certificate can be viewed by clicking on the IdP Signing Certificate link found on the tab.

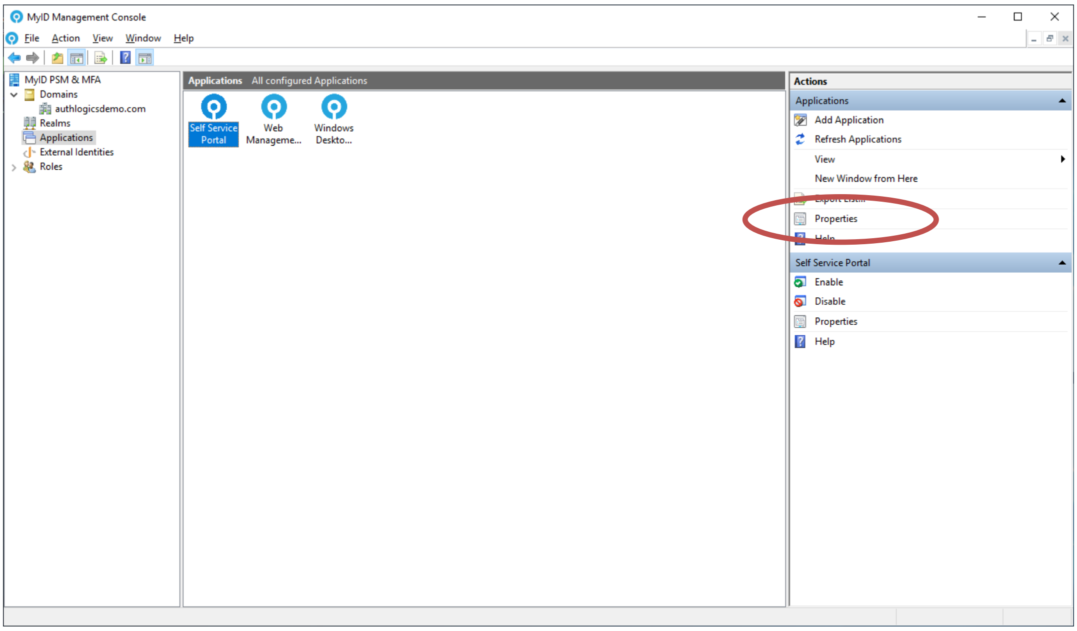
Self Service Portal Application Properties

The Self Service Portals tabs contains the customisation options for the Self Service Portal. The Authentication Server includes a user Self Service Portal where users can perform various common administrative tasks themselves such as register a new MFA device, change their Grid pattern, Phrase answers, static YubiKey and OTC PINs and reset their Active Directory password and update their mobile/cellular phone number. The Web Management Portal provides basic administration and operational capabilities suited to helpdesk personnel.

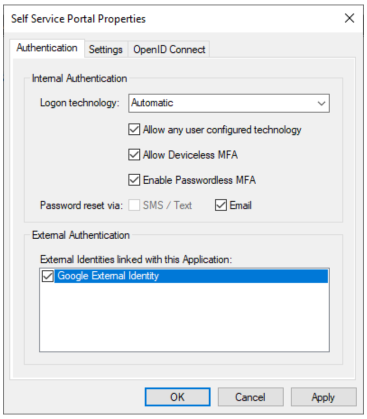
The portal is designed to be compatible with desktop and mobile browsers.

1. Open the MyID Authentication Server Management Console.
2. Highlight the **Self Service Portal** within the **Applications** node.

   Click *Properties* in the Actions pane.



Authentication Tab



Self Service Portal Properties

Internal Authentication

Logon technology: Automatic

☑ Allow any user configured technology

☑ Allow Deviceless MFA

☑ Enable Passwordless MFA

Password reset via: □ SMS / Text ☑ Email

External Authentication

External Identities linked with this Application:

☑ Google External Identity

Specify the logon technology users must use to authenticate to the portal. Options available are:

- Disabled
- Automatic (MFA only)
- Push
- Grid
- Phrase
- One Time Code
- Passkey
- YubiKey OTP
- Password (Active Directory password)
- Windows Authentication (pass-through authentication)
- Certificate

When an MFA licence is installed the default logon option for both portals is *Auto (MFA only)*. If only a PSM licence is installed the options are limited to *Password* and *Windows Authentication* with *Password* being the default logon option.

Automatic determines the most appropriate MFA technology that a user will authenticate with. If a user is enabled for multiple MFA technologies, the application will choose the highest security MFA technology based on in-built hierarchy.

The “Allow any user configured technology” allows a user to authenticate using any MFA technology they are provisioned for. If this option is not selected, the user must enter valid authentication credentials shown by the application only. Other MFA technology credentials that a user may be provisioned for will not work and they must provide the credentials display of the Self Service logon page.

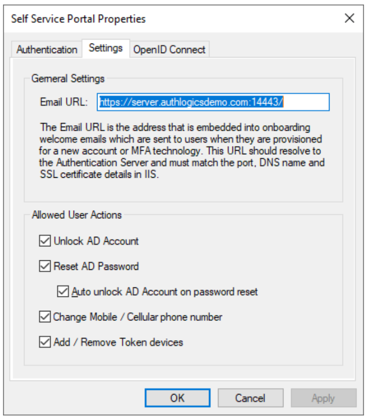
Grid and Phrase authentication technologies both support Deviceless authentication, check the “Allow Deviceless Logons” box to enable this support. If this is not enabled, then MFA will always be required.

The option of “Allow Passwordless MFA” enables passwordless logins. When disabled, users will be required to enter a valid AD password as well as their MFA credentials.

When only a PSM licence is installed the Self Service Portal can still issue One Time Codes via SMS/Text or Email for Active Directory Password reset purposes. To use this feature the logon type must be set to *Password* and either *SMS / Text* or *Email* must be checked.

The External Identities linked with this Application allows users to authenticate to the website or service using a pre-configured external identity provider (See External Identities)

Settings Tab



Gemeral Settings

Email URL: https://server.authlogicsdemo.com:14443/

The Email URL is the address that is embedded into onboarding welcome emails which are sent to users when they are provisioned for a new account or MFA technology. This URL should resolve to the Authentication Server and must match the port, DNS name and SSL certificate details in IIS.

Allowed User Actions

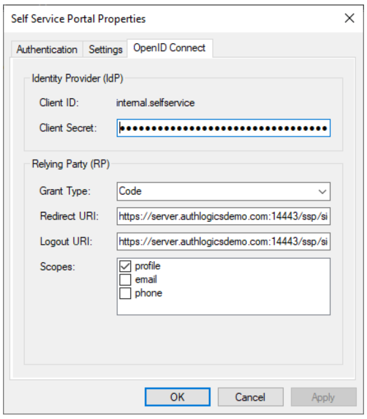
☑ Unlock AD Account
☑ Reset AD Password
☑ Auto unlock AD Account on password reset
☑ Change Mobile / Cellular phone number
☑ Add / Remove Token devices

The *Public URL* must be an accessible and resolvable web-based address that provides users access to the Self Service Portal hosted on the Authentication Server. The default HTTPS port (SSL) for the SSP is TCP:14443 although additional ports can be configured within IIS. A reverse proxy or SSL VPN device may be used to provide connectivity to the portal if required.

Administrators can enable or disable the user's ability to perform the following actions via the Self Service Portal (depending on the installed product licence):

- Allow users to reset their Active Directory Password
- Allow users to unlock their Active Directory Account
    - Auto unlock Active Directory Account when their password is reset
- Allow user to change their mobile/cellular phone number
- Allow users to add or remove token devices

OpenID Connect Tab



Identity Provider (IdP)

Client ID: internal.selfservice

Client Secret: ••••••••••••••••••••••••••••••••••

Relying Party (RP)

Grant Type: Code

Redirect URI: https://server.authlogicsdemo.com:14443/ssp/si

Logout URI: https://server.authlogicsdemo.com:14443/ssp/si

Scopes:
☑ profile
☐ email
☐ phone

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

Through this, you can specify the Self Service Portals' Grant Type, Redirect and Logout URIs and the scope for the relying party trust.

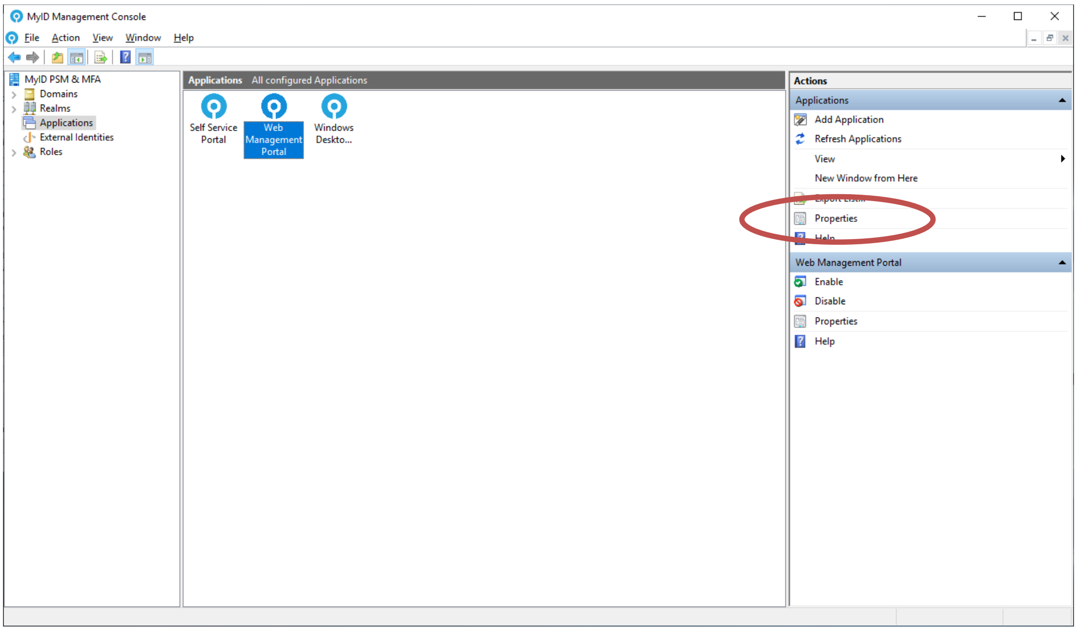
Web Management Portal Application Properties

The Web Management contains the customisation options for the Web Management Portal. The Authentication Server includes a user Web Management Portal where administrators and web operators can perform basic administration and operational capabilities suited to helpdesk personnel.

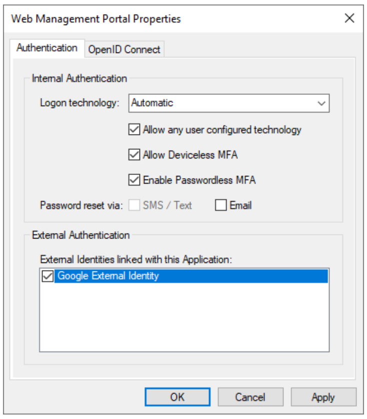
The portal is designed to be compatible with desktop and mobile browsers.

1. Open the MyID Authentication Server Management Console.
2. Highlight the **Web Management Portal** within the **Applications** node.

   Click *Properties* in the Actions pane.



Authentication Tab



Web Management Portal Properties

Internal Authentication

Logon technology: Automatic

☑ Allow any user configured technology

☑ Allow Deviceless MFA

☑ Enable Passwordless MFA

Password reset via: □ SMS / Text □ Email

External Authentication

External Identities linked with this Application:

☑ Google External Identity

Specify the logon technology users must use to authenticate to the portal. Options available are:

- Disabled
- Automatic (MFA only)
- Push
- Grid
- Phrase
- One Time Code
- Passkey
- YubiKey OTP
- Password (Active Directory password)
- Windows Authentication (pass-through authentication)
- Certificate

When an MFA licence is installed the default logon option for both portals is *Auto (MFA only)*. If only a PSM licence is installed the options are limited to *Password* and *Windows Authentication* with *Password* being the default logon option.

Automatic determines the most appropriate MFA technology that a user will authenticate with. If a user is enabled for multiple MFA technologies, the application will choose the highest security MFA technology based on in-built hierarchy.

The “Allow any user configured technology” allows a user to authenticate using any MFA technology they are provisioned for. If this option is not selected, the user must enter valid authentication credentials shown by the application only. Other MFA technology credentials that a user may be provisioned for will not work and they must provide the credentials display of the Web Management Portal logon page.

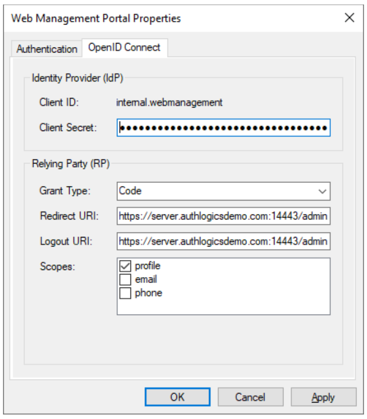
Grid and Phrase authentication technologies both support Deviceless authentication, check the “Allow Deviceless Logons” box to enable this support. If this is not enabled, then MFA will always be required.

The option of “Allow Passwordless MFA” enables passwordless logins. When disabled, users will be required to enter a valid AD password as well as their MFA credentials.

When only a PSM licence is installed the Web Management Portal can still issue One Time Codes via SMS/Text or Email for Active Directory Password reset purposes. To use this feature the logon type must be set to *Password* and either *SMS / Text* or *Email* must be checked.

The External Identities linked with this Application allows users to authenticate to the website or service using a pre-configured external identity provider (See External Identities)

OpenID Connect Tab



Web Management Portal Properties

Identity Provider (IdP)

Client ID: internal.webmanagement

Client Secret: ••••••••••••••••••••••••••••••••

Relying Party (RP)

Grant Type: Code

Redirect URI: https://server.authlogicsdemo.com:14443/admin

Logout URI: https://server.authlogicsdemo.com:14443/admin

Scopes:
☑ profile
☐ email
☐ phone

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

Through this, you can specify the Web Management Portals' Grant Type, Redirect and Logout URIs and the scope for the relying party trust.

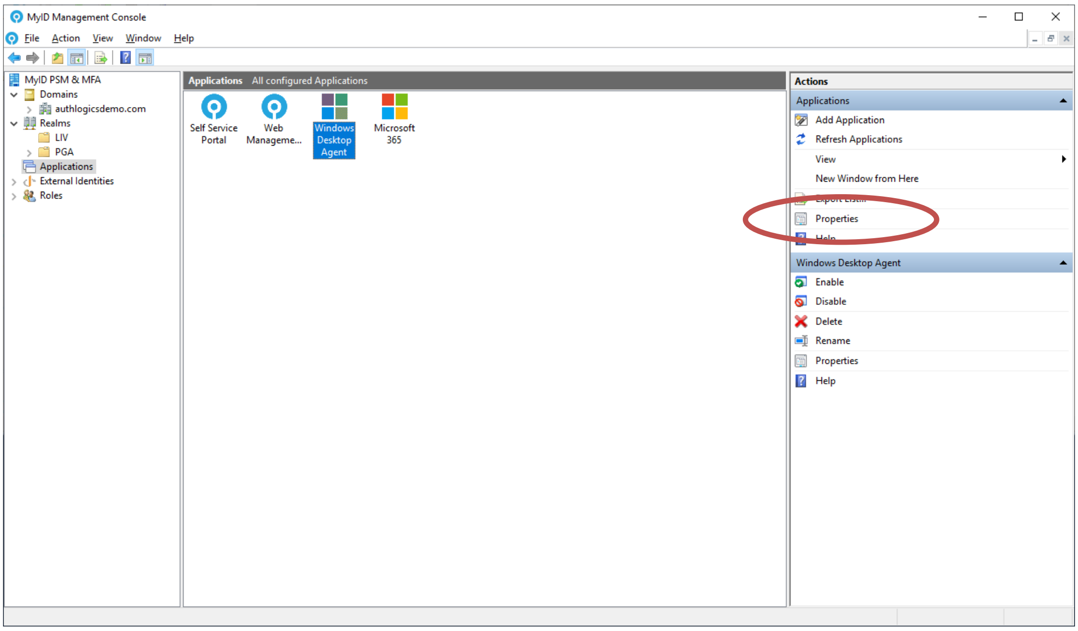
Windows Desktop Agent Application Properties

The MFA Windows Desktop Agent tabs contains the customisation options for the MyID MFA Windows Desktop Agent.

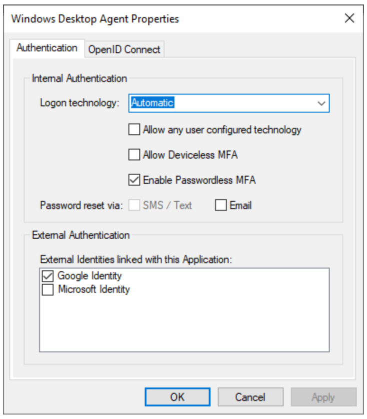
The portal is designed to be compatible with desktop and mobile browsers.

1. Open the MyID Authentication Server Management Console.
2. Highlight the **Windows Desktop Agent** within the **Applications** node.

   Click *Properties* in the Actions pane.


MyID Management Console
File Action View Window Help
MyID PSM & MFA
Domains
authlogicsdemo.com
Realms
LIV
PGA
Applications
External Identities
Roles
Applications All configured Applications
Self Service Portal
Web Manageme...
Windows Desktop Agent
Microsoft 365
Actions
Applications
Add Application
Refresh Applications
View
New Window from Here
Export List...
Properties
Help
Windows Desktop Agent
Enable
Disable
Delete
Rename
Properties
Help

Authentication Tab



Internal Authentication

Logon technology: Automatic

☐ Allow any user configured technology

☐ Allow Deviceless MFA

☑ Enable Passwordless MFA

Password reset via: ☐ SMS / Text ☐ Email

External Authentication

External Identities linked with this Application:

☑ Google Identity

☐ Microsoft Identity

Specify the logon technology users must use to authenticate to the portal. Options available are:

- Disabled
- Automatic (MFA only)
- Push
- Grid
- Phrase
- One Time Code
- Passkey
- YubiKey OTP
- Password (Active Directory password)
- Windows Authentication (pass-through authentication)
- Certificate

When an MFA licence is installed the default logon option for both portals is *Auto (MFA only)*. If only a PSM licence is installed the options are limited to *Password* and *Windows Authentication* with *Password* being the default logon option.

Automatic determines the most appropriate MFA technology that a user will authenticate with. If a user is enabled for multiple MFA technologies, the application will choose the highest security MFA technology based on in-built hierarchy.

The “Allow any user configured technology” allows a user to authenticate using any MFA technology they are provisioned for. If this option is not selected, the user must enter valid authentication credentials shown by the application only. Other MFA technology credentials that a user may be provisioned for will not work and they must provide the credentials display of the Windows Desktop Agents logon page.

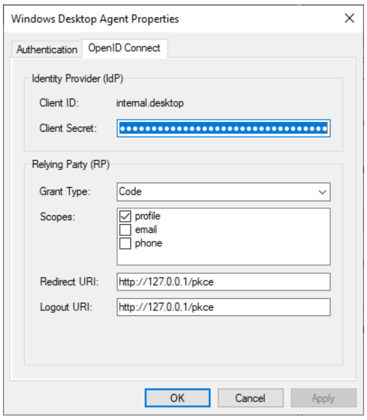
Grid and Phrase authentication technologies both support Deviceless authentication, check the “Allow Deviceless Logons” box to enable this support. If this is not enabled, then MFA will always be required.

The option of “Allow Passwordless MFA” enables passwordless logins. When disabled, users will be required to enter a valid AD password as well as their MFA credentials.

When only a PSM licence is installed the Self Service Portal can still issue One Time Codes via SMS/Text or Email for Active Directory Password reset purposes. To use this feature the logon type must be set to *Password* and either *SMS / Text* or *Email* must be checked.

The External Identities linked with this Application allows users to authenticate to the website or service using a pre-configured external identity provider (See External Identities)

OpenID Connect Tab



Windows Desktop Agent Properties

Identity Provider (IdP)

Client ID: internal.desktop

Client Secret: ••••••••••••••••••••••••••••••••

Relying Party (RP)

Grant Type: Code

Scopes:
- ☑ profile
- □ email
- □ phone

Redirect URI: http://127.0.0.1/pkce

Logout URI: http://127.0.0.1/pkce

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

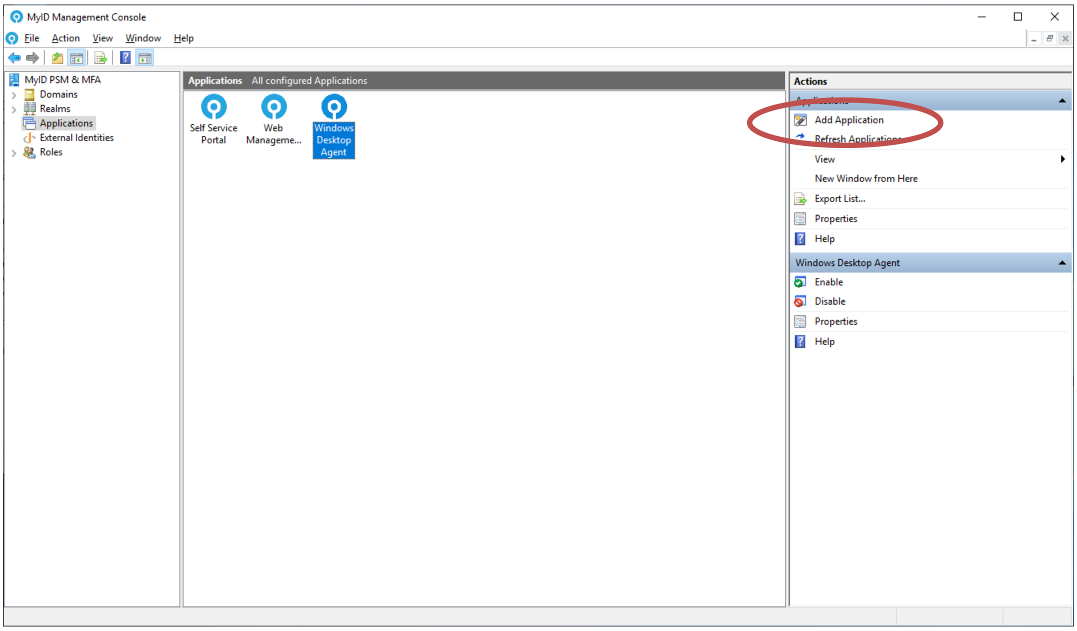
Through this, you can specify the Self Service Portals’ Grant Type, Redirect and Logout URIs and the scope for the relying party trust.

Adding New Applications

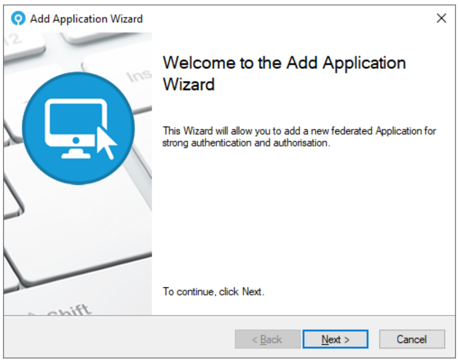
Additional websites and services can be added to the IdP Applications.

1. Open the MyID Authentication Server Management Console.
2. Highlight the **Applications** node.

   Click *Add Application* in the Actions pane.



Creating an OpenID Connect Application

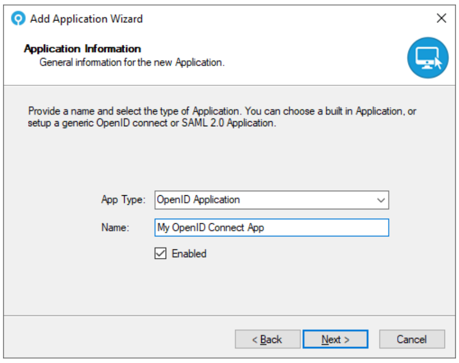


Welcome to the Add Application Wizard

This Wizard will allow you to add a new federated Application for strong authentication and authorisation.

To continue, click Next.

3. Click *Next.*



Add Application Wizard

Application Information

General information for the new Application.

Provide a name and select the type of Application. You can choose a built in Application, or setup a generic OpenID connect or SAML 2.0 Application.

App Type: OpenID Application

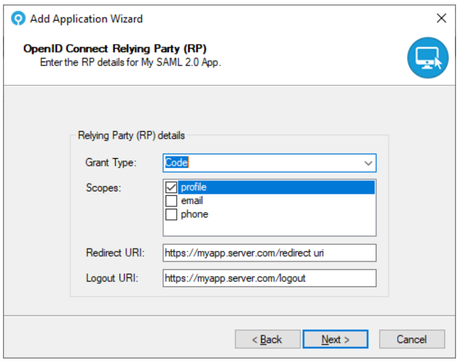
Name: My OpenID Connect App

☑ Enabled

4. Select App Type, provide a descriptive name for the application and set the application to be enabled.

   MyID Applications support applications of type:
   - OpenID Applications
   - SAML 2.0 Applications
   - MyID CMS
   - Microsoft 365

   Click Next



Add Application Wizard

OpenID Connect Relying Party (RP)

Enter the RP details for My SAML 2.0 App.

Relying Party (RP) details

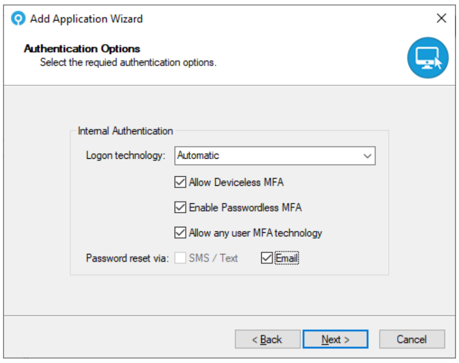
Grant Type: Code

Scopes: ☑ profile ☐ email ☐ phone

Redirect URI: https://myapp.server.com/redirect uri

Logout URI: https://myapp.server.com/logout

5. Enter the Relying Party trust details. These inputs will vary based on the App Type specified in the step above.
   Click Next



Add Application Wizard

Authentication Options

Select the requied authentication options.

Internal Authentication

Logon technology: Automatic

☑ Allow Deviceless MFA

☑ Enable Passwordless MFA

☑ Allow any user MFA technology

Password reset via: ☐ SMS / Text ☑ Email

6. Specify the logon technology users must use to authenticate to the portal. Options available are:

- Disabled
- Automatic (MFA only)
- Push
- Grid
- Phrase
- One Time Code
- Passkey
- YubiKey OTP
- Password (Active Directory password)
- Windows Authentication (pass-through authentication)
- Certificate

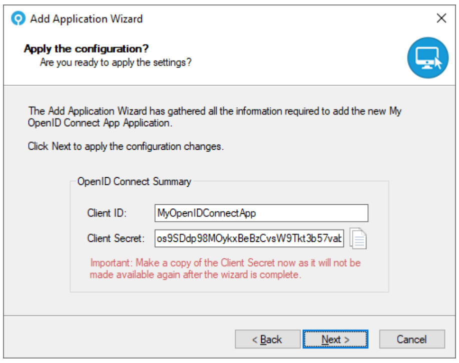
When an MFA licence is installed the default logon option for both portals is *Auto (MFA only)*. If only a PSM licence is installed the options are limited to *Password* and *Windows Authentication* with *Password* being the default logon option.

Automatic determines the most appropriate MFA technology that a user will authenticate with. If a user is enabled for multiple MFA technologies, the application will choose the highest security MFA technology based on in-built hierarchy.

The “Allow any user configured technology” allows a user to authenticate using any MFA technology they are provisioned for. If this option is not selected, the user must enter valid authentication credentials shown by the application only. Other MFA technology credentials that a user may be provisioned for will not work and they must provide the credentials display of the Windows Desktop Agents logon page.

Grid and Phrase authentication technologies both support Deviceless authentication, check the “Allow Deviceless Logons” box to enable this support. If this is not enabled, then MFA will always be required.

The option of “Allow Passwordless MFA” enables passwordless logins. When disabled, users will be required to enter a valid AD password as well as their MFA credentials.



Apply the configuration?
Are you ready to apply the settings?

The Add Application Wizard has gathered all the information required to add the new My OpenID Connect App Application.

Click Next to apply the configuration changes.

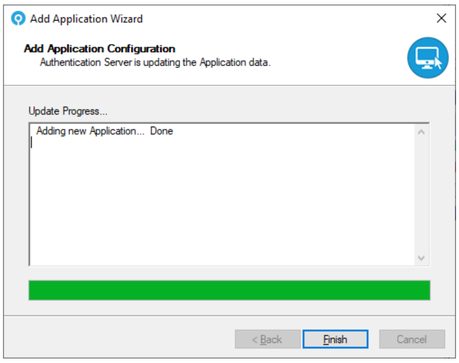
OpenID Connect Summary

Client ID: MyOpenIDConnectApp

Client Secret: os9SDdp98MOykxBeBzCvsW9Tkt3b57vak

Important: Make a copy of the Client Secret now as it will not be made available again after the wizard is complete.

7. Make a copy of the OpenID Connect client secret for integration with the calling application. Click *Next.*



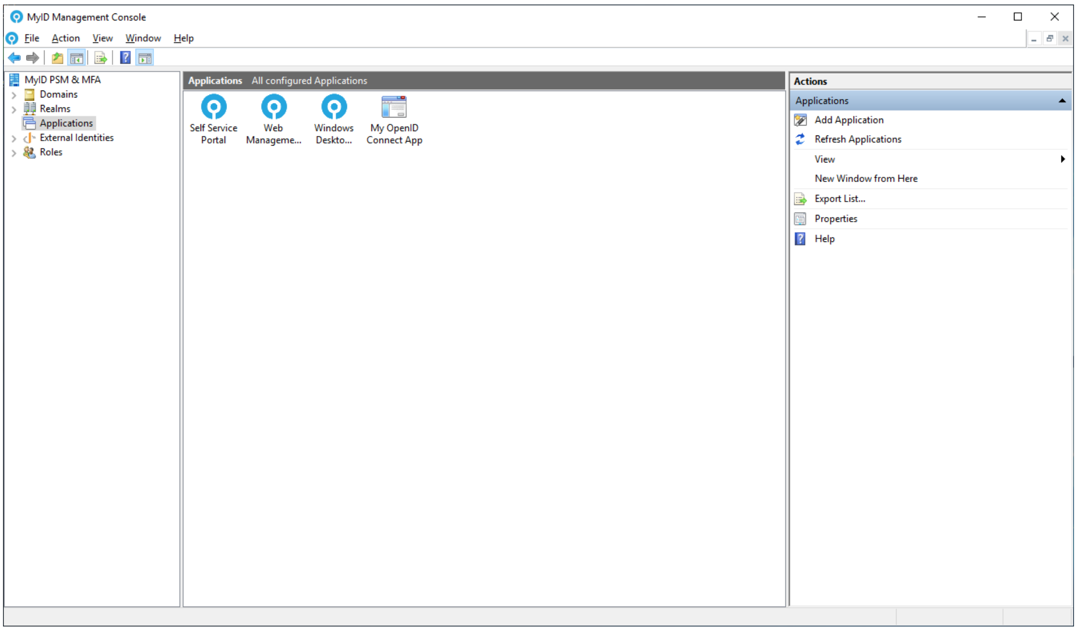
Add Application Wizard

Add Application Configuration
Authentication Server is updating the Application data.

Update Progress...

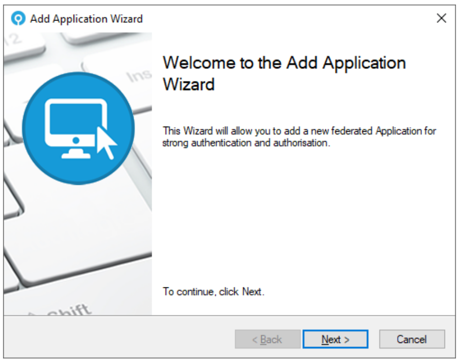
Adding new Application... Done

8. Click *Finish.*



Your application has now been configured.

Creating a SAML 2.0 Application



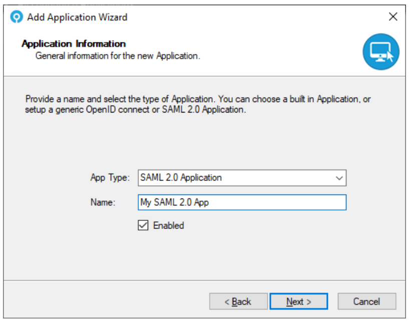
Add Application Wizard

Welcome to the Add Application Wizard

This Wizard will allow you to add a new federated Application for strong authentication and authorisation.

To continue, click Next.

1. Click *Next.*


Add Application Wizard

Application Information

General information for the new Application.

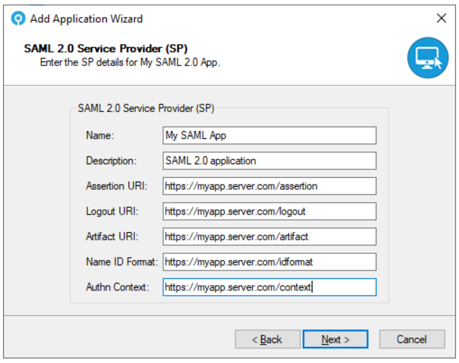
Provide a name and select the type of Application. You can choose a built in Application, or setup a generic OpenID connect or SAML 2.0 Application.

App Type: SAML 2.0 Application

Name: My SAML 2.0 App

☑ Enabled

2. Select SAML 2.0 Application, provide a descriptive name for the application and set the application to be enabled.
   Click Next


Add Application Wizard

SAML 2.0 Service Provider (SP)

Enter the SP details for My SAML 2.0 App.

SAML 2.0 Service Provider (SP)

Name: My SAML App

Description: SAML 2.0 application

Assertion URI: https://myapp.server.com/assertion

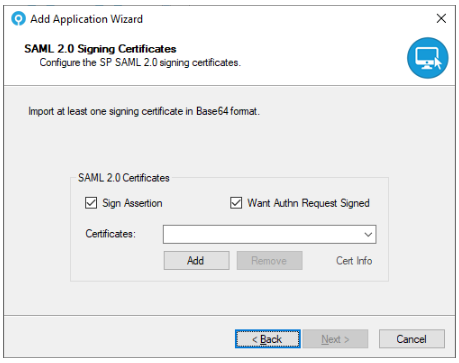
Logout URI: https://myapp.server.com/logout

Artifact URI: https://myapp.server.com/artifact

Name ID Format: https://myapp.server.com/idformat

Authn Context: https://myapp.server.com/context

3. Enter the Relying Party trust details. These inputs will vary based on the App Type specified in the step above.
   Click Next


Add Application Wizard

SAML 2.0 Signing Certificates

Configure the SP SAML 2.0 signing certificates.

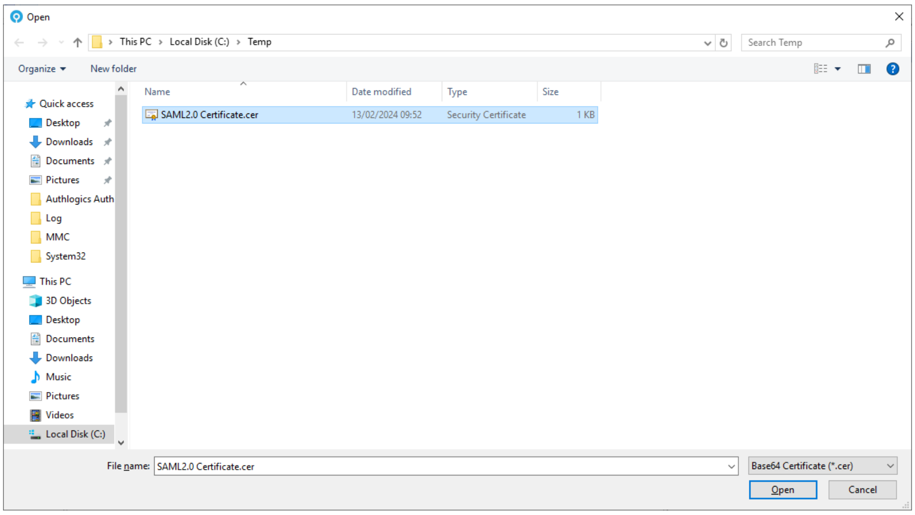
Import at least one signing certificate in Base64 format.

SAML 2.0 Certificates

☑ Sign Assertion ☑ Want Authn Request Signed

Certificates:

4. Enable *Sign Assertion* and *Want Authn Request Signed.* Select the SAML 2.0 signing certificate. Click Add.



Open

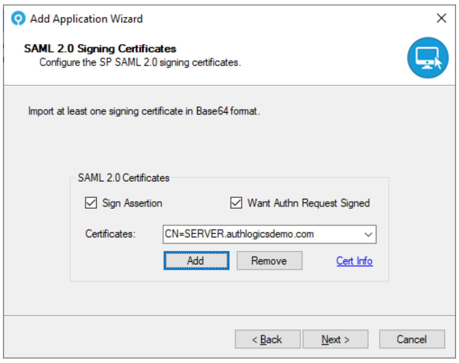
This PC > Local Disk (C:) > Temp

Name	Date modified	Type	Size
SAML2.0 Certificate.cer	13/02/2024 09:52	Security Certificate	1 KB

File name: SAML2.0 Certificate.cer

Base64 Certificate (*.cer)

Browse to the Signing Certificate and click *Open*.



Add Application Wizard

SAML 2.0 Signing Certificates

Configure the SP SAML 2.0 signing certificates.

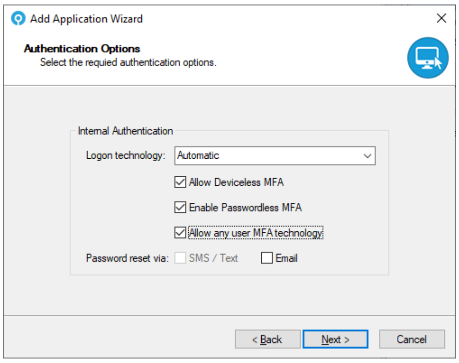
Import at least one signing certificate in Base64 format.

SAML 2.0 Certificates

☑ Sign Assertion ☑ Want Authn Request Signed

Certificates: CN=SERVER.authlogicsdemo.com

5. Click *Next.*



Add Application Wizard

Authentication Options

Select the requied authentication options.

Internal Authentication

Logon technology: Automatic

☑ Allow Deviceless MFA

☑ Enable Passwordless MFA

☑ Allow any user MFA technology

Password reset via: □ SMS / Text □ Email

6. Specify the logon technology users must use to authenticate to the portal. Options available are:

- Disabled
- Automatic (MFA only)
- Push
- Grid
- Phrase
- One Time Code
- Passkey
- YubiKey OTP

- Password (Active Directory password)
- Windows Authentication (pass-through authentication)
- Certificate

When an MFA licence is installed the default logon option for both portals is *Auto (MFA only)*. If only a PSM licence is installed the options are limited to *Password* and *Windows Authentication* with *Password* being the default logon option.

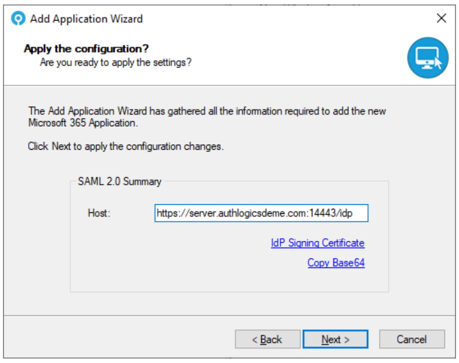
Automatic determines the most appropriate MFA technology that a user will authenticate with. If a user is enabled for multiple MFA technologies, the application will choose the highest security MFA technology based on in-built hierarchy.

The “Allow any user configured technology” allows a user to authenticate using any MFA technology they are provisioned for. If this option is not selected, the user must enter valid authentication credentials shown by the application only. Other MFA technology credentials that a user may be provisioned for will not work and they must provide the credentials display of the Windows Desktop Agents logon page.

Grid and Phrase authentication technologies both support Deviceless authentication, check the “Allow Deviceless Logons” box to enable this support. If this is not enabled, then MFA will always be required.

The option of “Allow Passwordless MFA” enables passwordless logins. When disabled, users will be required to enter a valid AD password as well as their MFA credentials.

Click *Next*.



Add Application Wizard

Apply the configuration?

Are you ready to apply the settings?

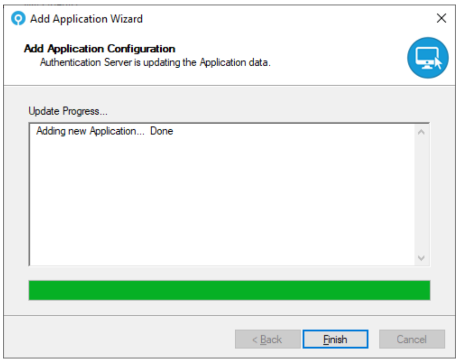
The Add Application Wizard has gathered all the information required to add the new Microsoft 365 Application.

Click Next to apply the configuration changes.

SAML 2.0 Summary

Host: https://server.authlogicsdeme.com:14443/idp

7. Confirm the Host configuration information.
   You can export or copy the IdP signing certificate at this stage which will be need by the SAML application. Click *Next.*



Add Application Wizard

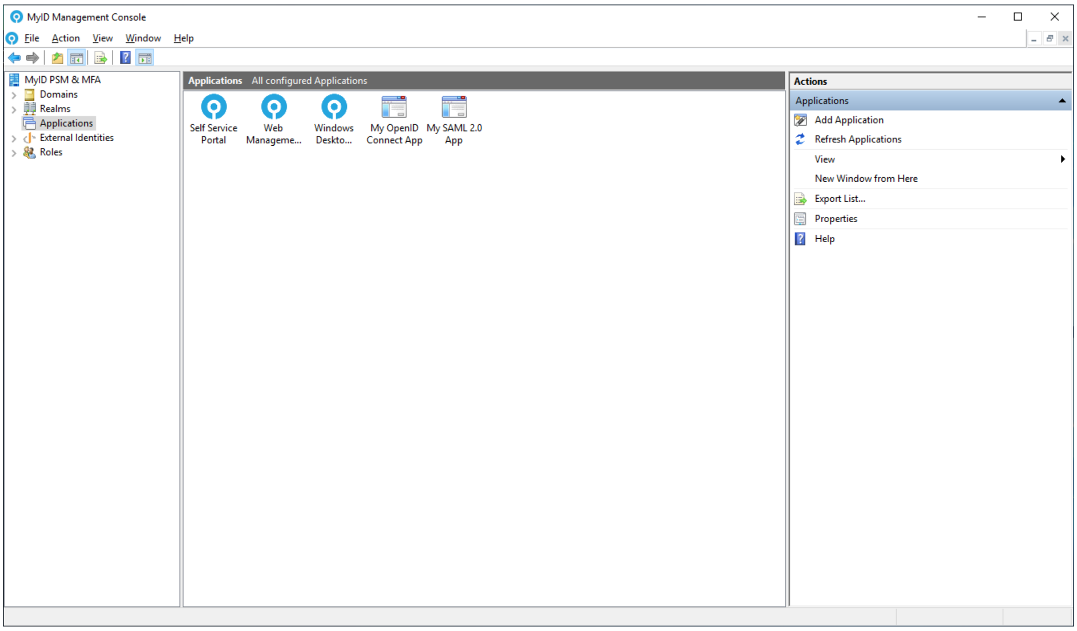
Add Application Configuration

Authentication Server is updating the Application data.

Update Progress...

Adding new Application... Done

8. Click *Finish.*



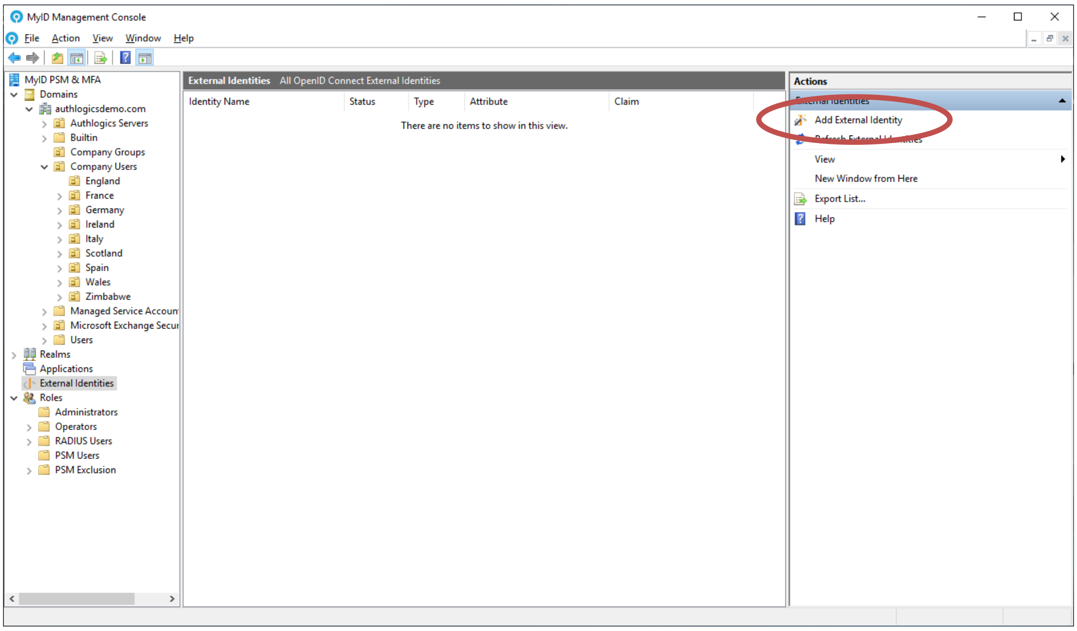
Your application has now been configured.

Adding External Identities

MyID supports OpenID Connect External Identity providers to be used as an authentication type for applications.

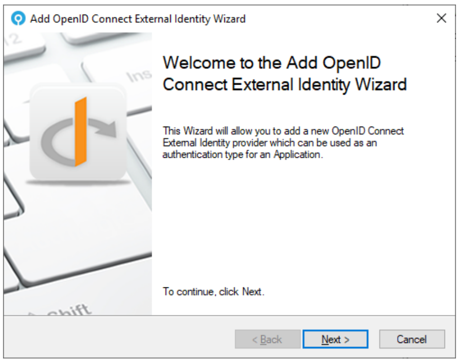
1. Open the MyID Authentication Server Management Console.
2. Highlight the **External Identities** node.

   Click *Add External Identity* in the Actions pane.



There are no items to show in this view.

Creating an OpenID Connect External Identity (Google)

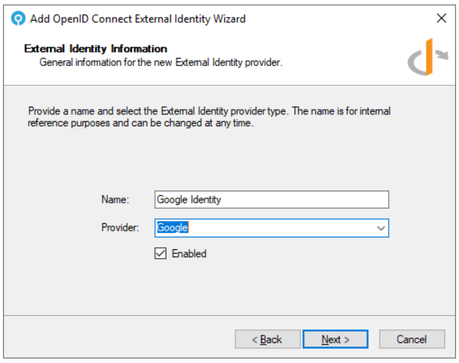


Welcome to the Add OpenID Connect External Identity Wizard

This Wizard will allow you to add a new OpenID Connect External Identity provider which can be used as an authentication type for an Application.

To continue, click Next.

3. Click *Next.*


Add OpenID Connect External Identity Wizard

External Identity Information
General information for the new External Identity provider.

Provide a name and select the External Identity provider type. The name is for internal reference purposes and can be changed at any time.

Name: Google Identity

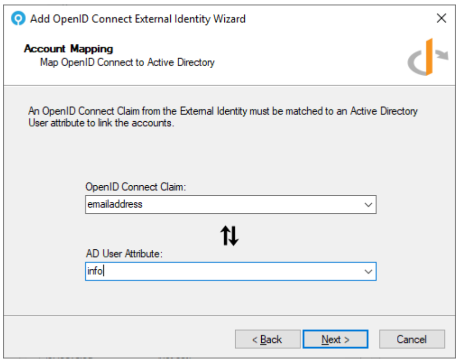
Provider: Google

☑ Enabled

4. Provide a descriptive name for the external identity and choose Google as the Provider. Set the External Identity to be enabled.

   MyID External Identities supports providers of type:
   - Google
   - Microsoft

   Click Next


Add OpenID Connect External Identity Wizard

Account Mapping
Map OpenID Connect to Active Directory

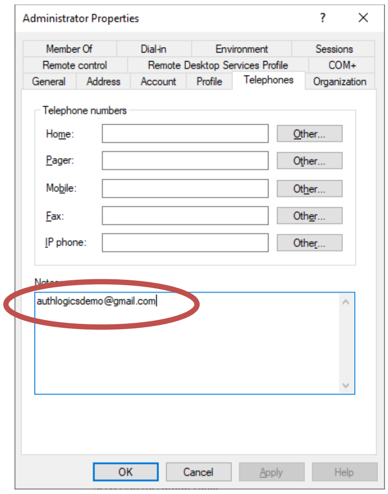
An OpenID Connect Claim from the External Identity must be matched to an Active Directory User attribute to link the accounts.

OpenID Connect Claim: emailaddress

AD User Attribute: info

5. Match the OpenID Connect Claim with the Active Directory User Attribute to link the accounts.

   In the example above, the user is being matched on the email address where the user's Google email address is stored in the user's Info field in AD.


Administrator Properties

Telephone numbers

Home:

Pager:

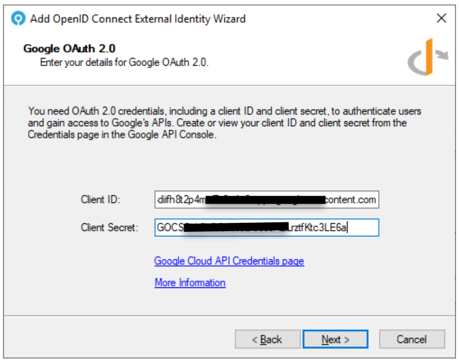
Mobile:

Fax:

IP phone:

Notes:
authlogicsdemo@gmail.com

Click Next



Add OpenID Connect External Identity Wizard

Google OAuth 2.0

Enter your details for Google OAuth 2.0.

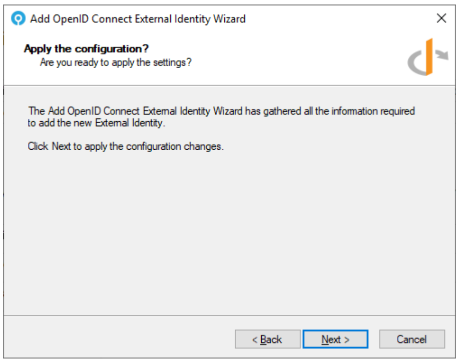
You need OAuth 2.0 credentials, including a client ID and client secret, to authenticate users and gain access to Google's APIs. Create or view your client ID and client secret from the Credentials page in the Google API Console.

Client ID: diifh8t2p4m[redacted]content.com

Client Secret: GOCS[redacted]rztfKtc3LE6a

6. Enter the Client ID and Client Secret retrieved from the Google Cloud API Credentials page.

   Click *Next.*



Add OpenID Connect External Identity Wizard

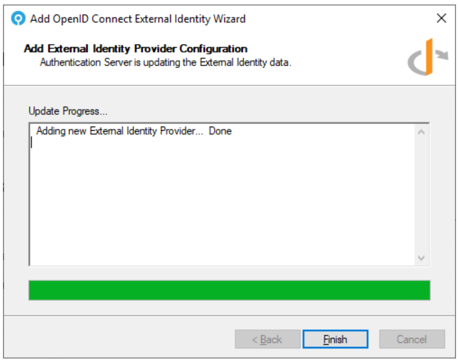
Apply the configuration?

Are you ready to apply the settings?

The Add OpenID Connect External Identity Wizard has gathered all the information required to add the new External Identity.

Click Next to apply the configuration changes.

7. Make a copy of the OpenID Connect client secret for integration with the calling application. Click *Next.*



Add OpenID Connect External Identity Wizard

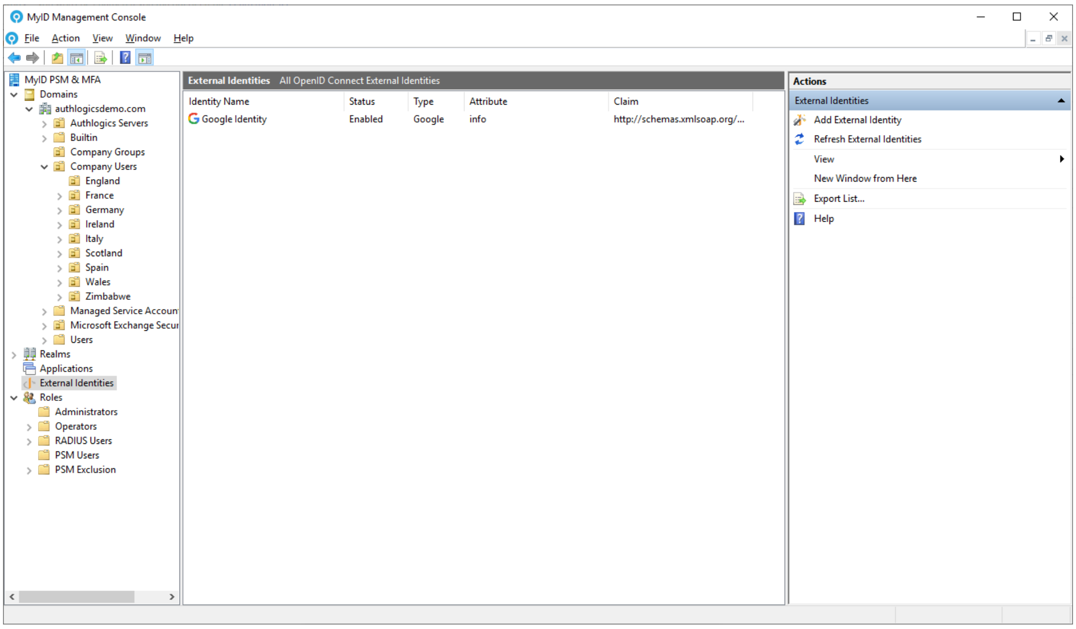
Add External Identity Provider Configuration

Authentication Server is updating the External Identity data.

Update Progress...

```
Adding new External Identity Provider... Done
```

8. Click *Finish.*

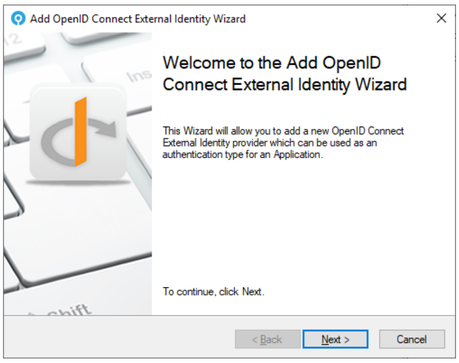


External Identities All OpenID Connect External Identities

Identity Name	Status	Type	Attribute	Claim
Google Identity	Enabled	Google	info	http://schemas.xmlsoap.org/...

Your Google External Identity has now been configured.

Creating an OpenID Connect External Identity (Microsoft)

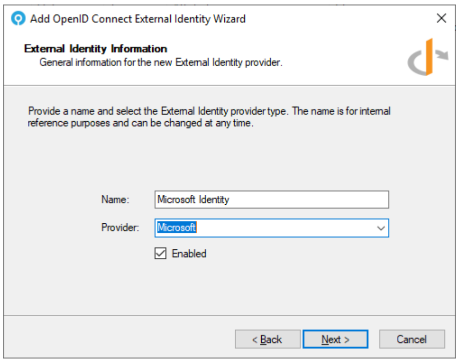

Add OpenID Connect External Identity Wizard

Welcome to the Add OpenID Connect External Identity Wizard

This Wizard will allow you to add a new OpenID Connect External Identity provider which can be used as an authentication type for an Application.

To continue, click Next.

1. Click *Next.*


Add OpenID Connect External Identity Wizard

External Identity Information

General information for the new External Identity provider.

Provide a name and select the External Identity provider type. The name is for internal reference purposes and can be changed at any time.

Name: Microsoft Identity

Provider: Microsoft

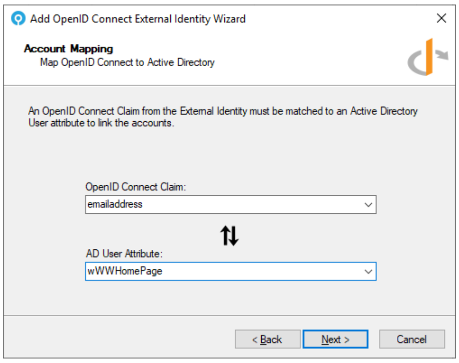
☑ Enabled

2. Provide a descriptive name for the external identity and choose Microsoft as the Provider. Set the External Identity to be enabled.

   MyID External Identities supports providers of type:

   - Google
   - Microsoft

Click Next



Add OpenID Connect External Identity Wizard

Account Mapping
Map OpenID Connect to Active Directory

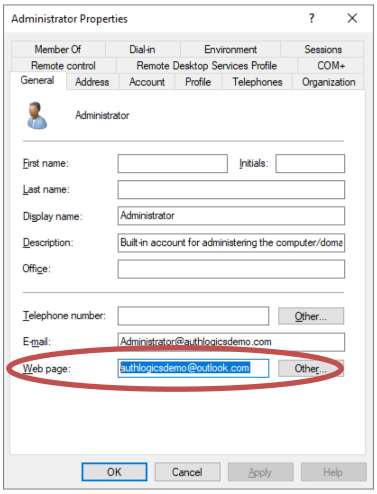
An OpenID Connect Claim from the External Identity must be matched to an Active Directory User attribute to link the accounts.

OpenID Connect Claim: emailaddress

AD User Attribute: wWWHomePage

3. Match the OpenID Connect Claim with the Active Directory User Attribute to link the accounts.

   In the example above, the user is being matched on the email address where the user's Microsoft Live email address is stored in the user's Web Page (wWWHomePage) field in AD.

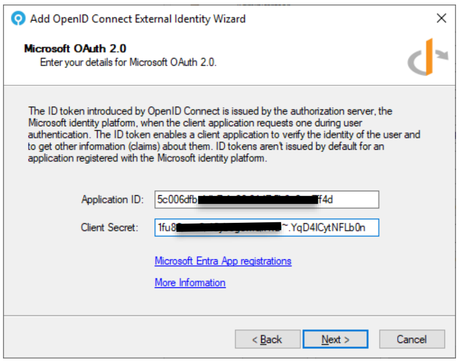


Administrator Properties

Administrator

First name:
Initials:
Last name:
Display name: Administrator
Description: Built-in account for administering the computer/doma
Office:
Telephone number:
E-mail: Administrator@authlogicsdemo.com
Web page: authlogicsdemo@outlook.com

Click Next



Add OpenID Connect External Identity Wizard

Microsoft OAuth 2.0
Enter your details for Microsoft OAuth 2.0.

The ID token introduced by OpenID Connect is issued by the authorization server, the Microsoft identity platform, when the client application requests one during user authentication. The ID token enables a client application to verify the identity of the user and to get other information (claims) about them. ID tokens aren't issued by default for an application registered with the Microsoft identity platform.

Application ID: 5c006dfb[redacted]f4d

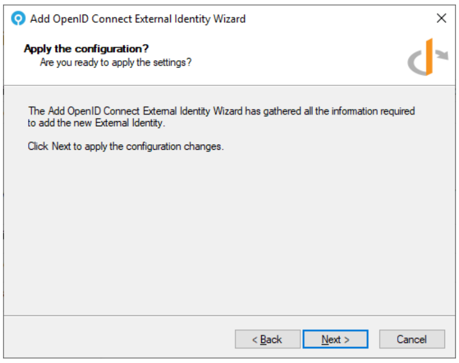
Client Secret: 1fu8[redacted]~YqD4lCytNFLb0n

Microsoft Entra App registrations

More Information

4. Enter the Application ID and Client Secret retrieved from the Microsoft Identity Platform.

Click *Next.*



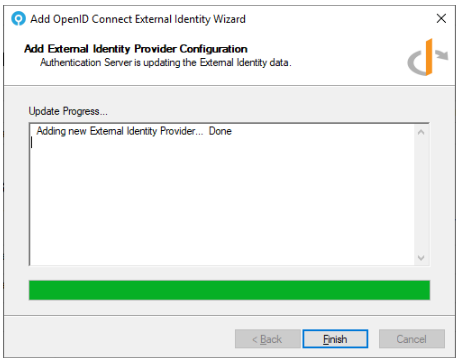
Apply the configuration?

Are you ready to apply the settings?

The Add OpenID Connect External Identity Wizard has gathered all the information required to add the new External Identity.

Click Next to apply the configuration changes.

5. Make a copy of the OpenID Connect client secret for integration with the calling application. Click *Next.*



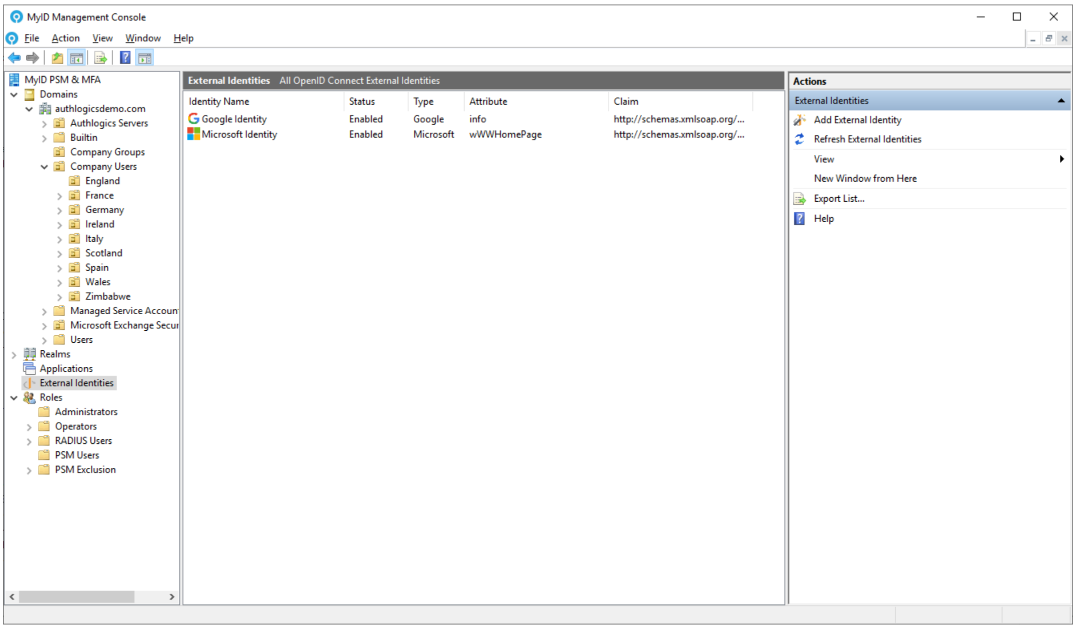
Add External Identity Provider Configuration

Authentication Server is updating the External Identity data.

Update Progress...

Adding new External Identity Provider... Done

6. Click *Finish.*



External Identities All OpenID Connect External Identities

Identity Name	Status	Type	Attribute	Claim
Google Identity	Enabled	Google	info	http://schemas.xmlsoap.org/...
Microsoft Identity	Enabled	Microsoft	wWWHomePage	http://schemas.xmlsoap.org/...

Your Microsoft External Identity has now been configured and is ready for use.

Managing Users

As MyID uses Active Directory as the user account database the base user accounts may already exist in most cases. AD users can be added one at a time or in bulk to the MyID MMC where they can be set up for various MFA technologies. They can be added from one or multiple OU's at a time as needed.

External User accounts can also be added without the need for a full AD Domain user account. These external accounts are stored within the forest root domain as LDAP "person" objects and cannot be used for Windows-based logons. A Realm must be created to contain an External User account.

External User accounts can be used together with the Windows Desktop Agent to add MFA to local Windows user accounts on both domain-joined and Workgroup based systems.

Adding a user account to the MyID MMC allows the user to make use of the Self Service Portal and, if an MFA licence is installed, they can be provisioned for Multi-Factor Authentication technologies.

Adding a New Realm

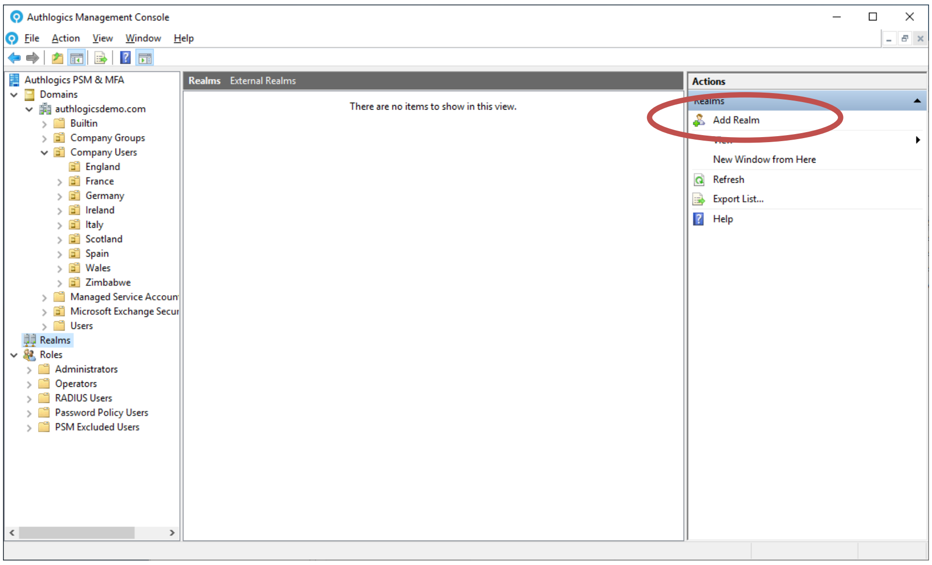
A Realm is a container to store External User accounts. Each account within a Realm must have a unique name. Realms can be nested, i.e. a Realm can be created inside another Realm for easier account management. Realms and account names can be renamed when needed.

> **Note**
> A realm name may contain letters, numbers, dot and underscore, but it cannot be the same as an existing Active Directory domain name.

The Realm name forms part of the user logon name. A user would enter their logon names as follows:

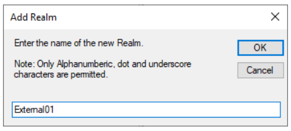
- Domain style: **realm\account**
- UPN style: **account@realm**

1. Select Realms in the Management Console.



There are no items to show in this view.

2. Click Add Realm.

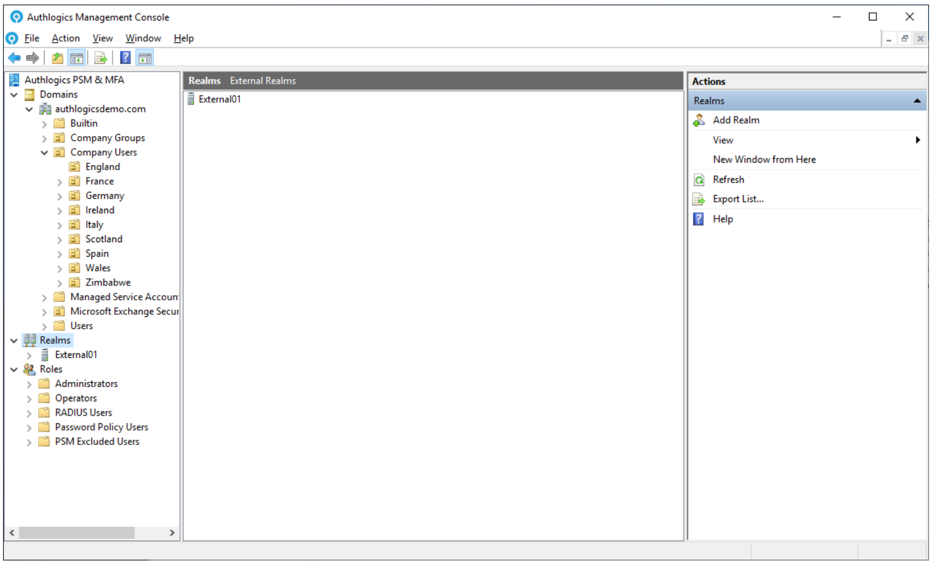


Enter the name of the new Realm.

Note: Only Alphanumberic, dot and underscore characters are permitted.

External01

3. Enter the name of the new Realm and Click *OK.*



4. Add additional Realms as needed.

User Account Types – MFA vs PSM

Different types of users can be added based on the type of licence installed. If an MFA licence is installed then a user account can be created which can be provisioned for various MFA logon technologies and devices.

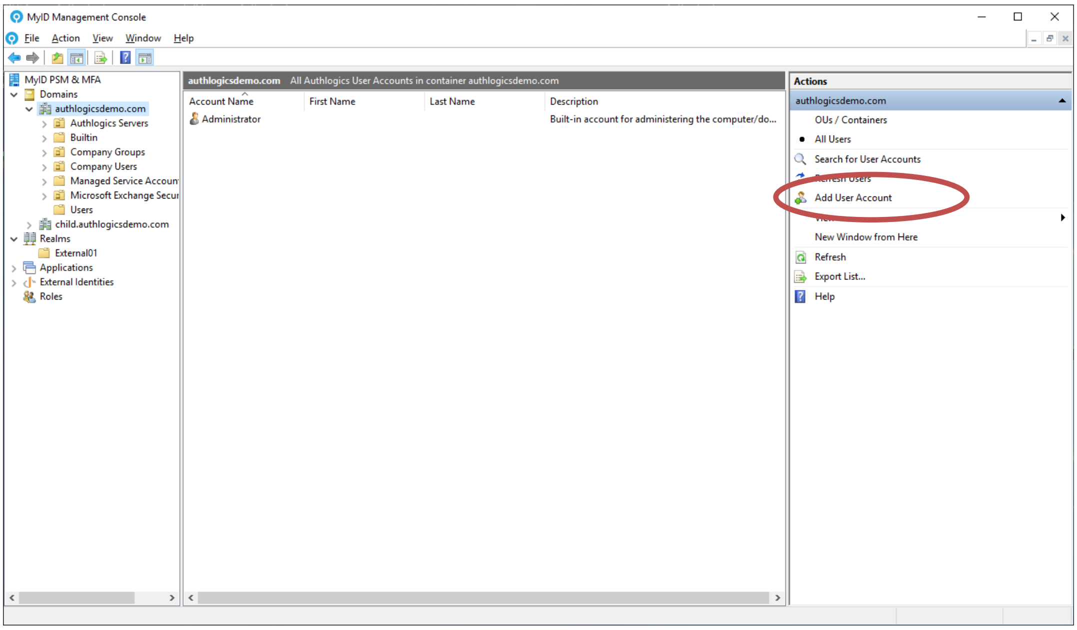
If only a PSM licence is installed then users can be created with PSM self-services features only. PSM users can access the Self Service Portal to change reset their password with One Time Codes. PSM users cannot be provisioned for use with Multi-Factor Authentication.

If an MFA licence is added to an installation that previously only had a PSM licence then existing users can immediately be provisioned for Multi-Factor Authentication.

> **Note**
> External User Accounts can only be used with MFA as PSM requires an Active Directory user account.

Adding a New MyID User Account

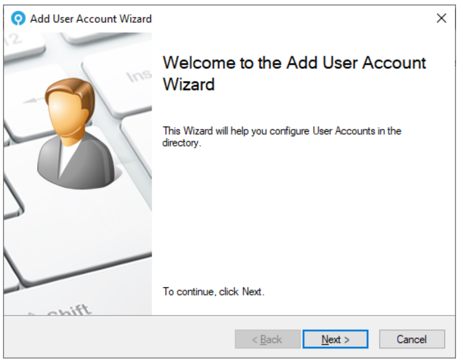
1. Expand Domains and select the appropriate domain. Expand the list of OU's as needed to see which accounts already exist.



authlogicsdemo.com All Authlogics User Accounts in container authlogicsdemo.com

Account Name	First Name	Last Name	Description
Administrator			Built-in account for administering the computer/do...

2. Click Add User Account.



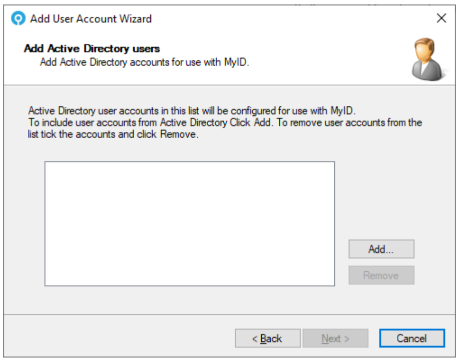
Add User Account Wizard

Welcome to the Add User Account Wizard

This Wizard will help you configure User Accounts in the directory.

To continue, click Next.

3. The Add MFA User Account Wizard starts. Click *Next.*



Add User Account Wizard

Add Active Directory users

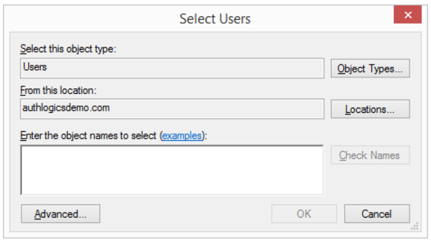
Add Active Directory accounts for use with MyID.

Active Directory user accounts in this list will be configured for use with MyID.
To include user accounts from Active Directory Click Add. To remove user accounts from the list tick the accounts and click Remove.

4. To add existing Active Directory users click *Add.*

Note

This process does not create user accounts in the Active Directory Domain, it simply adds MyID metadata to an existing account. Ensure that the domain accounts exist before adding them to the MyID MMC.



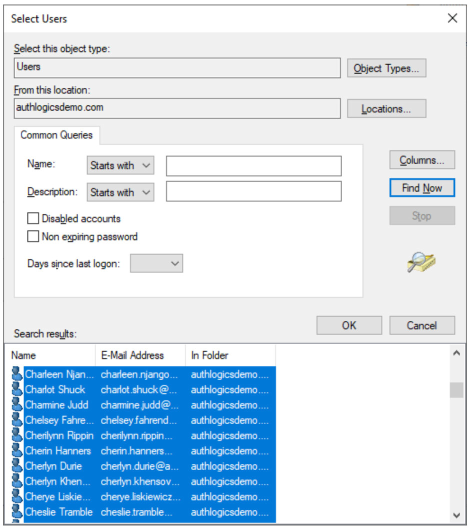
Select Users

Select this object type: Users

From this location: authlogicsdemo.com

Enter the object names to select (examples):

5. Click Advanced... then click Find Now



Select this object type: Users

From this location: authlogicsdemo.com

Name: Starts with

Description: Starts with

☐ Disabled accounts

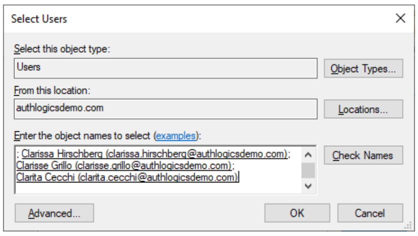
☐ Non expiring password

Days since last logon:

Search results:

Name	E-Mail Address	In Folder
Charleen Njan...	charleen.njango...	authlogicsdemo....
Charlot Shuck	charlot.shuck@...	authlogicsdemo....
Charmine Judd	charmine.judd@...	authlogicsdemo....
Chelsey Fahre...	chelsey.fahrend...	authlogicsdemo....
Cherilynn Rippin	cherilynn.rippin...	authlogicsdemo....
Cherin Hanners	cherin.hanners...	authlogicsdemo....
Cherlyn Durie	cherlyn.durie@a...	authlogicsdemo....
Cherlyn Khen...	cherlyn.khensov...	authlogicsdemo....
Cherye Liskie...	cherye.liskiewicz...	authlogicsdemo....
Cheslie Tramble	cheslie.tramble...	authlogicsdemo....

6. Select the required users from Active Directory and click *OK*.



Select this object type: Users

From this location: authlogicsdemo.com

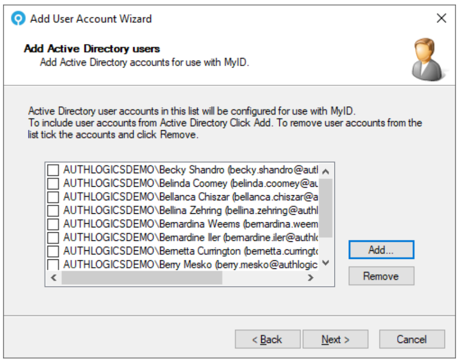
Enter the object names to select (examples):

; Clarissa Hirschberg (clarissa.hirschberg@authlogicsdemo.com);
Clarisse Grillo (clarisse.grillo@authlogicsdemo.com);
Clarita Cecchi (clarita.cecchi@authlogicsdemo.com)

7. Click *OK*.

Tip

To remove accounts from the list, check the box next to the name and click *Remove*.



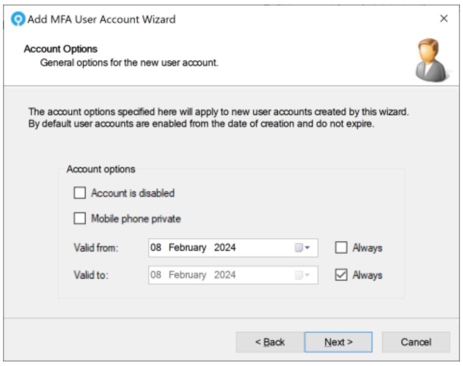
Add Active Directory users

Add Active Directory accounts for use with MyID.

Active Directory user accounts in this list will be configured for use with MyID.
To include user accounts from Active Directory Click Add. To remove user accounts from the list tick the accounts and click Remove.

☐ AUTHLOGICSDEMO\Becky Shandro (becky.shandro@autl
☐ AUTHLOGICSDEMO\Belinda Coomey (belinda.coomey@au
☐ AUTHLOGICSDEMO\Bellanca Chiszar (bellanca.chiszar@a
☐ AUTHLOGICSDEMO\Bellina Zehring (bellina.zehring@authl
☐ AUTHLOGICSDEMO\Bernardina Weems (bernardina.weem
☐ AUTHLOGICSDEMO\Bernardine Iler (bernardine.iler@authl
☐ AUTHLOGICSDEMO\Bernetta Currington (bernetta.curringt
☐ AUTHLOGICSDEMO\Berry Mesko (berry.mesko@authlogic

8. Click *Next*.



Add MFA User Account Wizard

Account Options

General options for the new user account.

The account options specified here will apply to new user accounts created by this wizard.
By default user accounts are enabled from the date of creation and do not expire.

Account options

□ Account is disabled

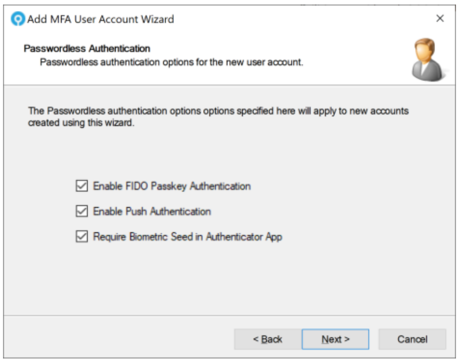
□ Mobile phone private

Valid from: 08 February 2024 □ Always

Valid to: 08 February 2024 ☑ Always

9. Account options determine the user's initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use.
   The mobile phone privacy setting can also be specified.

   Make any required changes and click *Next.*



Add MFA User Account Wizard

Passwordless Authentication

Passwordless authentication options for the new user account.

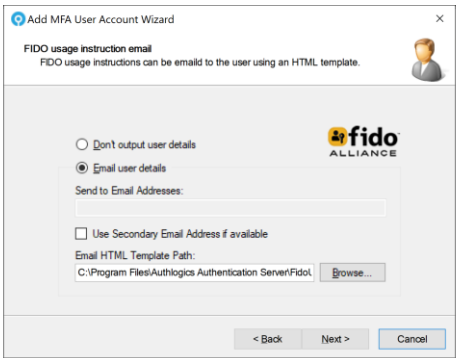
The Passwordless authentication options options specified here will apply to new accounts created using this wizard.

☑ Enable FIDO Passkey Authentication

☑ Enable Push Authentication

☑ Require Biometric Seed in Authenticator App

10. Choose if the users should be enabled for FIDO and/or Mobile Push authentication or not and click *Next.*



Add MFA User Account Wizard

FIDO usage instruction email

FIDO usage instructions can be emaild to the user using an HTML template.

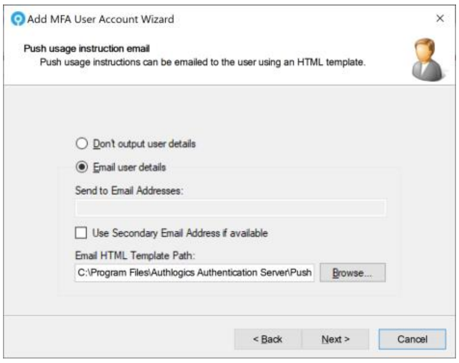
○ Don't output user details

● Email user details

Send to Email Addresses:

□ Use Secondary Email Address if available

Email HTML Template Path: C:\Program Files\Authlogics Authentication Server\Fido\

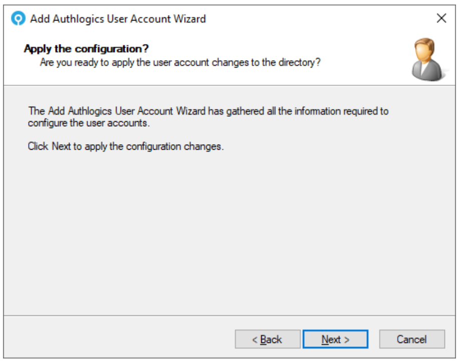


Push usage instruction email
Push usage instructions can be emailed to the user using an HTML template.

○ Don't output user details
● Email user details
Send to Email Addresses:
□ Use Secondary Email Address if available
Email HTML Template Path: C:\Program Files\Authlogics Authentication Server\Push

11. Choose how and if the users will receive a welcome email with instructions on how to setup their device for FIDO and Mobile Push based on your selection above. If a single user is selected, you can specify the email address to deliver the email to. When adding multiple users, the user's email address will be retrieved from AD or the alternate email address field and sent to them automatically.

    The appropriate FIDO and PUSH HTML template files can be selected to use for the email.
    Click *Next*.

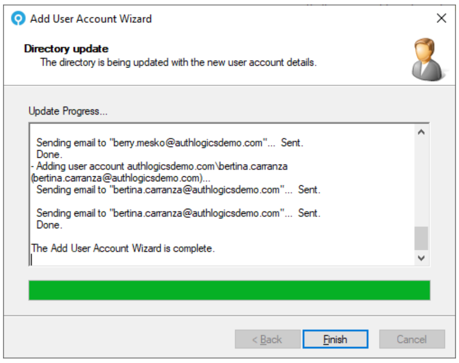


Apply the configuration?
Are you ready to apply the user account changes to the directory?

The Add Authlogics User Account Wizard has gathered all the information required to configure the user accounts.

Click Next to apply the configuration changes.

12. Click *Next*.

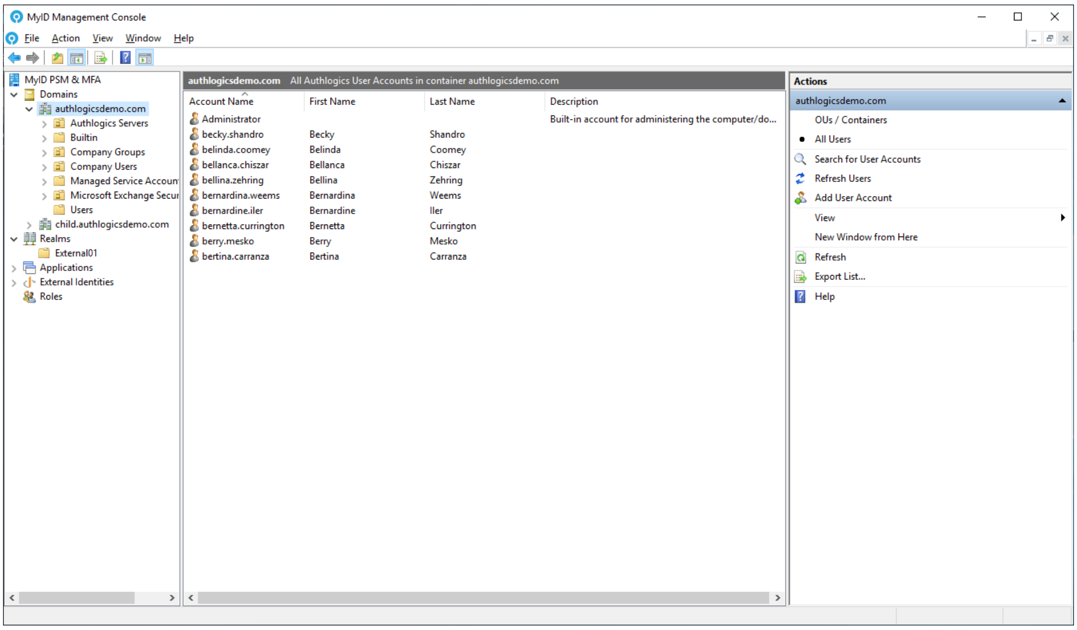


Directory update
The directory is being updated with the new user account details.

Update Progress...

```
  Sending email to "berry.mesko@authlogicsdemo.com"...  Sent.
  Done.
- Adding user account authlogicsdemo.com\bertina.carranza
(bertina.carranza@authlogicsdemo.com)...
  Sending email to "bertina.carranza@authlogicsdemo.com"...  Sent.

  Sending email to "bertina.carranza@authlogicsdemo.com"...  Sent.
  Done.

The Add User Account Wizard is complete.
```

13. The New User Account(s) has/have been created.
    Click *Finish*.



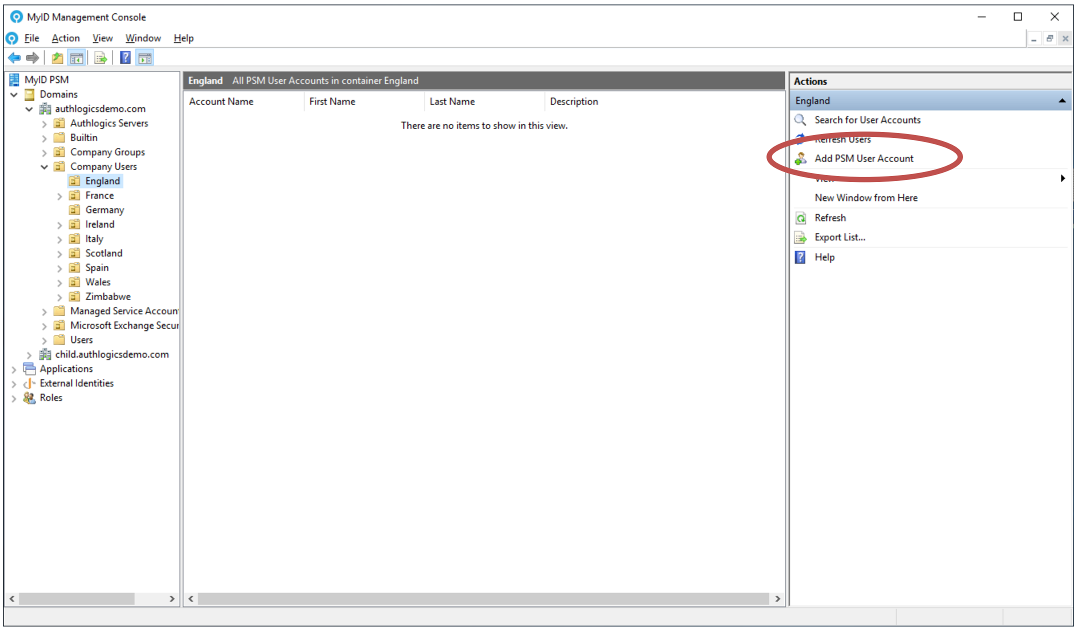
authlogicsdemo.com All Authlogics User Accounts in container authlogicsdemo.com

Account Name	First Name	Last Name	Description
Administrator			Built-in account for administering the computer/do...
becky.shandro	Becky	Shandro	
belinda.coomey	Belinda	Coomey	
bellanca.chiszar	Bellanca	Chiszar	
bellina.zehring	Bellina	Zehring	
bernardina.weems	Bernardina	Weems	
bernardine.iler	Bernardine	Iler	
bernetta.currington	Bernetta	Currington	
berry.mesko	Berry	Mesko	
bertina.carranza	Bertina	Carranza	

Adding a New MyID PSM User Account

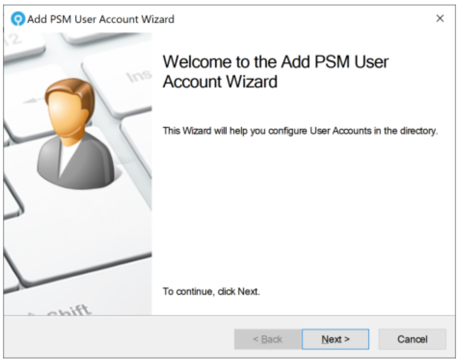
PSM user account can be manually added if required, however PSM users will automatically apprear when a user changes their password or logs onto the Self Service Portal.

1. Expand Domains and select the appropriate domain. Expand the list of OU's as needed to see which accounts already exist.



There are no items to show in this view.

2. Click Add PSM User Account.

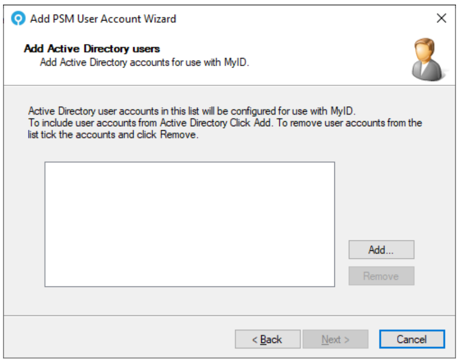


Welcome to the Add PSM User Account Wizard

This Wizard will help you configure User Accounts in the directory.

To continue, click Next.

3. The Add PSM User Account Wizard starts. Click *Next.*



Add PSM User Account Wizard

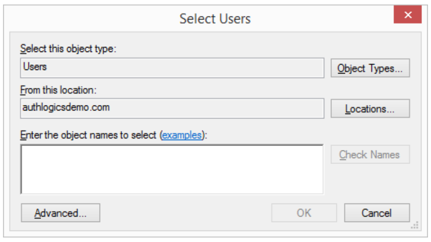
Add Active Directory users

Add Active Directory accounts for use with MyID.

Active Directory user accounts in this list will be configured for use with MyID. To include user accounts from Active Directory Click Add. To remove user accounts from the list tick the accounts and click Remove.

4. To add existing Active Directory users click *Add.*

> **Note**
>
> This process does not create user accounts in the Active Directory Domain, it simply adds MyID metadata to an existing account. Ensure that the domain accounts exist before adding them to the MyID MMC.



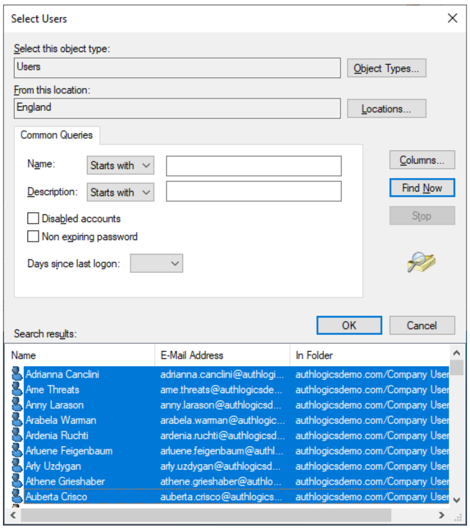
Select Users

Select this object type: Users

From this location: authlogicsdemo.com

Enter the object names to select (examples):

5. Click Advanced… then click Find Now



Select Users

Select this object type: Users

From this location: England

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

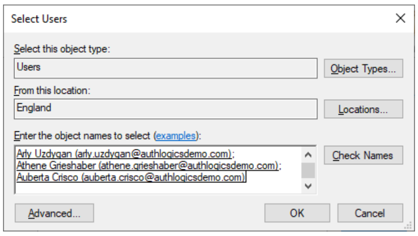
□ Non expiring password

Days since last logon:

Search results:

Name	E-Mail Address	In Folder
Adrianna Canclini	adrianna.canclini@authlogi...	authlogicsdemo.com/Company User
Ame Threats	ame.threats@authlogicsde...	authlogicsdemo.com/Company User
Anny Larason	anny.larason@authlogicsd...	authlogicsdemo.com/Company User
Arabela Warman	arabela.warman@authlogic...	authlogicsdemo.com/Company User
Ardenia Ruchti	ardenia.ruchti@authlogicsd...	authlogicsdemo.com/Company User
Arluene Feigenbaum	arluene.feigenbaum@authl...	authlogicsdemo.com/Company User
Arly Uzdygan	arly.uzdygan@authlogicsd...	authlogicsdemo.com/Company User
Athene Grieshaber	athene.grieshaber@authlo...	authlogicsdemo.com/Company User
Auberta Crisco	auberta.crisco@authlogics...	authlogicsdemo.com/Company User

6. Select the required users from Active Directory and click *OK.*



Select Users

Select this object type: Users

From this location: England

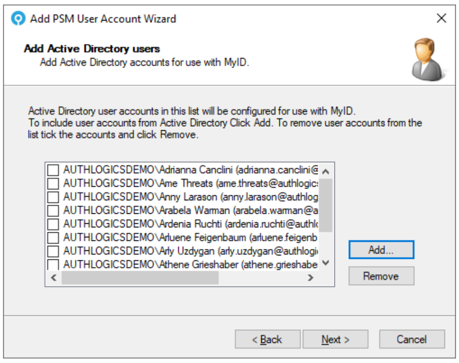
Enter the object names to select (examples):

Arly Uzdygan (arly.uzdygan@authlogicsdemo.com); Athene Grieshaber (athene.grieshaber@authlogicsdemo.com); Auberta Crisco (auberta.crisco@authlogicsdemo.com)

7. Click *OK*.

Note

To remove accounts from the list, check the box next to the name and click *Remove*.



Add PSM User Account Wizard

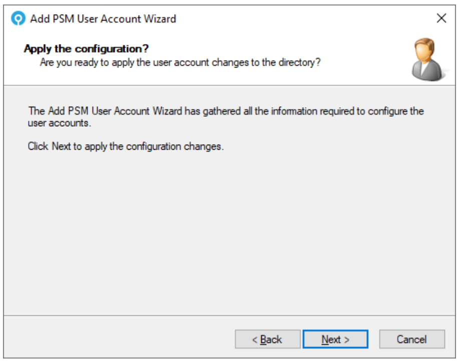
Add Active Directory users

Add Active Directory accounts for use with MyID.

Active Directory user accounts in this list will be configured for use with MyID.
To include user accounts from Active Directory Click Add. To remove user accounts from the list tick the accounts and click Remove.

- □ AUTHLOGICSDEMO\Adrianna Canclini (adrianna.canclini@
- □ AUTHLOGICSDEMO\Ame Threats (ame.threats@authlogic
- □ AUTHLOGICSDEMO\Anny Larason (anny.larason@authlog
- □ AUTHLOGICSDEMO\Arabela Warman (arabela.warman@a
- □ AUTHLOGICSDEMO\Ardenia Ruchti (ardenia.ruchti@authl
- □ AUTHLOGICSDEMO\Arluene Feigenbaum (arluene.feigenb
- □ AUTHLOGICSDEMO\Arly Uzdygan (arly.uzdygan@authlogi
- □ AUTHLOGICSDEMO\Athene Grieshaber (athene.grieshabe

8. Click *Next*.



Add PSM User Account Wizard

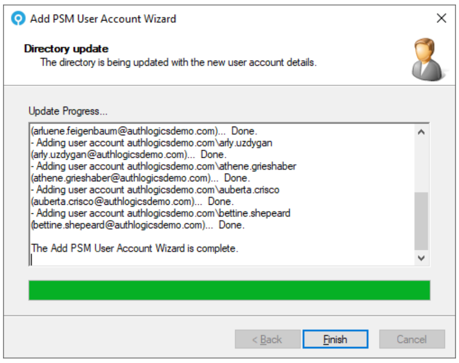
Apply the configuration?

Are you ready to apply the user account changes to the directory?

The Add PSM User Account Wizard has gathered all the information required to configure the user accounts.

Click Next to apply the configuration changes.

9. Click *Next*.



Add PSM User Account Wizard

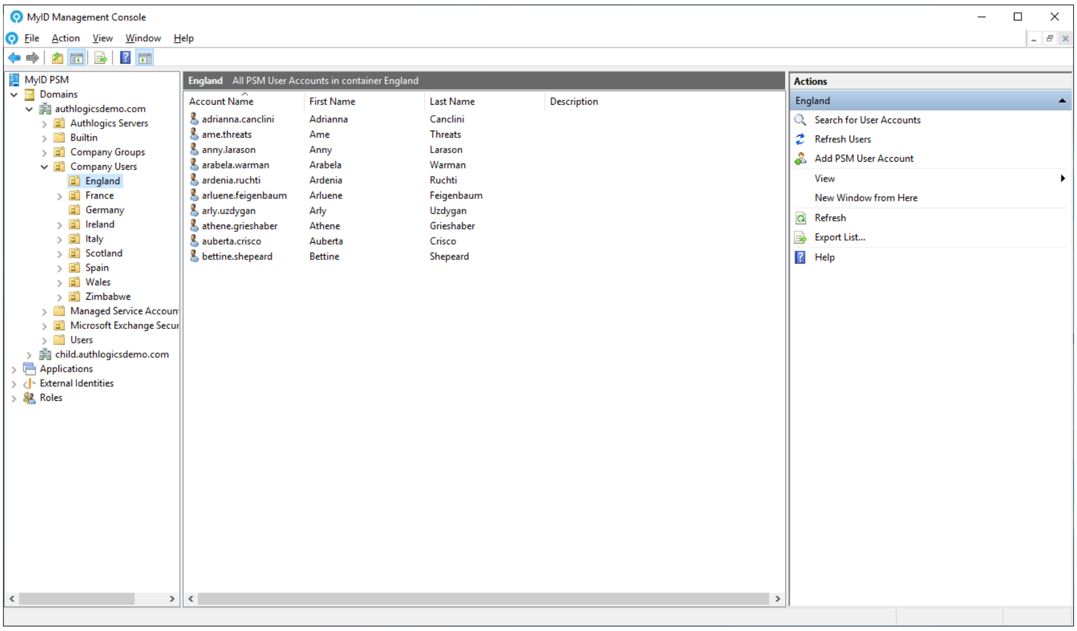
Directory update

The directory is being updated with the new user account details.

Update Progress...

```
(arluene.feigenbaum@authlogicsdemo.com)...  Done.
- Adding user account authlogicsdemo.com\arly.uzdygan
(arly.uzdygan@authlogicsdemo.com)...  Done.
- Adding user account authlogicsdemo.com\athene.grieshaber
(athene.grieshaber@authlogicsdemo.com)...  Done.
- Adding user account authlogicsdemo.com\auberta.crisco
(auberta.crisco@authlogicsdemo.com)...  Done.
- Adding user account authlogicsdemo.com\bettine.shepeard
(bettine.shepeard@authlogicsdemo.com)...  Done.

The Add PSM User Account Wizard is complete.
```

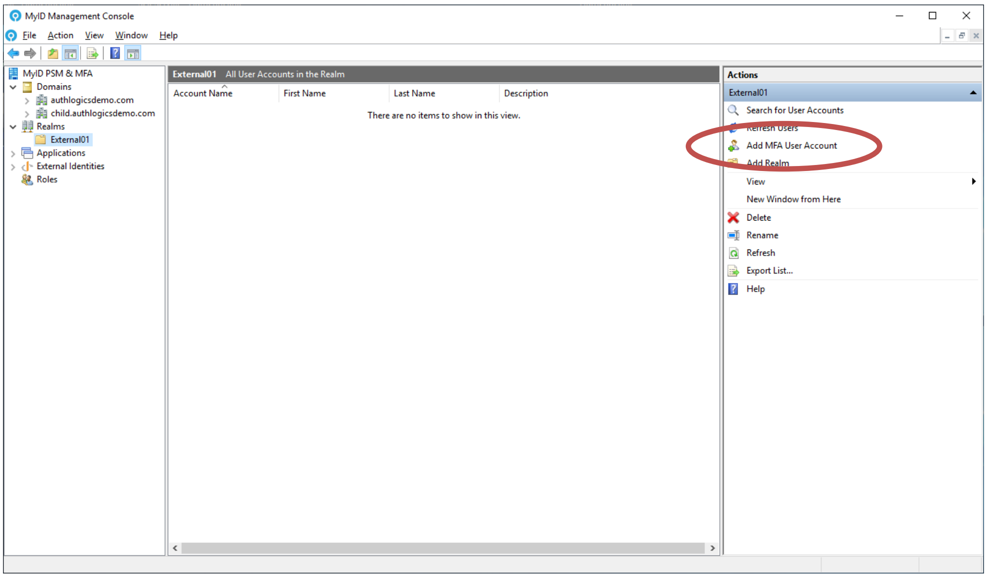
10. The New User Account(s) has/have been created.
    Click *Finish*.



Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

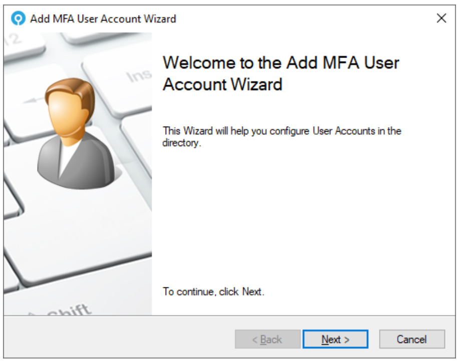
Adding a New External MFA User Account

1. Expand Reams and select the appropriate Realm to add the account.



There are no items to show in this view.

2. Click Add External MFA User Account.

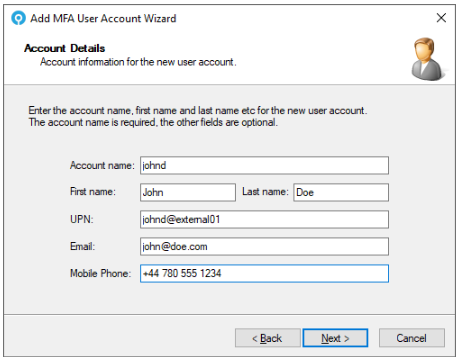


Welcome to the Add MFA User Account Wizard

This Wizard will help you configure User Accounts in the directory.

To continue, click Next.

3. The Add External MFA User Account Wizard starts. Click *Next.*

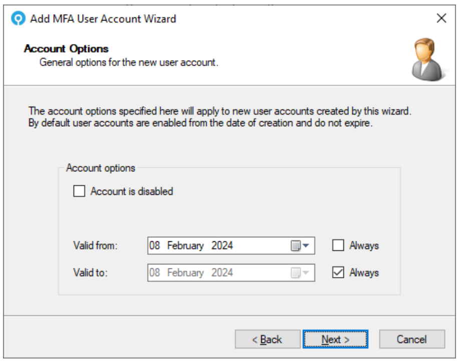


Account Details
Account information for the new user account.

Enter the account name, first name and last name etc for the new user account.
The account name is required, the other fields are optional.

Account name: johnd
First name: John Last name: Doe
UPN: johnd@external01
Email: john@doe.com
Mobile Phone: +44 780 555 1234

4. Enter the details for the new user account. Only the *Account name* is required, all other fields are optional. The *UPN* will be automatically generated based on the *Realm* and *Account* name however it may be manually edited as needed.
   Click *Next*

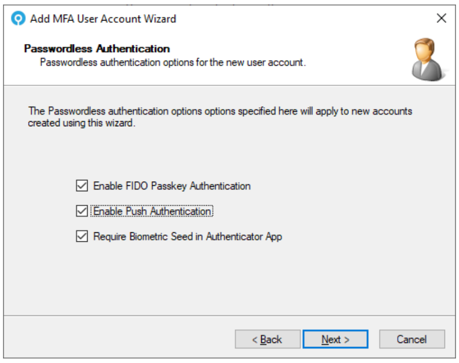


Account Options
General options for the new user account.

The account options specified here will apply to new user accounts created by this wizard.
By default user accounts are enabled from the date of creation and do not expire.

Account options
☐ Account is disabled
Valid from: 08 February 2024 ☐ Always
Valid to: 08 February 2024 ☑ Always

5. Account options determine the user’s initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use.
   Make any required changes and click *Next.*



Add MFA User Account Wizard

Passwordless Authentication

Passwordless authentication options for the new user account.

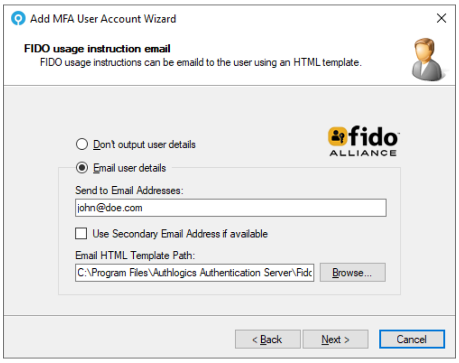
The Passwordless authentication options options specified here will apply to new accounts created using this wizard.

☑ Enable FIDO Passkey Authentication

☑ Enable Push Authentication

☑ Require Biometric Seed in Authenticator App

6. Choose if the users should be enabled for FIDO, Mobile Push authentication or not. At this stage, you can force Mobile App users to provide Biometric information as part of the authentication process. Click *Next.*



Add MFA User Account Wizard

FIDO usage instruction email

FIDO usage instructions can be emaild to the user using an HTML template.

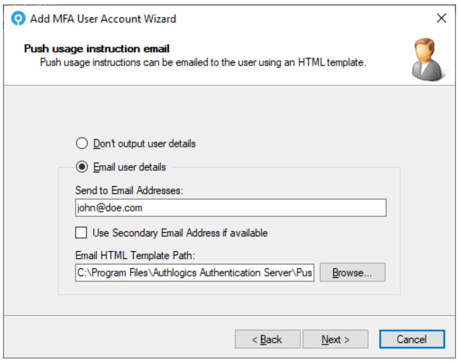
○ Don't output user details

● Email user details

Send to Email Addresses: john@doe.com

□ Use Secondary Email Address if available

Email HTML Template Path: C:\Program Files\Authlogics Authentication Server\Fidc



Add MFA User Account Wizard

Push usage instruction email

Push usage instructions can be emailed to the user using an HTML template.

○ Don't output user details

● Email user details

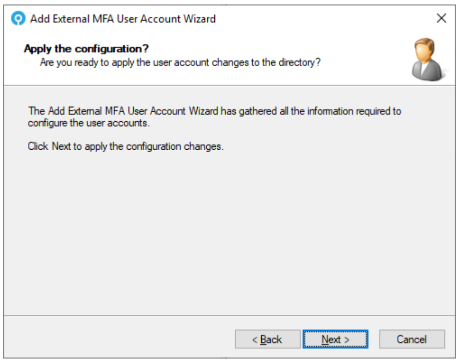
Send to Email Addresses: john@doe.com

□ Use Secondary Email Address if available

Email HTML Template Path: C:\Program Files\Authlogics Authentication Server\Pus

7. Choose how and if the users will receive a welcome email with instructions on how to setup their device for FIDO and Mobile Push based on your selection above. If a single user is selected, you can specify the email address to deliver the email to. When adding multiple users, the user's email address will be retrieved from AD or the alternate email address field and sent to them automatically.

   The appropriate FIDO and PUSH HTML template files can be selected to use for the email.



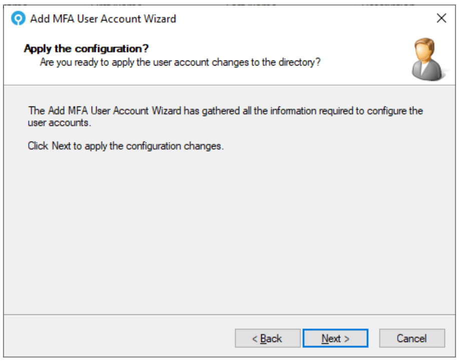
Add External MFA User Account Wizard

Apply the configuration?
Are you ready to apply the user account changes to the directory?

The Add External MFA User Account Wizard has gathered all the information required to configure the user accounts.

Click Next to apply the configuration changes.

8. Click *Next.*



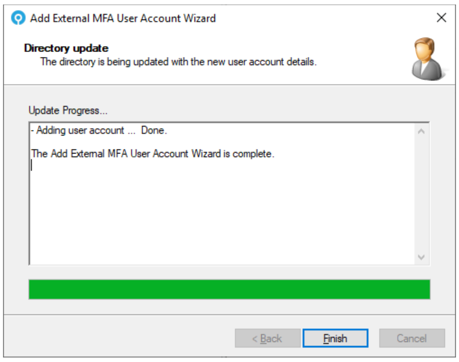
Add MFA User Account Wizard

Apply the configuration?
Are you ready to apply the user account changes to the directory?

The Add MFA User Account Wizard has gathered all the information required to configure the user accounts.

Click Next to apply the configuration changes.

9. Click *Next.*



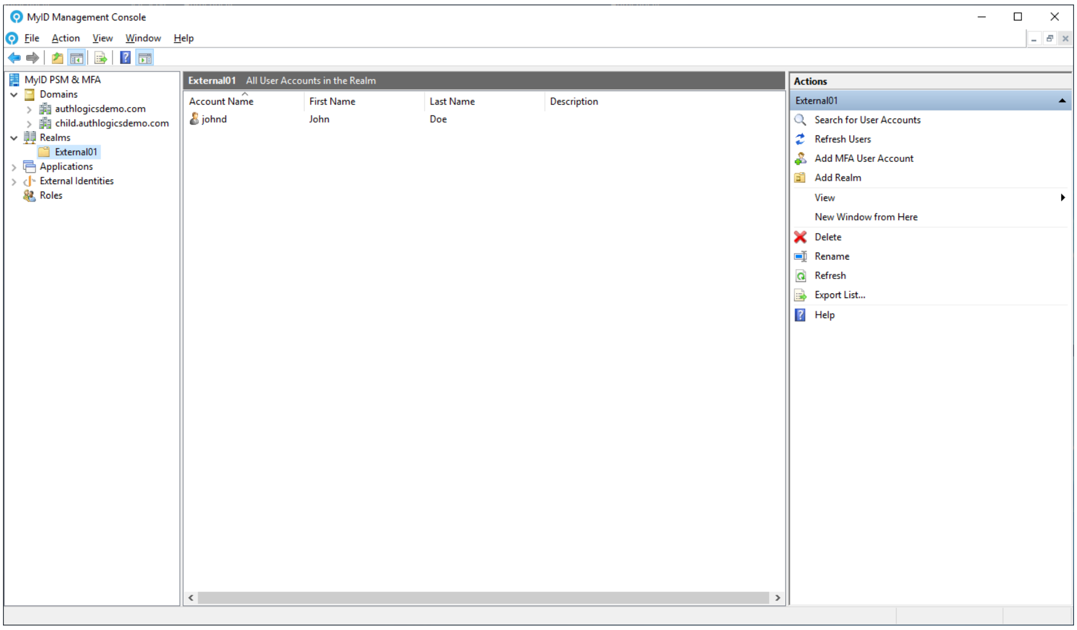
Add External MFA User Account Wizard

Directory update
The directory is being updated with the new user account details.

Update Progress...

```
- Adding user account ... Done.

The Add External MFA User Account Wizard is complete.
```

10. The New User Account has been created.
    Click *Finish.*

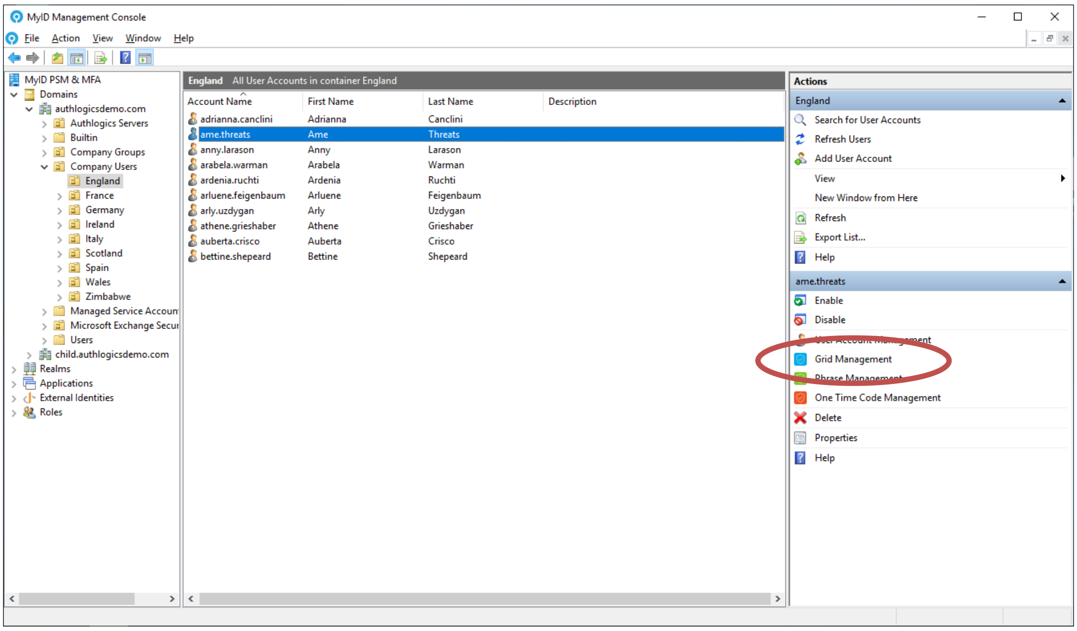


Account Name	First Name	Last Name	Description
johnd	John	Doe	

Setting up a user for Grid Pattern Authentication

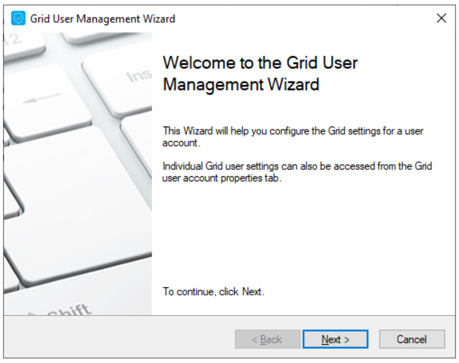
Once a MyID user account has been created you can configure it for use with Grid Pattern Authentication.

1. Expand Domains and select the appropriate OU or expand Realms and select the appropriate Realm. Select the user account (or accounts) to manage Grid settings.



Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

2. Click *Grid Management* from the menu on the right or from the right-click menu to start the Grid User Management Wizard.



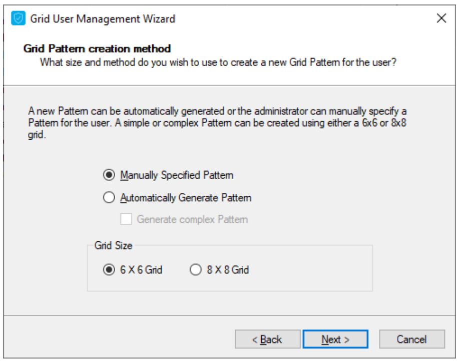
Welcome to the Grid User Management Wizard

This Wizard will help you configure the Grid settings for a user account.

Individual Grid user settings can also be accessed from the Grid user account properties tab.

To continue, click Next.

3. Click *Next.*



Grid User Management Wizard

Grid Pattern creation method

What size and method do you wish to use to create a new Grid Pattern for the user?

A new Pattern can be automatically generated or the administrator can manually specify a Pattern for the user. A simple or complex Pattern can be created using either a 6x6 or 8x8 grid.

● Manually Specified Pattern

○ Automatically Generate Pattern

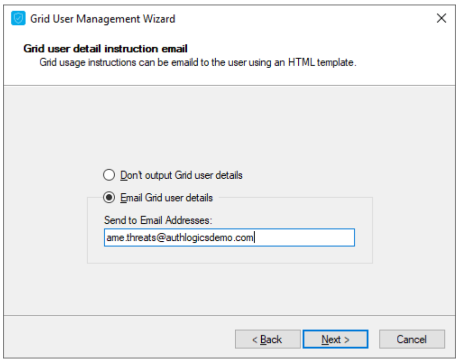
□ Generate complex Pattern

Grid Size

● 6 X 6 Grid ○ 8 X 8 Grid

4. Users can have random Patterns generated automatically or the administrator can choose to manually configure the user's information. By default, "simple" patterns will be generated for the user, tick the *Generate complex Pattern* box for a more secure pattern. If multiple accounts were selected before starting the wizard then only the automatic option is available.

   Choose the Pattern provisioning method and grid size for the selected users.
   Click *Next.*



Grid User Management Wizard

Grid user detail instruction email

Grid usage instructions can be emaild to the user using an HTML template.

○ Don't output Grid user details

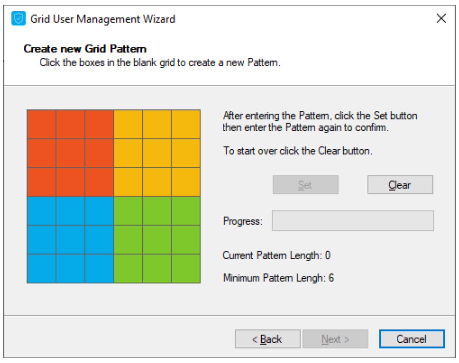
● Email Grid user details

Send to Email Addresses: ame.threats@authlogicsdemo.com

5. Select the method used to distribute the Pattern, as well as Grid usage instructions to the user. Auto-generated information can be emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details; this option is not available for auto-generated details. You can send the email to multiple addresses by entering multiple email addresses separated by a semi-colon ";".
   Click *Next.*

Note

For instructions on manually specifying a pattern proceed to step 6, otherwise, skip to step 9.



Grid User Management Wizard

Create new Grid Pattern

Click the boxes in the blank grid to create a new Pattern.

After entering the Pattern, click the Set button then enter the Pattern again to confirm.

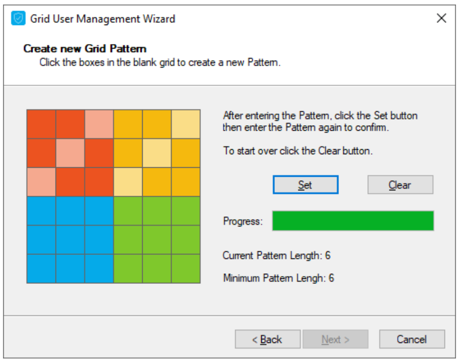
To start over click the Clear button.

Progress:

Current Pattern Length: 0

Minimum Pattern Lengh: 6

6. Enter the required pattern and click *Set*.



Grid User Management Wizard

Create new Grid Pattern

Click the boxes in the blank grid to create a new Pattern.

After entering the Pattern, click the Set button then enter the Pattern again to confirm.

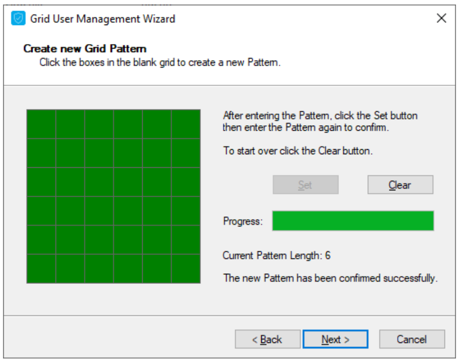
To start over click the Clear button.

Progress:

Current Pattern Length: 6

Minimum Pattern Lengh: 6

7. Confirm the Pattern entered previously.



Grid User Management Wizard

Create new Grid Pattern

Click the boxes in the blank grid to create a new Pattern.

After entering the Pattern, click the Set button then enter the Pattern again to confirm.

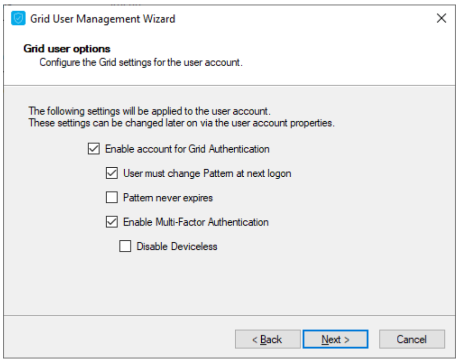
To start over click the Clear button.

Progress:

Current Pattern Length: 6

The new Pattern has been confirmed successfully.

8. If the patterns match, the displayed grid will turn green. A red grid denotes a pattern mismatch. Click *Clear* to re-enter the pattern or Click *Next* to continue.



Grid User Management Wizard

Grid user options

Configure the Grid settings for the user account.

The following settings will be applied to the user account.
These settings can be changed later on via the user account properties.

☑ Enable account for Grid Authentication

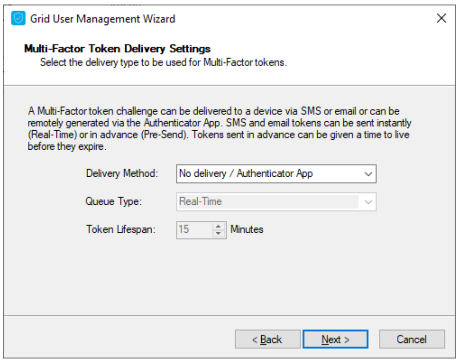
☑ User must change Pattern at next logon

☐ Pattern never expires

☑ Enable Multi-Factor Authentication

☐ Disable Deviceless

9. Configure Grid pattern user options.
   A user’s Pattern can be set to never expire or set so that the next time the user logins with this account, that user will be forced to change the Pattern.
   In MFA deployments, you can enable and enforce the user account to use a Multi-Factor device. An MFA device will need to be registered with the user account or the challenge delivered via email or SMS/TEXT otherwise authentication will fail.
   Click Next.



Grid User Management Wizard

Multi-Factor Token Delivery Settings
Select the delivery type to be used for Multi-Factor tokens.

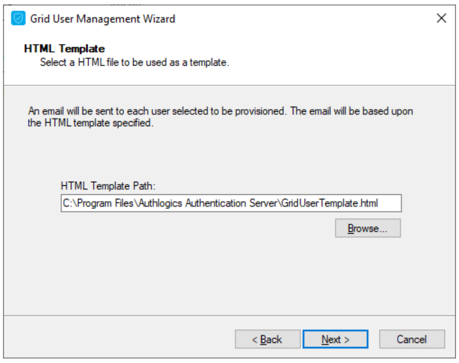
A Multi-Factor token challenge can be delivered to a device via SMS or email or can be remotely generated via the Authenticator App. SMS and email tokens can be sent instantly (Real-Time) or in advance (Pre-Send). Tokens sent in advance can be given a time to live before they expire.

Delivery Method: No delivery / Authenticator App

Queue Type: Real-Time

Token Lifespan: 15 Minutes

10. Select the delivery method for Multi-Factor tokens. When selecting a method, ensure that the user has either an Email address or Mobile telephone number that tokens will be delivered to.
    Queue Type determines whether tokens will be pre-sent or generated in Real-Time. When Queue Type is set to Pre-Send, an administrator must then specify the Token Lifespan for these token types.
    The *Enable remote seed for soft tokens* requires that the remote seed value generated by the Authentication Server be configured on the MFA device registered with the user account otherwise authentication will fail. This value will automatically be installed via the QR code device enrolment process.
    Click *Next.*



Grid User Management Wizard

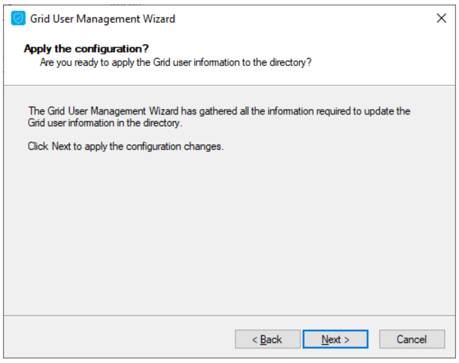
HTML Template
Select a HTML file to be used as a template.

An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified.

HTML Template Path:
C:\Program Files\Authlogics Authentication Server\GridUserTemplate.html

11. Specify an HTML Template Path to the automated notification letter/email each user will receive. This HTML file can be modified and customised for your organisation. Each letter/email will be customised for the user to contain their unique information by substituting HTML comment values in the template.

To locate a custom template click *Browse...* otherwise, click *Next.*



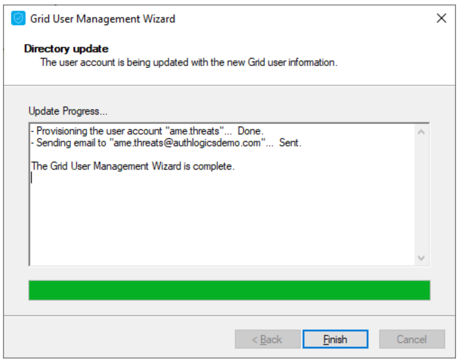
Apply the configuration?

Are you ready to apply the Grid user information to the directory?

The Grid User Management Wizard has gathered all the information required to update the Grid user information in the directory.

Click Next to apply the configuration changes.

12. Click *Next*.



Directory update

The user account is being updated with the new Grid user information.

Update Progress...

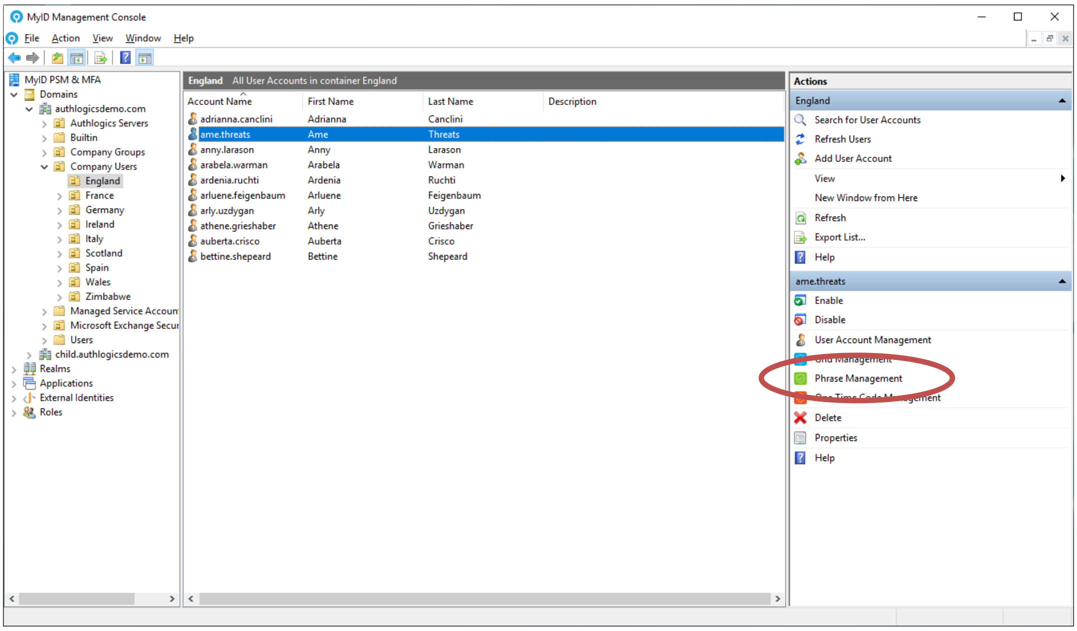
```
- Provisioning the user account "ame.threats"... Done.
- Sending email to "ame.threats@authlogicsdemo.com"... Sent.

The Grid User Management Wizard is complete.
```

13. Click *Finish*.

Setting up a user for Phrase authentication

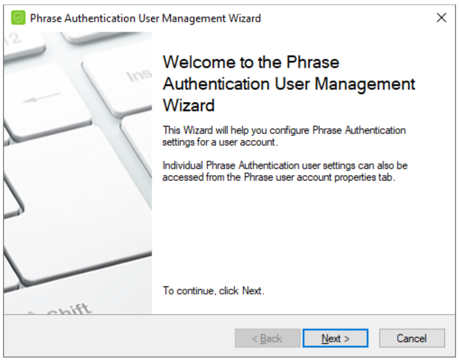
Once an MyID user account has been created you can configure it for use with Phrase authentication.

1. Expand Domains and select the appropriate OU or expand Realms and select the appropriate Realm. Select the user account (or accounts) to manage Phrase settings.



Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

2. Click *Phrase Management* from the menu on the right or from the right-click menu to start the Phrase Authentication User Management Wizard.



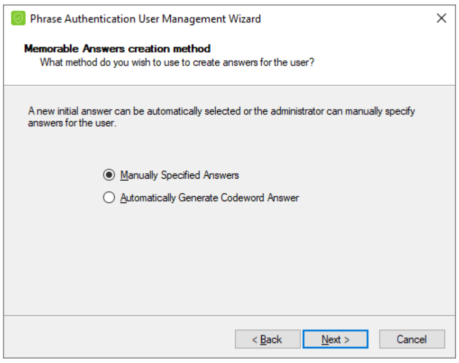
Welcome to the Phrase Authentication User Management Wizard

This Wizard will help you configure Phrase Authentication settings for a user account.

Individual Phrase Authentication user settings can also be accessed from the Phrase user account properties tab.

To continue, click Next.

3. Click *Next*.


Phrase Authentication User Management Wizard

Memorable Answers creation method

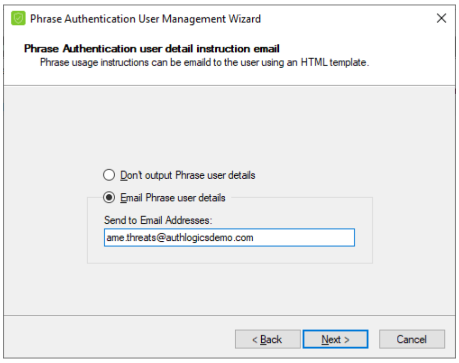
What method do you wish to use to create answers for the user?

A new initial answer can be automatically selected or the administrator can manually specify answers for the user.

● Manually Specified Answers

○ Automatically Generate Codeword Answer

4. Users can have a randomly generated Codeword answer or the administrator can choose to manually configure the user's information. If multiple accounts were selected before starting the wizard then only the automatic option is available. Choose the provisioning method.
   Click *Next.*


Phrase Authentication User Management Wizard

Phrase Authentication user detail instruction email

Phrase usage instructions can be emaild to the user using an HTML template.

○ Don't output Phrase user details

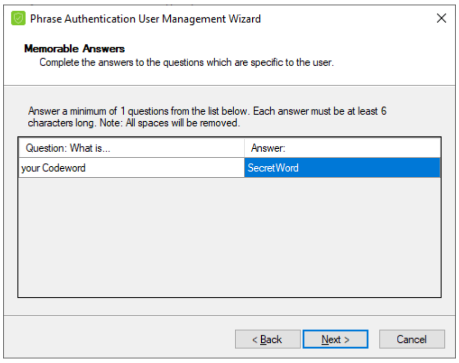
● Email Phrase user details

Send to Email Addresses: ame.threats@authlogicsdemo.com

5. Select the method used to distribute the Phrase settings as well as the Phrase usage instructions to the user. Auto-generated information can be emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details, this option is not available for auto-generated details.
   Click *Next.*

Note

For instructions on manually specifying a pattern proceed to step 6, otherwise, skip to step 7.


Phrase Authentication User Management Wizard

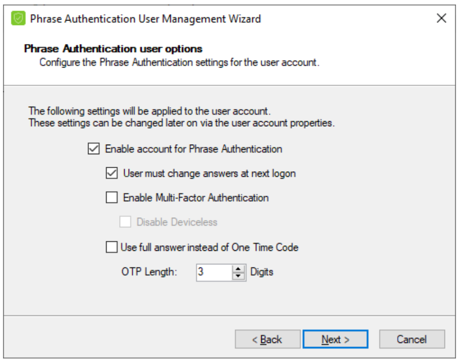
Memorable Answers

Complete the answers to the questions which are specific to the user.

Answer a minimum of 1 questions from the list below. Each answer must be at least 6 characters long. Note: All spaces will be removed.

Question: What is...	Answer:
your Codeword	SecretWord

6. Enter answers for the questions ensuring that each answer is at least the minimum number of prescribed characters and that enough questions have been answered. When all Phrase conditions have been met, the *Next* button will be available.
   Click *Next.*

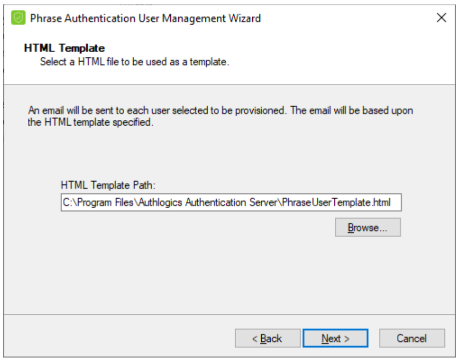

Phrase Authentication User Management Wizard

Phrase Authentication user options
Configure the Phrase Authentication settings for the user account.

The following settings will be applied to the user account.
These settings can be changed later on via the user account properties.

☑ Enable account for Phrase Authentication
☑ User must change answers at next logon
☐ Enable Multi-Factor Authentication
☐ Disable Deviceless
☐ Use full answer instead of One Time Code
OTP Length: 3 Digits

7. Configure Phrase Authentication user options.
   An account can be set so that the next time the user logins with this account, that user will be forced to change the answers at the next logon.
   In MFA deployments, you can enable and enforce the user account to use a Multi-Factor device by selecting the *Disable Deviceless* option.
   An account can be configured to require the full answer to be entered instead of random letters from the answer. Note: This is not meant to be used as a true password-based system and is disabled by default.
   Set the *OTC Length* for the number of characters a user will need to provide from the predetermined answer.
   Click *Next.*

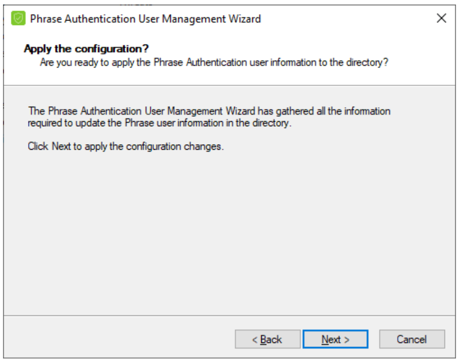

Phrase Authentication User Management Wizard

HTML Template
Select a HTML file to be used as a template.

An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified.

HTML Template Path:
C:\Program Files\Authlogics Authentication Server\PhraseUserTemplate.html

8. Specify an HTML Template Path to the automated notification letter/email each user will receive. This HTML file can be modified and customised for your organisation. Each letter/email will be customised for the user to contain their unique information by substituting HTML comment values in the template.



Phrase Authentication User Management Wizard

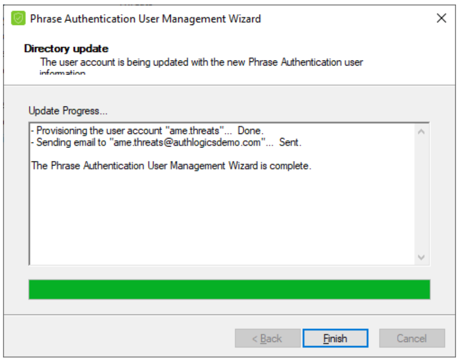
Apply the configuration?

Are you ready to apply the Phrase Authentication user information to the directory?

The Phrase Authentication User Management Wizard has gathered all the information required to update the Phrase user information in the directory.

Click Next to apply the configuration changes.

9. Click *Next* to apply the configuration changes.



Phrase Authentication User Management Wizard

Directory update

The user account is being updated with the new Phrase Authentication user information

Update Progress...

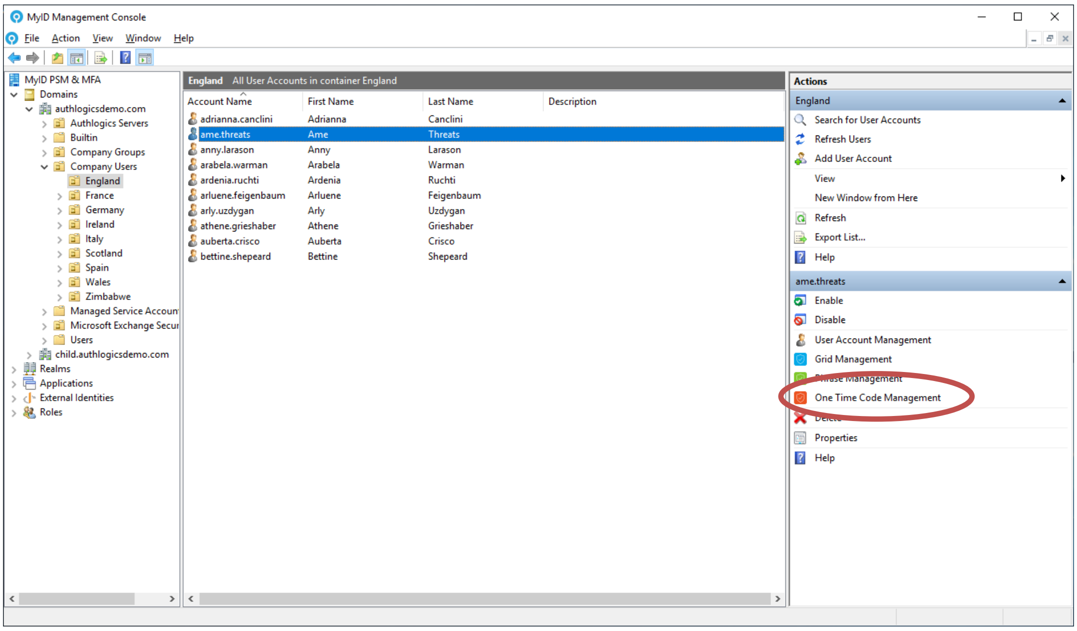
```
- Provisioning the user account "ame.threats"...  Done.
- Sending email to "ame.threats@authlogicsdemo.com"...  Sent.

The Phrase Authentication User Management Wizard is complete.
```

10. Click *Finish*.

Setting up a user for One Time Code

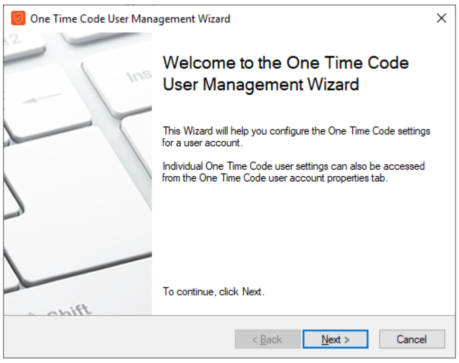
Once an MyID user account has been created you can configure it for use with One Time Code.

1. Expand Domains and select the appropriate OU or expand Realms and select the appropriate Realm. Select the user account (or accounts) to manage One Time Code settings.



Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

2. Click *One Time Code Management* from the menu on the right or from the right-click menu to start the One Time Code Management Wizard.



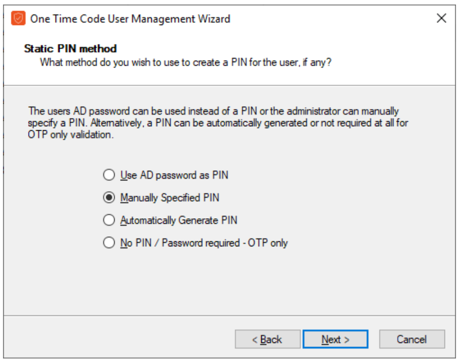
Welcome to the One Time Code User Management Wizard

This Wizard will help you configure the One Time Code settings for a user account.

Individual One Time Code user settings can also be accessed from the One Time Code user account properties tab.

To continue, click Next.

3. Click *Next*.



One Time Code User Management Wizard

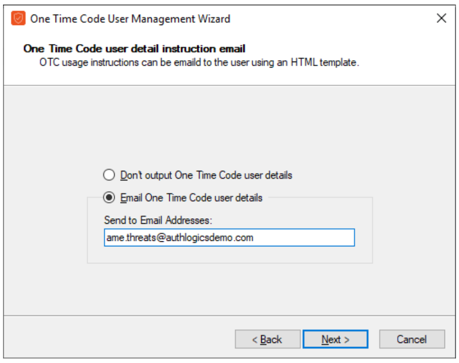
Static PIN method

What method do you wish to use to create a PIN for the user, if any?

The users AD password can be used instead of a PIN or the administrator can manually specify a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation.

○ Use AD password as PIN
● Manually Specified PIN
○ Automatically Generate PIN
○ No PIN / Password required - OTP only

4. The user’s AD password can be used instead of a PIN, or the administrator can manually specify a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation. Finally, if enabled through Global settings, No additional PIN can be specified. If multiple accounts were selected before starting the wizard then the *Manually Specified* option is not available.
   Click Next.



One Time Code User Management Wizard

One Time Code user detail instruction email

OTC usage instructions can be emaild to the user using an HTML template.

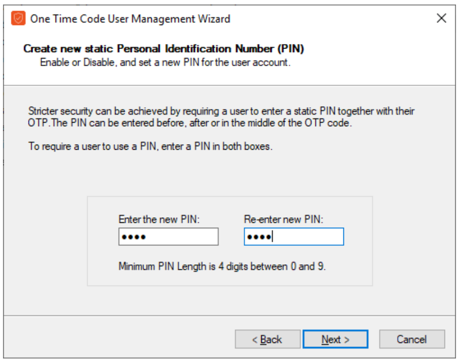
○ Don't output One Time Code user details
● Email One Time Code user details

Send to Email Addresses: ame.threats@authlogicsdemo.com

5. Select the method used to distribute the One Time Code settings as well as One Time Code usage instructions to the user. Auto-generated information can be either printed or emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details, this option is not available for auto-generated details.
   Click *Next*.

Note

For instructions on manually specifying a PIN proceed to step 6, otherwise, skip to step 7.



One Time Code User Management Wizard

Create new static Personal Identification Number (PIN)
Enable or Disable, and set a new PIN for the user account.

Stricter security can be achieved by requiring a user to enter a static PIN together with their OTP. The PIN can be entered before, after or in the middle of the OTP code.

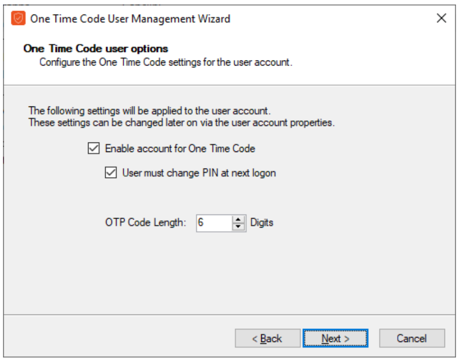
To require a user to use a PIN, enter a PIN in both boxes.

Enter the new PIN: ••••

Re-enter new PIN: ••••

Minimum PIN Length is 4 digits between 0 and 9.

6. Enter the user’s PIN and confirm the PIN. Click *Next*.



One Time Code User Management Wizard

One Time Code user options
Configure the One Time Code settings for the user account.

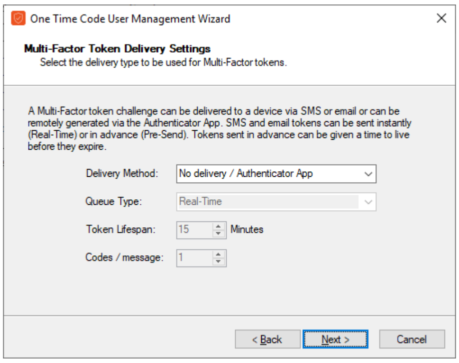
The following settings will be applied to the user account.
These settings can be changed later on via the user account properties.

☑ Enable account for One Time Code

☑ User must change PIN at next logon

OTP Code Length: 6 Digits

7. Configure One Time Code user options.
   An account can be set so that the next time the user logins with this account, that user will be forced to change the PIN at the next logon.
   Set the *OTP Code Length* for the number of characters.
   Click *Next*.



One Time Code User Management Wizard

Multi-Factor Token Delivery Settings
Select the delivery type to be used for Multi-Factor tokens.

A Multi-Factor token challenge can be delivered to a device via SMS or email or can be remotely generated via the Authenticator App. SMS and email tokens can be sent instantly (Real-Time) or in advance (Pre-Send). Tokens sent in advance can be given a time to live before they expire.

Delivery Method: No delivery / Authenticator App

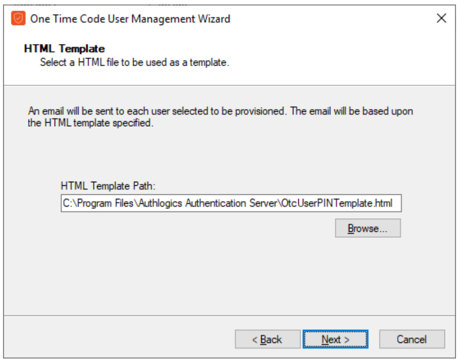
Queue Type: Real-Time

Token Lifespan: 15 Minutes

Codes / message: 1

8. Select the delivery method for Multi-Factor tokens. When selecting a method, ensure that the user has either an Email address or Mobile telephone number that tokens will be delivered to.
   Queue Type determines whether tokens will be pre-sent or generated in Real-Time. When Queue Type is set to Pre-Send, an administrator must then specify the Token Lifespan for these token types and how many pre-sent tokens are delivered per message.
   The *Enable remote seed for soft tokens* requires that the remote seed value generated by the Authentication Server be configured on the MFA device registered

with the user account otherwise authentication will fail. This value will automatically be installed via the QR code device enrolment process.
Click Next.



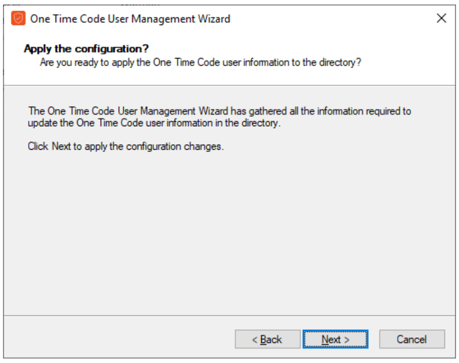
HTML Template

Select a HTML file to be used as a template.

An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified.

HTML Template Path: C:\Program Files\Authlogics Authentication Server\OtcUserPINTemplate.html

9. Specify an HTML Template Path to the automated notification letter/email each user will receive. This HTML file can be modified and customised for your organisation. Each letter/email will be customised for the user to contain their unique information by substituting HTML comment values in the template.



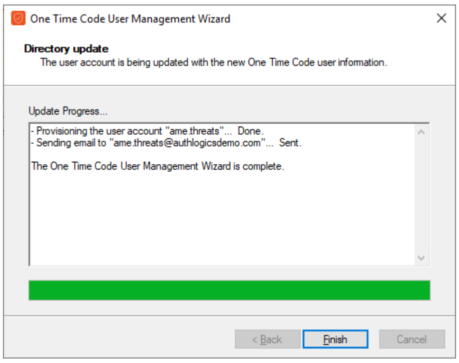
Apply the configuration?

Are you ready to apply the One Time Code user information to the directory?

The One Time Code User Management Wizard has gathered all the information required to update the One Time Code user information in the directory.

Click Next to apply the configuration changes.

10. Click *Next* to apply the configuration changes.



Directory update

The user account is being updated with the new One Time Code user information.

Update Progress...

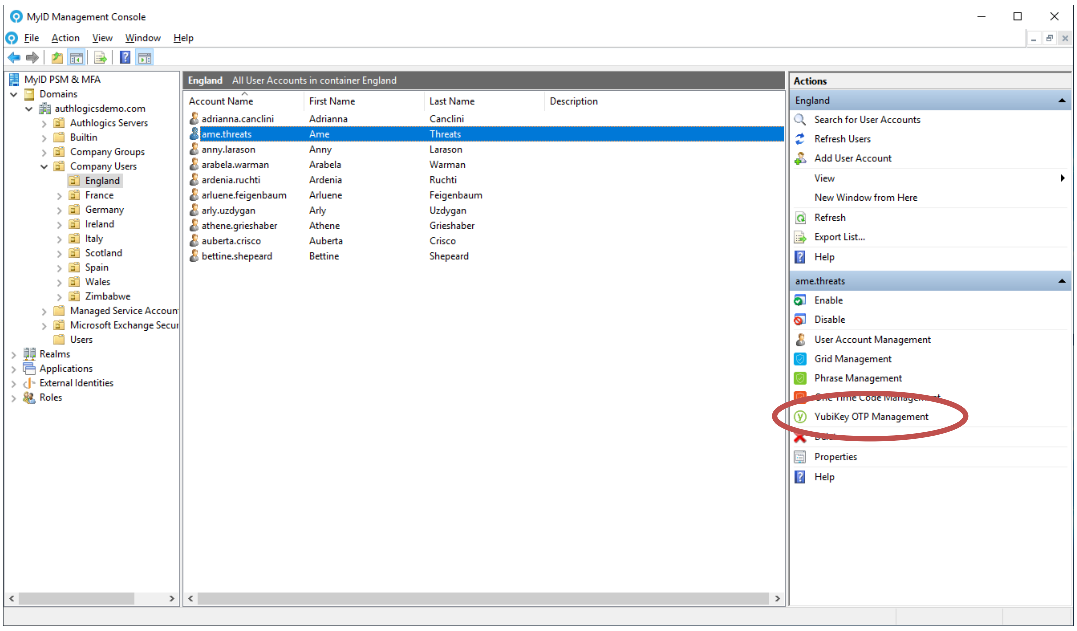
```
- Provisioning the user account "ame.threats"...  Done.
- Sending email to "ame.threats@authlogicsdemo.com"...  Sent.

The One Time Code User Management Wizard is complete.
```

11. Click *Finish*.

Setting up a user for YubiKey OTP

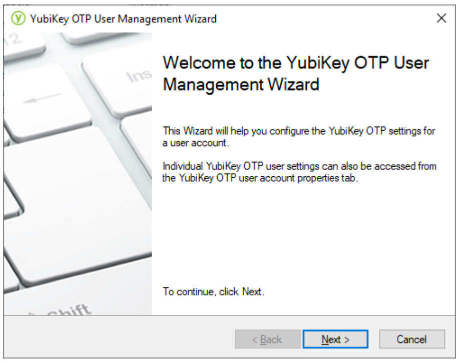
Once an MyID user account has been created you can configure it for use with One Time Code.

1. Expand Domains and select the appropriate OU or expand Realms and select the appropriate Realm. Select the user account (or accounts) to manage YubiKey OTP settings.



Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

2. Click *YubiKey OTP Management* from the menu on the right or from the right-click menu to start the YubiKey OTP User Management Wizard.



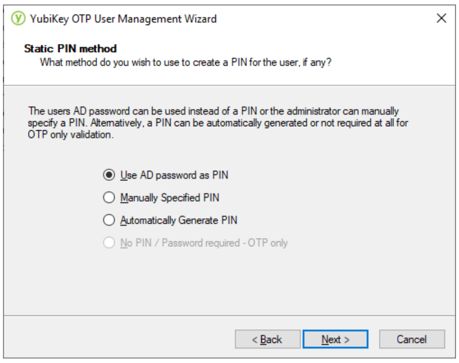
Welcome to the YubiKey OTP User Management Wizard

This Wizard will help you configure the YubiKey OTP settings for a user account.

Individual YubiKey OTP user settings can also be accessed from the YubiKey OTP user account properties tab.

To continue, click Next.

3. Click *Next*.



Static PIN method

What method do you wish to use to create a PIN for the user, if any?

The users AD password can be used instead of a PIN or the administrator can manually specify a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation.

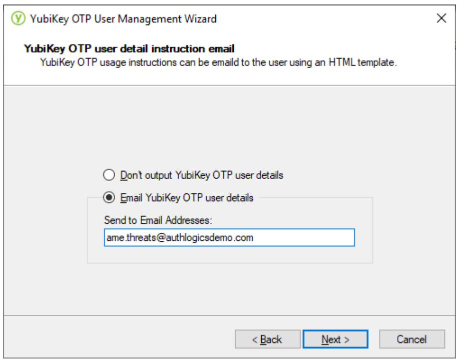
● Use AD password as PIN

○ Manually Specified PIN

○ Automatically Generate PIN

○ No PIN / Password required - OTP only

4. The user’s AD password can be used instead of a PIN, or the administrator can manually specify a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation. Finally, if enabled through Global settings, No additional PIN can be specified. If multiple accounts were selected before starting the wizard then the *Manually Specified* option is not available.
   Click Next.



YubiKey OTP user detail instruction email

YubiKey OTP usage instructions can be emaild to the user using an HTML template.

○ Don't output YubiKey OTP user details

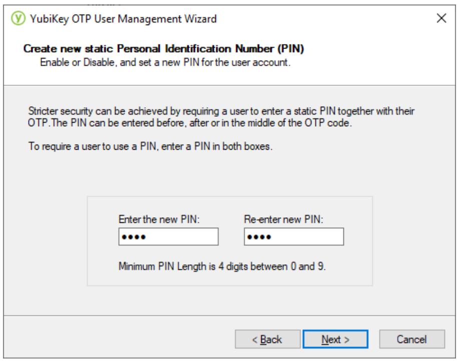
● Email YubiKey OTP user details

Send to Email Addresses: ame.threats@authlogicsdemo.com

5. Select the method used to distribute the One Time Code settings as well as One Time Code usage instructions to the user. Auto-generated information can be either printed or emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details, this option is not available for auto-generated details.
   Click *Next*.

Note

For instructions on manually specifying a PIN proceed to step 6, otherwise, skip to step 7.



YubiKey OTP User Management Wizard

Create new static Personal Identification Number (PIN)
Enable or Disable, and set a new PIN for the user account.

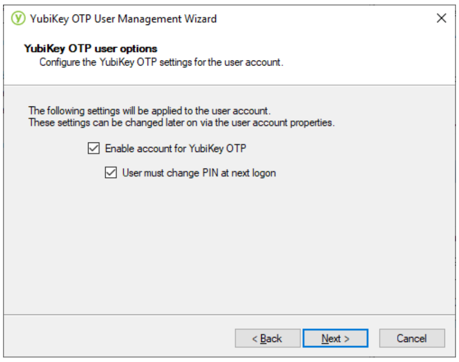
Stricter security can be achieved by requiring a user to enter a static PIN together with their OTP. The PIN can be entered before, after or in the middle of the OTP code.

To require a user to use a PIN, enter a PIN in both boxes.

Enter the new PIN: ••••
Re-enter new PIN: ••••

Minimum PIN Length is 4 digits between 0 and 9.

6. Enter the user's PIN and confirm the PIN. Click *Next*.



YubiKey OTP User Management Wizard

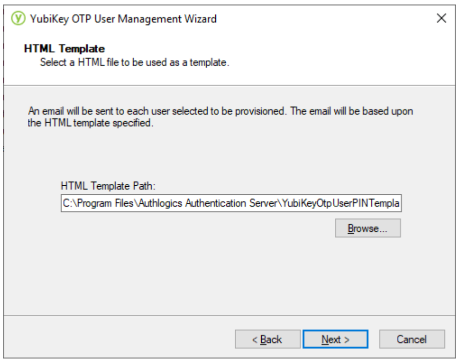
YubiKey OTP user options
Configure the YubiKey OTP settings for the user account.

The following settings will be applied to the user account.
These settings can be changed later on via the user account properties.

☑ Enable account for YubiKey OTP

☑ User must change PIN at next logon

7. Configure YubiKey OTP user options.
   An account can be set so that the next time the user logins with this account, that user will be forced to change the PIN at the next logon.
   Click *Next*.



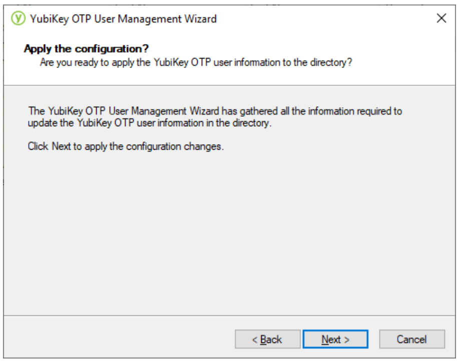
YubiKey OTP User Management Wizard

HTML Template
Select a HTML file to be used as a template.

An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified.

HTML Template Path: C:\Program Files\Authlogics Authentication Server\YubiKeyOtpUserPINTempla

8. Specify an HTML Template Path to the automated notification letter/email each user will receive. This HTML file can be modified and customised for your organisation. Each letter/email will be customised for the user to contain their unique information by substituting HTML comment values in the template.

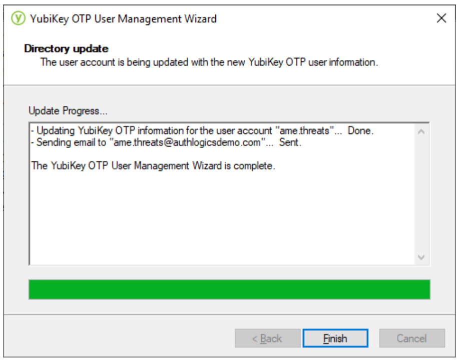


Apply the configuration?
Are you ready to apply the YubiKey OTP user information to the directory?

The YubiKey OTP User Management Wizard has gathered all the information required to update the YubiKey OTP user information in the directory.

Click Next to apply the configuration changes.

9. Click *Next* to apply the configuration changes.



Directory update
The user account is being updated with the new YubiKey OTP user infomation.

Update Progress...

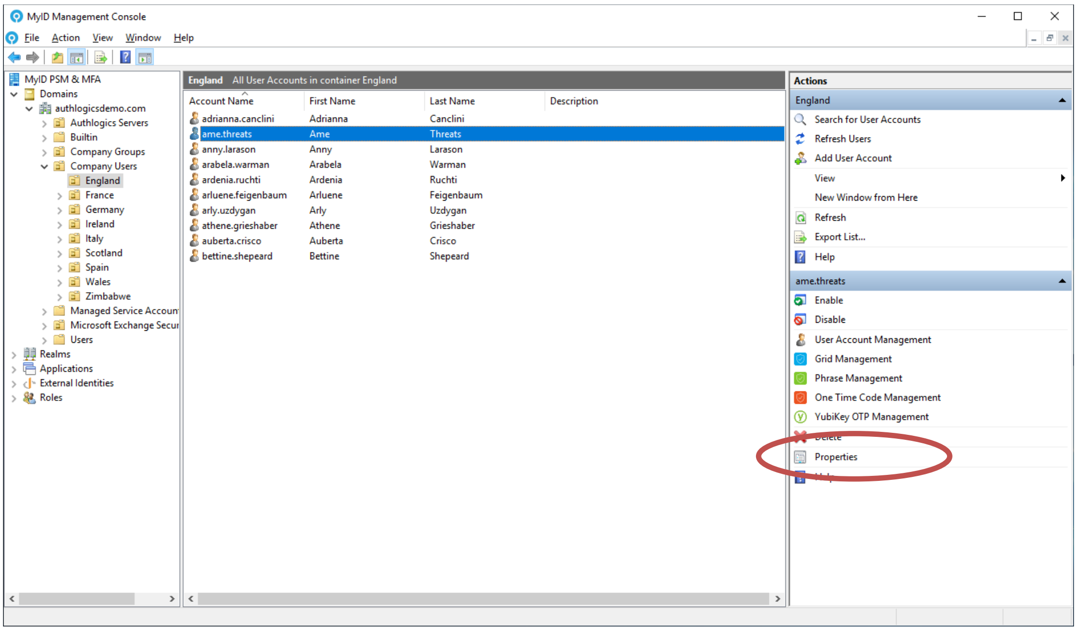
```
- Updating YubiKey OTP infomation for the user account "ame.threats"...  Done.
- Sending email to "ame.threats@authlogicsdemo.com"...  Sent.

The YubiKey OTP User Management Wizard is complete.
```

10. Click *Finish*.

Multi-Factor Devices assigned to a user account

Users will enrol their MFA device via the self-service portal. The devices assigned to the user can be viewed through the MyID MMC.

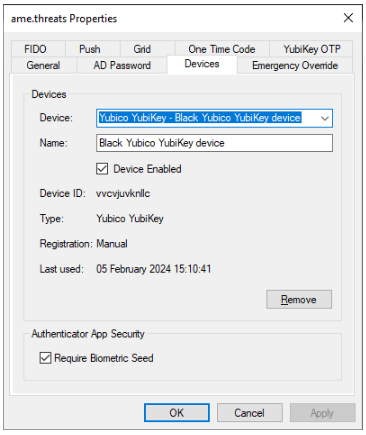
1. Expand the Domain and select the appropriate OU and user account to manage.



England All User Accounts in container England

Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

2. Click *Properties* and select the *Devices* tab.



Devices

Device: Yubico YubiKey - Black Yubico YubiKey device

Name: Black Yubico YubiKey device

☑ Device Enabled

Device ID: vvcvjuvknllc

Type: Yubico YubiKey

Registration: Manual

Last used: 05 February 2024 15:10:41

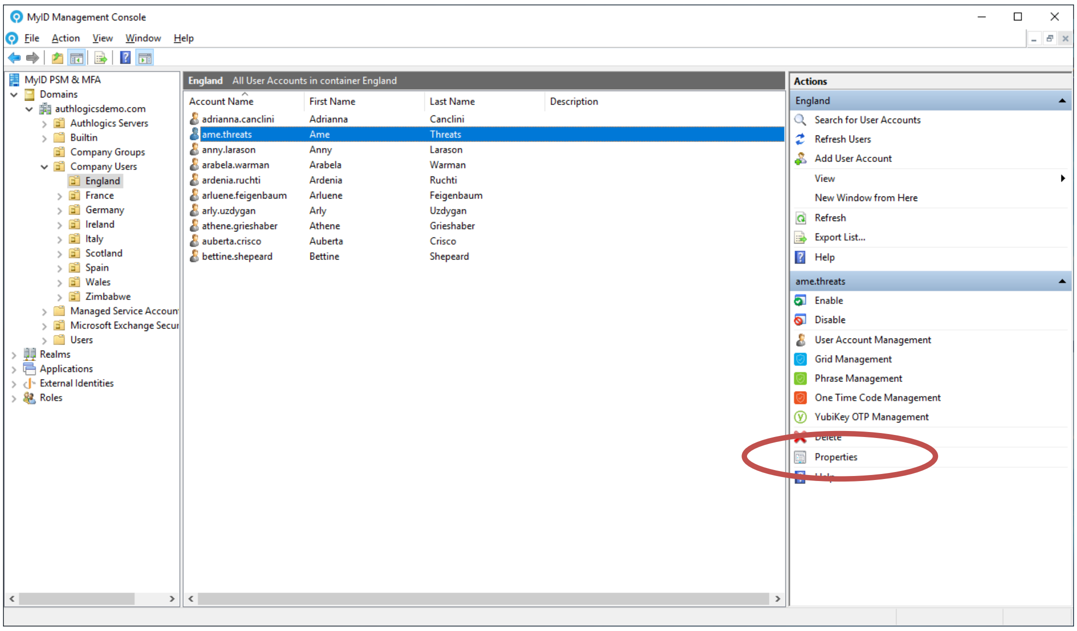
Authenticator App Security

☑ Require Biometric Seed

Up to 10 devices can be added for each user, repeat the process for each MFA device. Each device can be enabled or disabled as needed, e.g. it if is temporarily misplaced. Administrators can also enforce the user to provide Biometrics when access tokens that support Biometric validation.

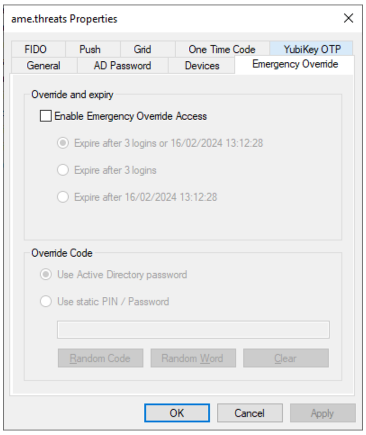
Assigning Emergency Override Access to a user (MMC)

1. Ensure that Allow *Emergency Override Access* is ticked on the global settings *General* tab. See the Global Settings Walkthrough section for further information.



Account Name	First Name	Last Name	Description
adrianna.canclini	Adrianna	Canclini	
ame.threats	Ame	Threats	
anny.larason	Anny	Larason	
arabela.warman	Arabela	Warman	
ardenia.ruchti	Ardenia	Ruchti	
arluene.feigenbaum	Arluene	Feigenbaum	
arly.uzdygan	Arly	Uzdygan	
athene.grieshaber	Athene	Grieshaber	
auberta.crisco	Auberta	Crisco	
bettine.shepeard	Bettine	Shepeard	

2. Expand Domains and select the appropriate OU or expand Realms and select the appropriate Realm. Select the user account to manage.
Click Properties and select the Emergency Override tab.



Override and expiry

□ Enable Emergency Override Access

● Expire after 3 logins or 16/02/2024 13:12:28

○ Expire after 3 logins

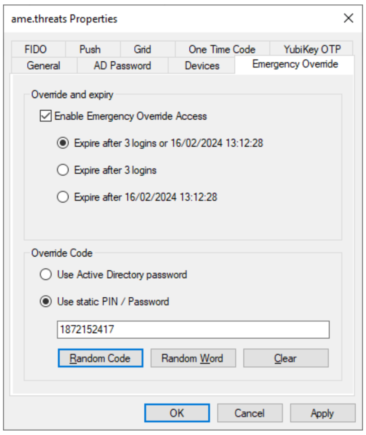
○ Expire after 16/02/2024 13:12:28

Override Code

● Use Active Directory password

○ Use static PIN / Password

3. Tick the Enable Emergency Override Access box.
Select under which circumstances the emergency override functionally will be automatically disabled. Options include at a specific date and time, after a specific number of uses or both; the default is both.
Configure the user to utilise their existing Active Directory password as an emergency override code as it is something they should already know.
Alternatively, specify a PIN or a Password for the user of at least 6 digits. To assist in choosing a PIN or password you can click the Random Code or Random Word buttons to create one for you.



Override and expiry

☑ Enable Emergency Override Access

● Expire after 3 logins or 16/02/2024 13:12:28

○ Expire after 3 logins

○ Expire after 16/02/2024 13:12:28

Override Code

○ Use Active Directory password

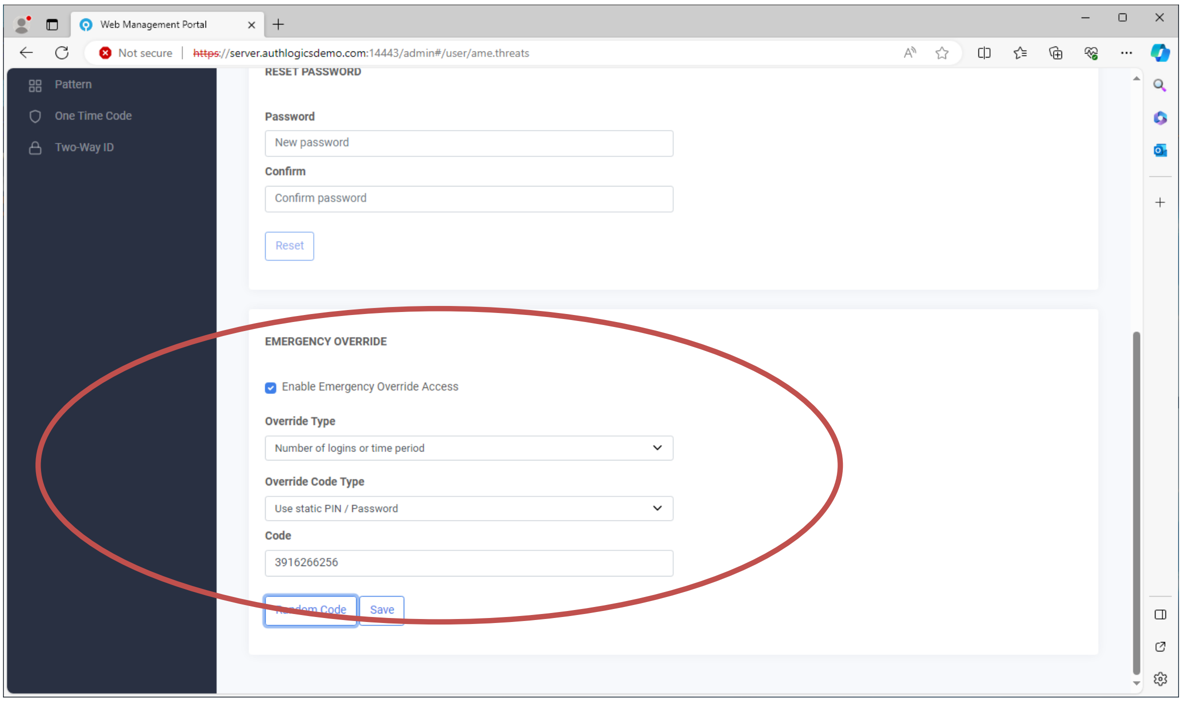
● Use static PIN / Password

1872152417

4. Click *Apply* or *OK* to save the configured settings for the user account.

Assigning Emergency Override Access to a user (Web Management Portal)

1. Ensure that Allow *Emergency Override Access* is ticked on the global settings *General* tab in the MMC. See the Global Settings Walkthrough section for further information.



RESET PASSWORD

Password: New password

Confirm: Confirm password

EMERGENCY OVERRIDE

☑ Enable Emergency Override Access

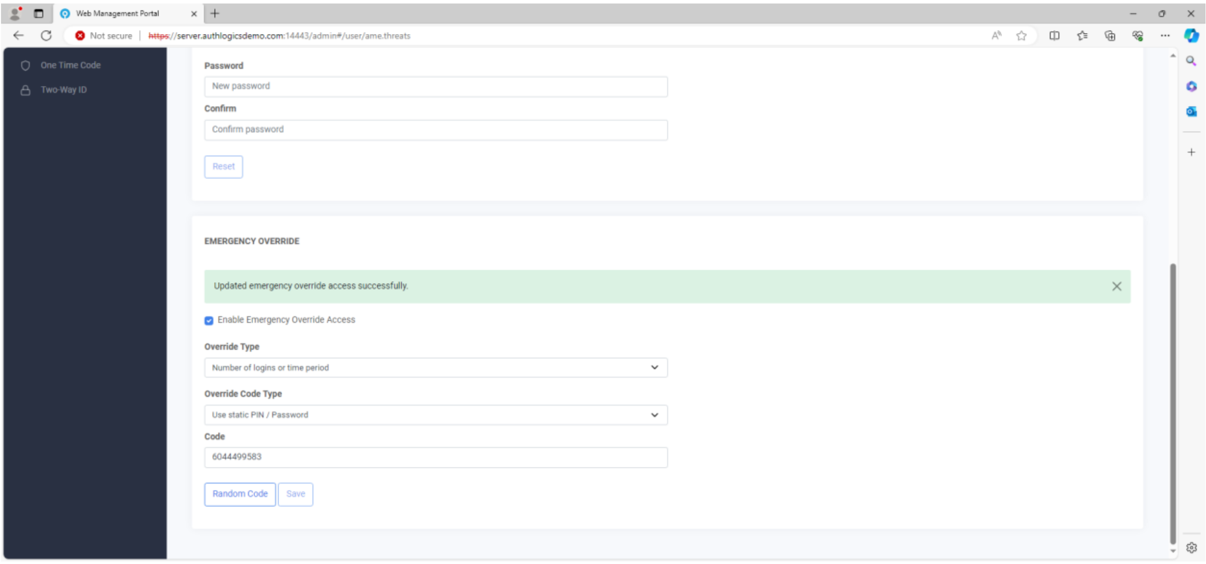
Override Type: Number of logins or time period

Override Code Type: Use static PIN / Password

Code: 3916266256

2. Load the Web Management Portal and select the user account to manage.
3. Check the Enable Emergency Override Access box.
4. Select the override type based on the number of logons, a period or both.
5. Configure the user to use their existing Active Directory password as an emergency override code as it is something they should already know. Alternatively, specify a PIN or a password for the user of at least 6 digits.

> **Tip**
> Click the **Random Code** button to generate a new random emergency override code.


Web Management Portal
Not secure
https://server.authlogicsdemo.com:14443/admin#/user/ame.threats
One Time Code
Two-Way ID

Password

New password

Confirm

Confirm password

Reset

EMERGENCY OVERRIDE

Updated emergency override access successfully.

☑ Enable Emergency Override Access

Override Type: Number of logins or time period

Override Code Type: Use static PIN / Password

Code: 6044499583

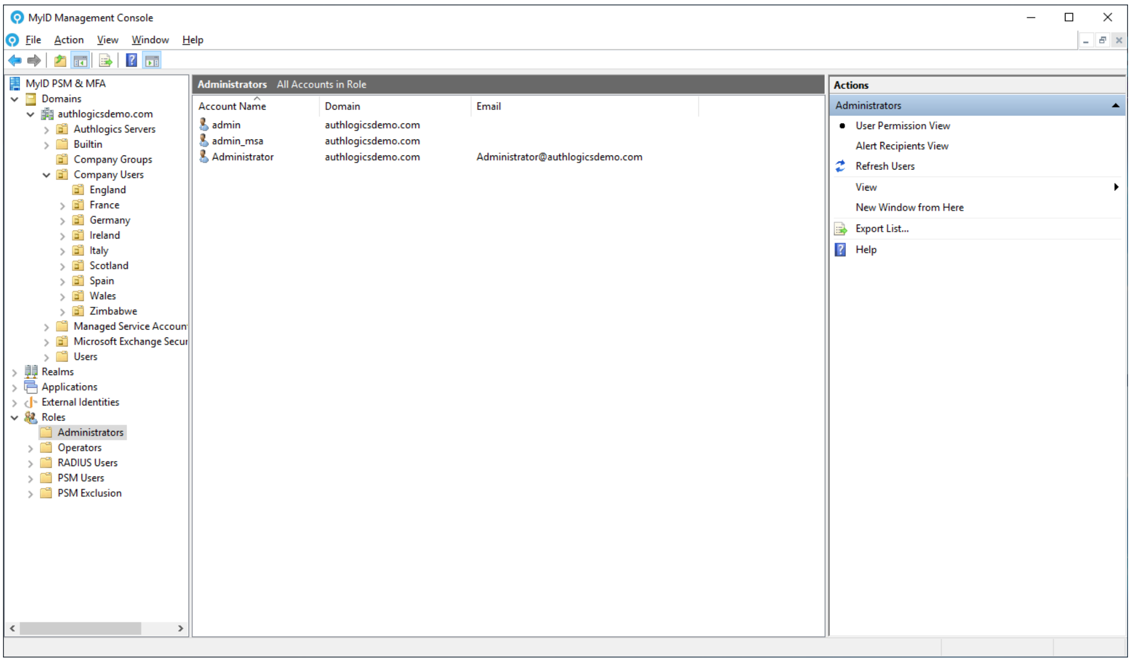
Random Code | Save

6. Click Save when done.

Roles

MyID Authentication Server provides administrators with the ability to assign rights to users for MyID administrative functions and product features. Users can be designated as Administrators and Operators.

Administrators can fully administer MyID via the MyID Management Console and perform day-to-day operational functions via the Web Management Portal. Members of the Operators role have access to the Web Management Portal which provides day-to-day operational functions, but they do not have access to the MyID Management Console.



Administrators All Accounts in Role

Account Name	Domain	Email
admin	authlogicsdemo.com	
admin_msa	authlogicsdemo.com	
Administrator	authlogicsdemo.com	Administrator@authlogicsdemo.com

MFA Only: Authorisation via RADIUS can be restricted via the RADIUS Users role.

PSM Only: User accounts that should be protected by PSM can be specified via the PSM Users role.

> **Note**
> Active Directory groups are created automatically for Administrators and Operators and are assigned to the roles by default. For all other roles, an AD group must be created manually first.

AD Group types for Roles

Both Global and Universal Security groups can be used with all MyID Roles. Group nesting is also supported, i.e. the groups may also contain other groups.

In addition, both Global and Universal Distribution groups can be used with the MyID Administrators Role to allow people to receive administrative alerts, but not have administrative permissions. See the *Administrator Role Views* section for further information.

For multi-domain forests, the groups can be created in any domain in the forest. It is recommended that Universal groups are used in multi-domain forests so that Global Catalog servers can be contacted to check role membership, otherwise, DCs from other domains may need to be contacted which can affect performance depending on the infrastructure.

Administrator Role Views

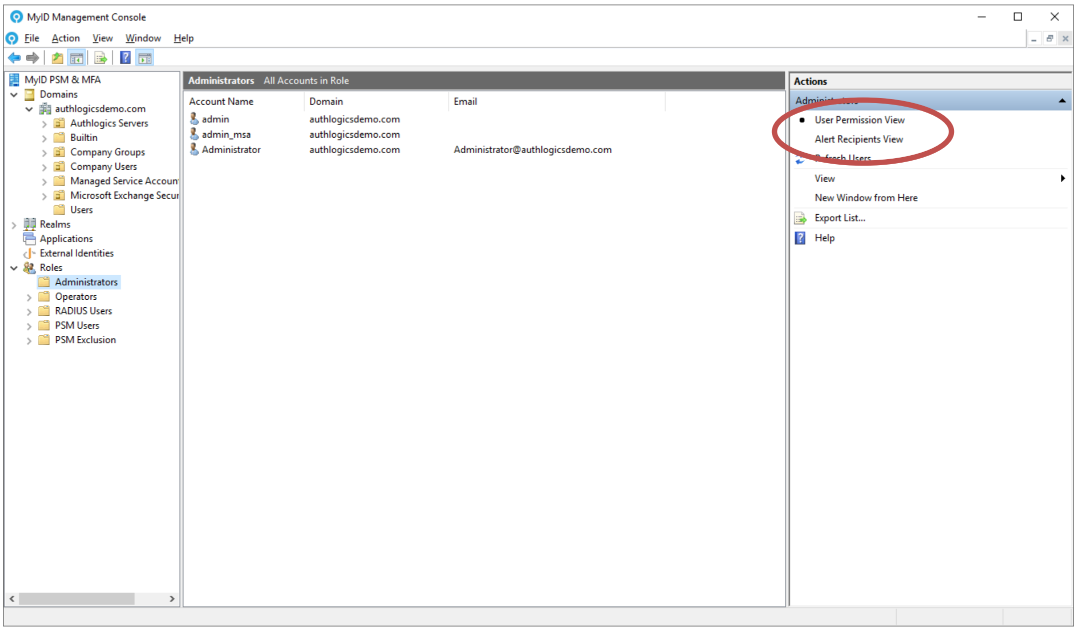
The Administrator Role is dual purposes and thus has two views:

1. **User Permissions View**: User accounts that have MyID Administrative permissions.
2. **Alert Recipients View**: Email addresses that should receive Admin Alerts.

The views can be toggled on the Actions pane in the MMC which allows you to determine the resultant set of users in each use case. To achieve this the members of the Authlogics Administrators group are processed differently as needed.

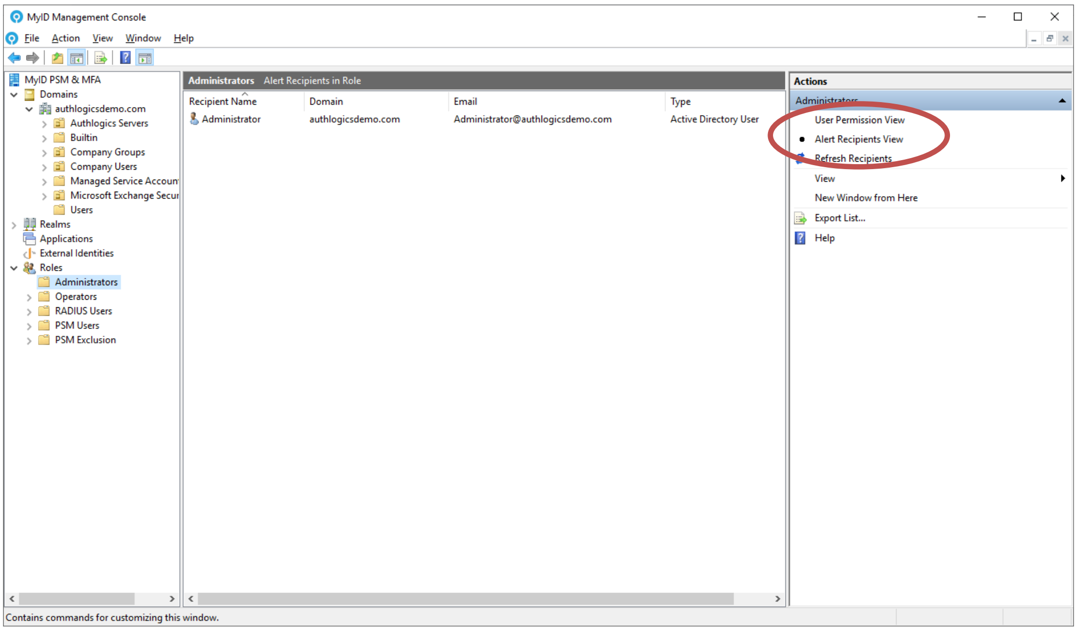
This feature is useful where admin personnel have split role user accounts and need to use their "admin" user account to perform administrative tasks but need to receive Admin Alerts on a "non-admin" user account.

Administrative Permissions can only be assigned to Active Directory User Accounts either through direct membership of the MyID Administrators group, or by being a member of a nested **Security group** (Global or Universal). Permissions are not assigned to Active Directory Contacts or via membership of a Distribution Group. The existence of an email address on a user account or group has no effect.



Account Name	Domain	Email
admin	authlogicsdemo.com	
admin_msa	authlogicsdemo.com	
Administrator	authlogicsdemo.com	Administrator@authlogicsdemo.com

Admin Alerts can be sent to Active Directory User Accounts, Contacts or Groups (Global or Universal, Security or Distribution) that **have an email address configured**. They can be direct members of the Authlogics Administrators group, or a member of a nested Security or Distribution group (Global or Universal). If a nested group does not have an email address configured on it then the members of the group will be processed individually, including other nested groups. However, if a group does has an email address configured on it then the email address of the group will be used and the members of the group will be ignored; leaving the email system (e.g Microsoft Exchange) to deliver the email to the group members.



Recipient Name	Domain	Email	Type
Administrator	authlogicsdemo.com	Administrator@authlogicsdemo.com	Active Directory User

To use split role user accounts for Admin Alerts simply create a Distribution group in AD, add the non-admin user accounts to it, then add the group to the Authlogics Administrators group.

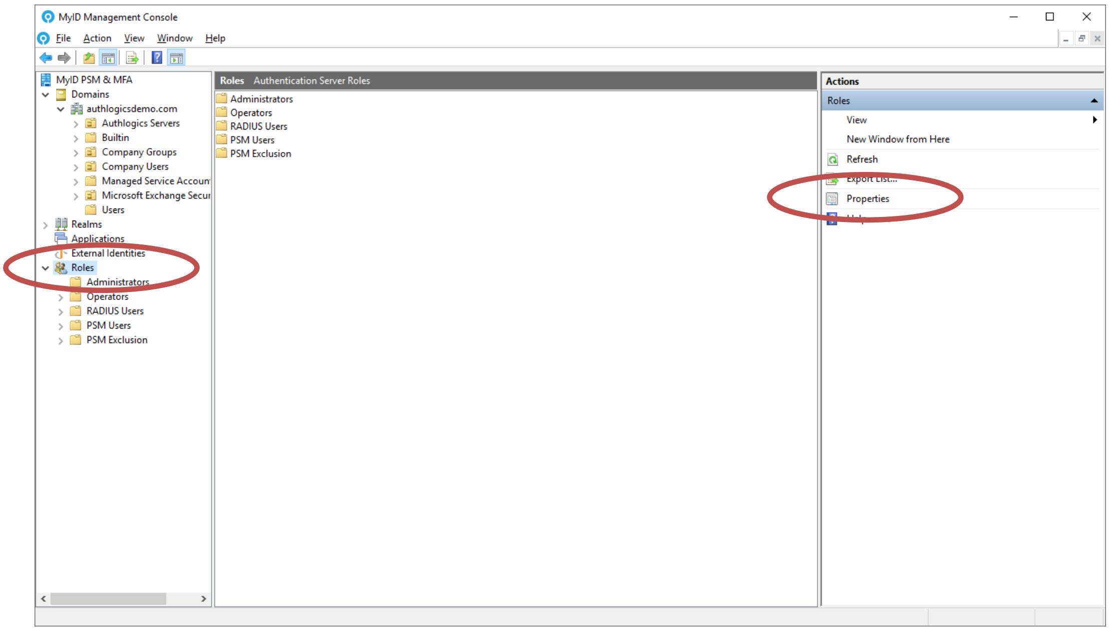
When using Microsoft Exchange, create a Mail Enabled Distribution group, add the non-admin user accounts to it, then add the group to the Authlogics Administrators group. MyID will then send Admin Alerts to the group and not directly to the member.

Managing Administrative Roles

Role membership is managed via the corresponding Active Directory groups which are created during the directory configuration. These groups can be renamed and moved to different OU's as needed but **should not be deleted**. Non-administrative roles are optional and the group filtering for the role can be enabled/disabled as needed.

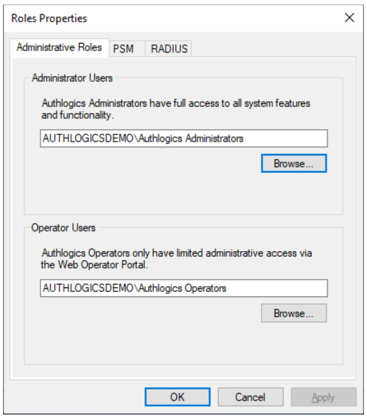
Role members cannot be added and removed via the MyID Management Console, this must be done by editing the appropriate Windows group either via the *Active Directory Users and Computers* MMC, or the *Local Users and Groups* MMC.

1. Open the MyID Authentication Server Management Console then expand Roles.



2. To assign Active Directory groups to Authlogics roles, select Roles and click *Properties.*

> **Note**
> The Active Directory groups must already exist in the domain.
> Authlogics Admin groups are created during setup.


Roles Properties

Administrative Roles | PSM | RADIUS

Administrator Users

Authlogics Administrators have full access to all system features and functionality.

AUTHLOGICSDEMO\Authlogics Administrators

Browse...

Operator Users

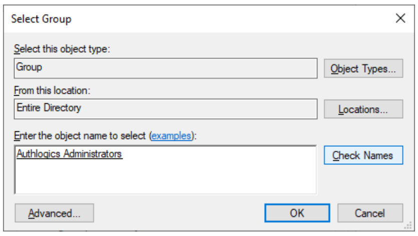
Authlogics Operators only have limited administrative access via the Web Operator Portal.

AUTHLOGICSDEMO\Authlogics Operators

Browse...

OK Cancel Apply

3. To select Administrators, Click *Browse...* in the Administrators Group section.

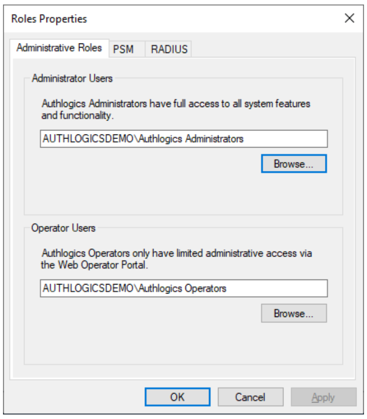


Select this object type: Group

From this location: Entire Directory

Enter the object name to select (examples): Authlogics Administrators

4. Locate the Active Directory group and click *OK.*



Administrator Users

Authlogics Administrators have full access to all system features and functionality.

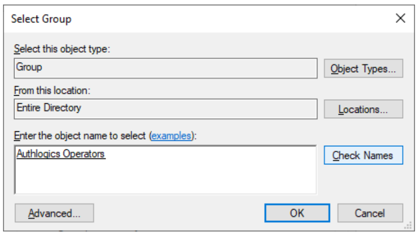
AUTHLOGICSDEMO\Authlogics Administrators

Operator Users

Authlogics Operators only have limited administrative access via the Web Operator Portal.

AUTHLOGICSDEMO\Authlogics Operators

5. To select Operators, Click *Browse...* in the Operator Group section.



Select this object type: Group

From this location: Entire Directory

Enter the object name to select (examples): Authlogics Operators

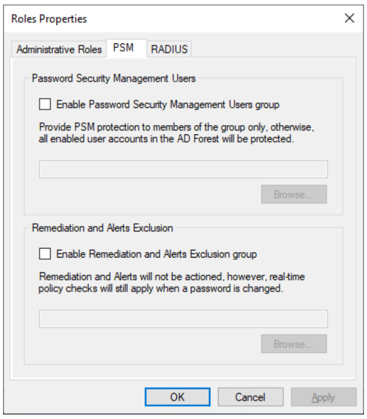
6. Locate the Active Directory group and click *OK.*

Managing the Password Security Management Users Role

1. To assign Active Directory groups to Authlogics roles, select Roles and click *Properties.*

> **Note**
>
> The Active Directory groups must already exist in the domain.
>
> Default PSM groups are NOT created during setup.

2. Select the *PSM Filters* tab.



Password Security Management Users

☐ Enable Password Security Management Users group

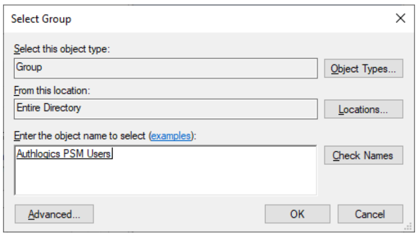
Provide PSM protection to members of the group only, otherwise, all enabled user accounts in the AD Forest will be protected.

Remediation and Alerts Exclusion

☐ Enable Remediation and Alerts Exclusion group

Remediation and Alerts will not be actioned, however, real-time policy checks will still apply when a password is changed.

3. Check the Enable Password Security Management Users group box and click Browse…

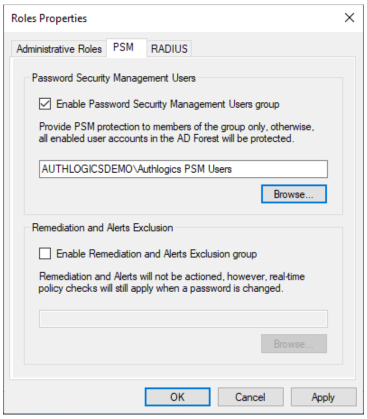


Select this object type: Group

From this location: Entire Directory

Enter the object name to select (examples): Authlogics PSM Users

4. Locate the Active Directory Password Policy group and click *OK.*



Password Security Management Users

☑ Enable Password Security Management Users group

Provide PSM protection to members of the group only, otherwise, all enabled user accounts in the AD Forest will be protected.

AUTHLOGICSDEMO\Authlogics PSM Users

Remediation and Alerts Exclusion

☐ Enable Remediation and Alerts Exclusion group

Remediation and Alerts will not be actioned, however, real-time policy checks will still apply when a password is changed.

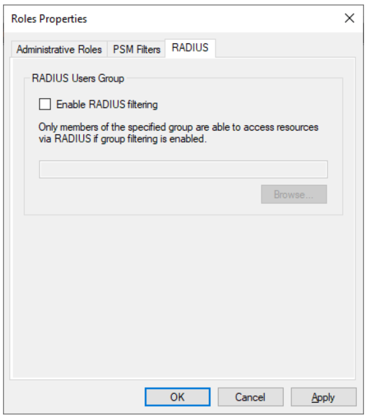
5. Click *OK.*

6. Select / Refresh the *PSM Users* role to view the members.

Managing the RADIUS Users Role

1. To assign Active Directory groups to Authlogics roles, select Roles and click *Properties.*

> **Note**
>
> The Active Directory groups must already exist in the domain.
>
> A default RADIUS group is NOT created during setup.



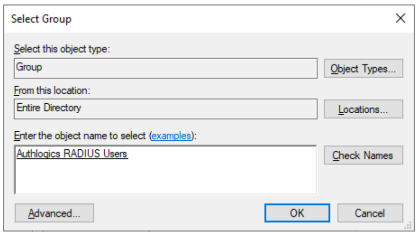
Roles Properties

RADIUS Users Group

☐ Enable RADIUS filtering

Only members of the specified group are able to access resources via RADIUS if group filtering is enabled.

2. Select the *RADIUS* tab.
3. Check the *Enable RADIUS filtering* box and click Browse...



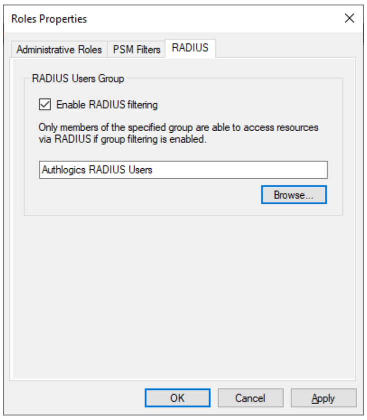
Select Group

Select this object type: Group

From this location: Entire Directory

Enter the object name to select (examples): Authlogics RADIUS Users

4. Locate the Active Directory RADIUS group and click *OK.*



Roles Properties

RADIUS Users Group

☑ Enable RADIUS filtering

Only members of the specified group are able to access resources via RADIUS if group filtering is enabled.

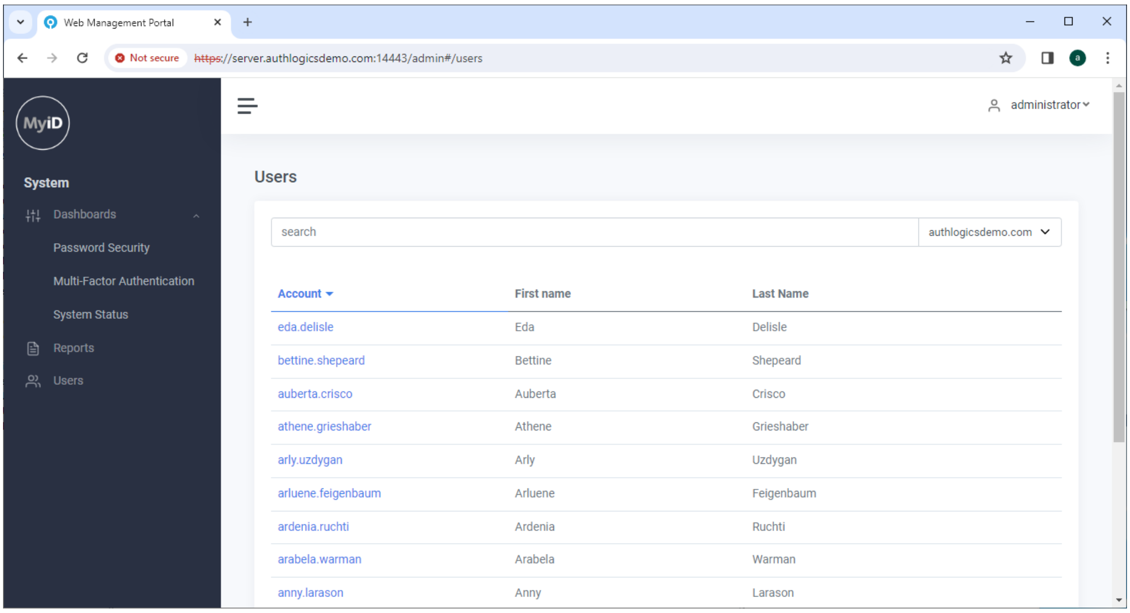
Authlogics RADIUS Users

5. Click *OK.*
6. Select / Refresh the *RADIUS Users* role to view the members.

The Web Management Portal

The MyID Web Management Portal provides operational staff with an easy-to-use web-based interface to perform common administrative tasks. Unlike the MMC UI, members of the Operators Role may only use the Web Management Portal. The Web Management Portal UI is well suited to tablet and touch-based devices.

The Web Management Portal includes dashboards to provide a high-level overview of the core Password Security and Multi-Factor Authentication events. The dashboard also provides administrators with the ability to generate reports.



Users

Account	First name	Last Name
eda.delisle	Eda	Delisle
bettine.shepeard	Bettine	Shepeard
auberta.crisco	Auberta	Crisco
athene.grieshaber	Athene	Grieshaber
arly.uzdygan	Arly	Uzdygan
arluene.feigenbaum	Arluene	Feigenbaum
ardenia.ruchti	Ardenia	Ruchti
arabela.warman	Arabela	Warman
anny.larason	Anny	Larason

Day to day user management functions available via the Web Management Portal include:

- View all MyID events for the selected user
- Enabled / Disable an account
- Unlock an account
- Update a Mobile / Cellular phone number
- Reset user passwords
- Configure Emergency Override Access
- View, Enable/Disable and resync MFA devices
- Configure MFA settings
- Reset a Grid Pattern
- Reset a Phrase answers
- Reset a One Time Code PIN
- Verify a One Time Code
- Perform 2-Way-Identification

The Web Management Portal does not allow the following actions:

- Modification of the global settings
- Adding new user accounts
- Provisioning MFA technologies
- Change the Pattern size
- Change logon times

The Web Management Portal is compatible with multiple web browsers including Microsoft Edge, Google Chrome, Firefox and Safari. Internet Explorer may function but is no longer recommended or supported.

Accessing the Web Management Portal

The Web Management Portal is accessed using Forms-based authentication with MFA or passwords, or Windows-based authentication. There is a start menu shortcut on the MyID server for easy access. Alternatively, you can use the following URL from any remote location:

https://servername:14443/admin

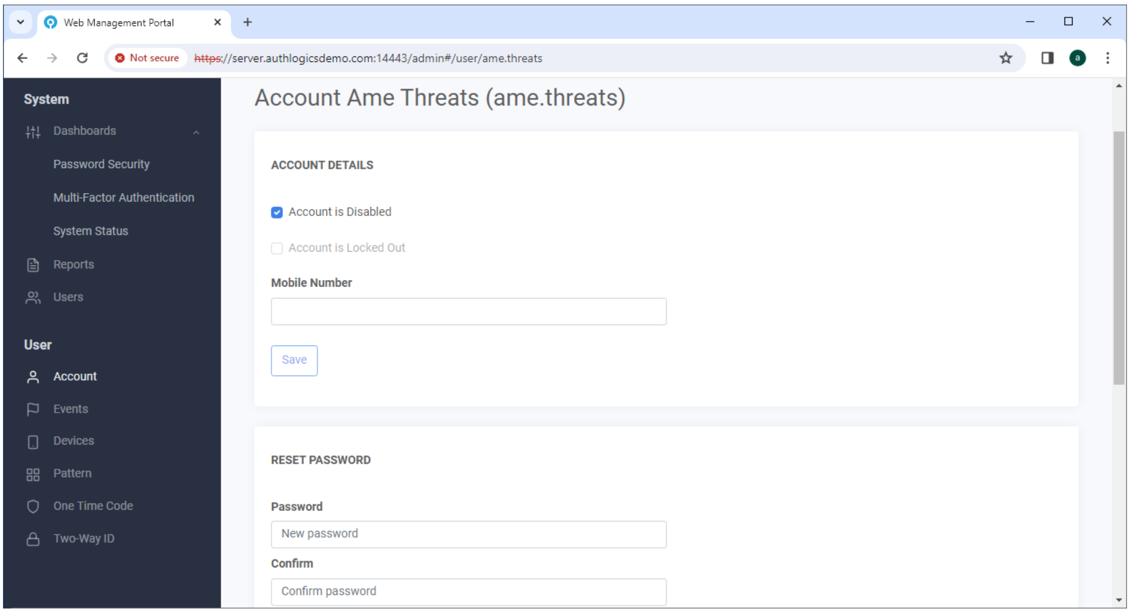
The portal can be accessed via HTTPS on port TCP:14443. The installation process configures a self-signed SSL certificate for use with the MyID Authentication Server, however, this certificate can be replaced with one from an internal or 3rd party trusted root when needed.

Using the Web Management Portal

The Web Management Portal is very simple to use and very intuitive. You start by selecting the domain in the forest to administer, if there is only a single domain then it will be selected automatically.

To search for a particular user, or to simply narrow down the list of users, enter some search criteria in the *Search* box and press enter.

To make changes to a user account simply click a user and the account details appear.



~~https~~://server.authlogicsdemo.com:14443/admin#/user/ame.threats

Account Ame Threats (ame.threats)

ACCOUNT DETAILS

☑ Account is Disabled

□ Account is Locked Out

Mobile Number

RESET PASSWORD

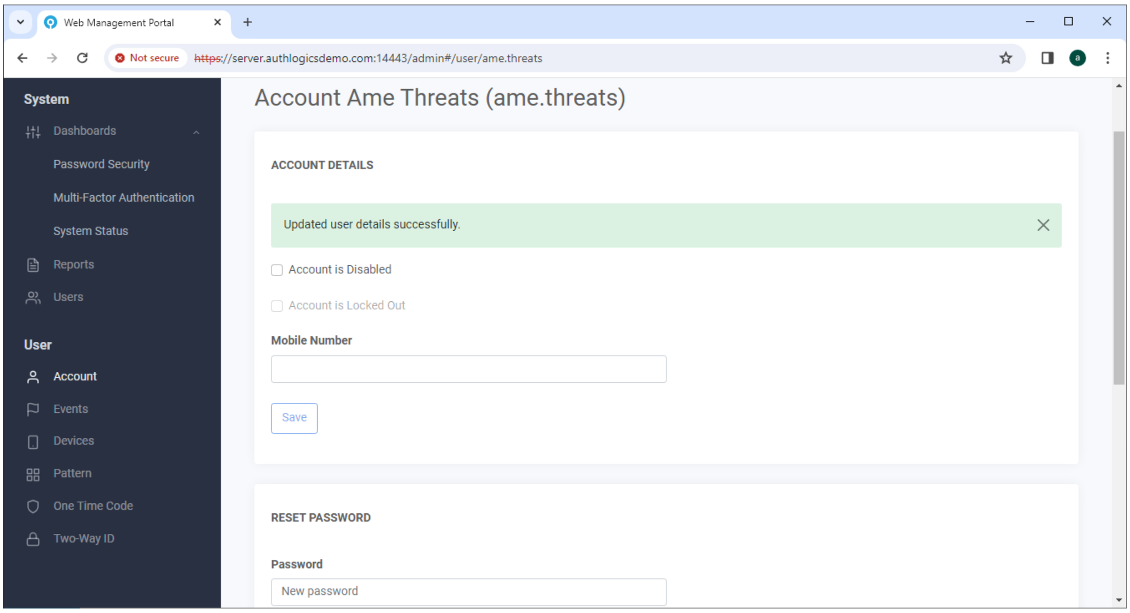
Password

New password

Confirm

Confirm password

Once you have made any required changes to a user account click the *Save* button. A notification will be displayed at the top of the console to show if the save was successful or not.



Account Ame Threats (ame.threats)

ACCOUNT DETAILS

Updated user details successfully.

□ Account is Disabled

□ Account is Locked Out

Mobile Number

RESET PASSWORD

Password

New password

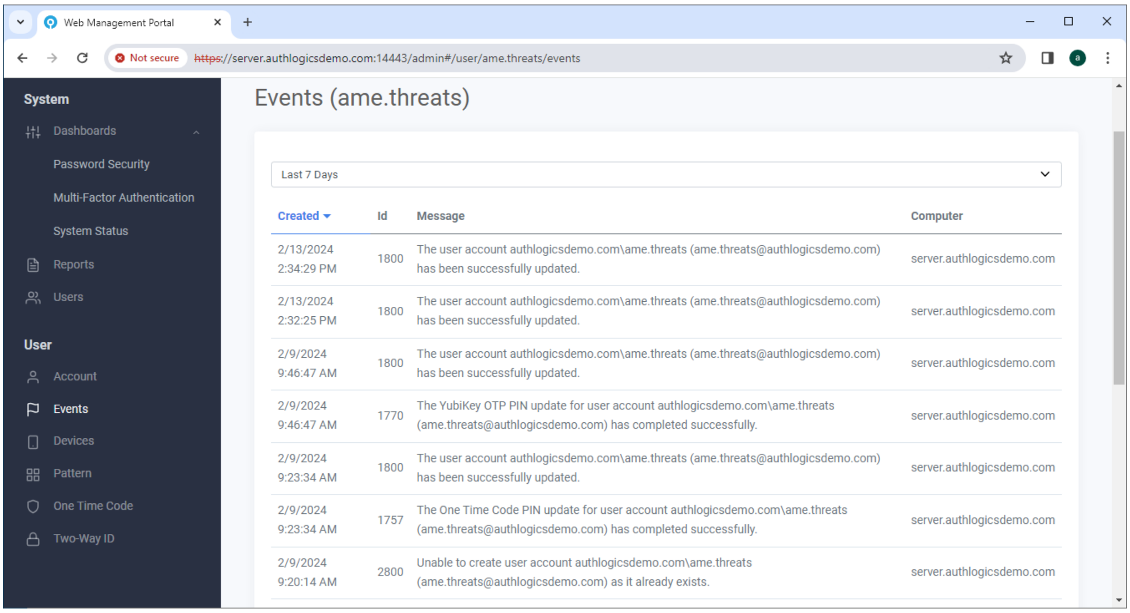
A record is kept in the MyID Server Application Event Log of changes made to user accounts.

Viewing all user events

Every user-related event is registered in the Windows Events log on the MyID Authentication Server or Domain Controller which processed the request. In environments containing multiple MyID Authentication Servers and Domain Controllers it can be challenging to locate the server containing the required log data.

The Web Management Portal Events view consolidates events from all servers into a single per user view.

1. Select the user account to access events for
2. Select the *Events* menu item.



Events (ame.threats)

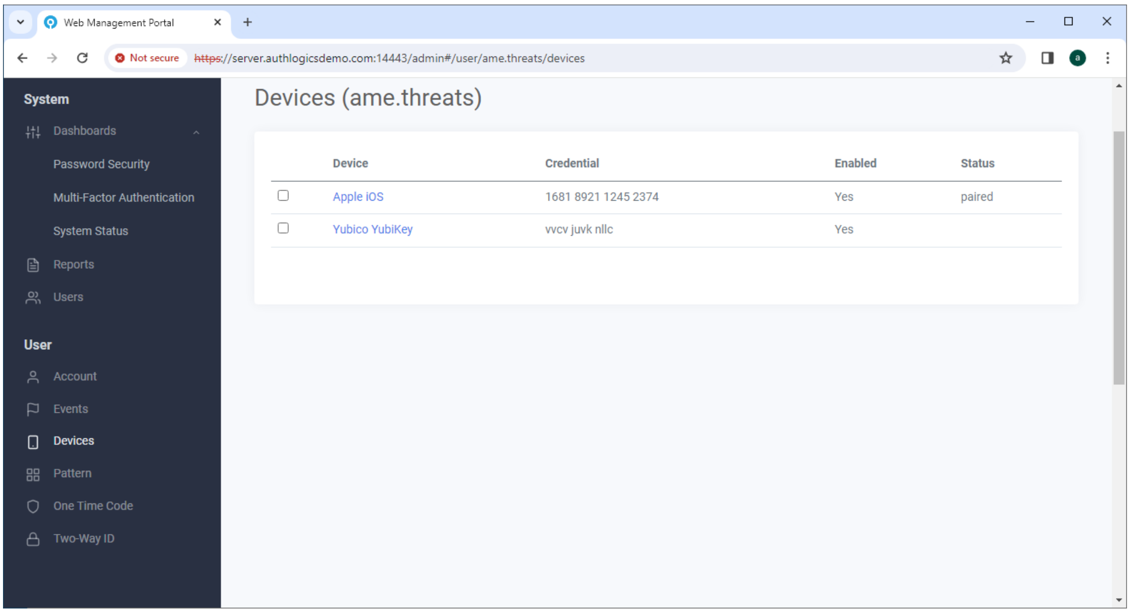
Last 7 Days

Created	Id	Message	Computer
2/13/2024 2:34:29 PM	1800	The user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) has been successfully updated.	server.authlogicsdemo.com
2/13/2024 2:32:25 PM	1800	The user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) has been successfully updated.	server.authlogicsdemo.com
2/9/2024 9:46:47 AM	1800	The user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) has been successfully updated.	server.authlogicsdemo.com
2/9/2024 9:46:47 AM	1770	The YubiKey OTP PIN update for user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) has completed successfully.	server.authlogicsdemo.com
2/9/2024 9:23:34 AM	1800	The user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) has been successfully updated.	server.authlogicsdemo.com
2/9/2024 9:23:34 AM	1757	The One Time Code PIN update for user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) has completed successfully.	server.authlogicsdemo.com
2/9/2024 9:20:14 AM	2800	Unable to create user account authlogicsdemo.com\ame.threats (ame.threats@authlogicsdemo.com) as it already exists.	server.authlogicsdemo.com

Viewing and Disabling Token Devices for a user account

A user account can have up to 10 devices running a soft token app linked to it. These can be assigned via the Web Management Portal, the MMC or the User Self Service Portal.

1. Select the user account to modify, then select the *Devices* tab.

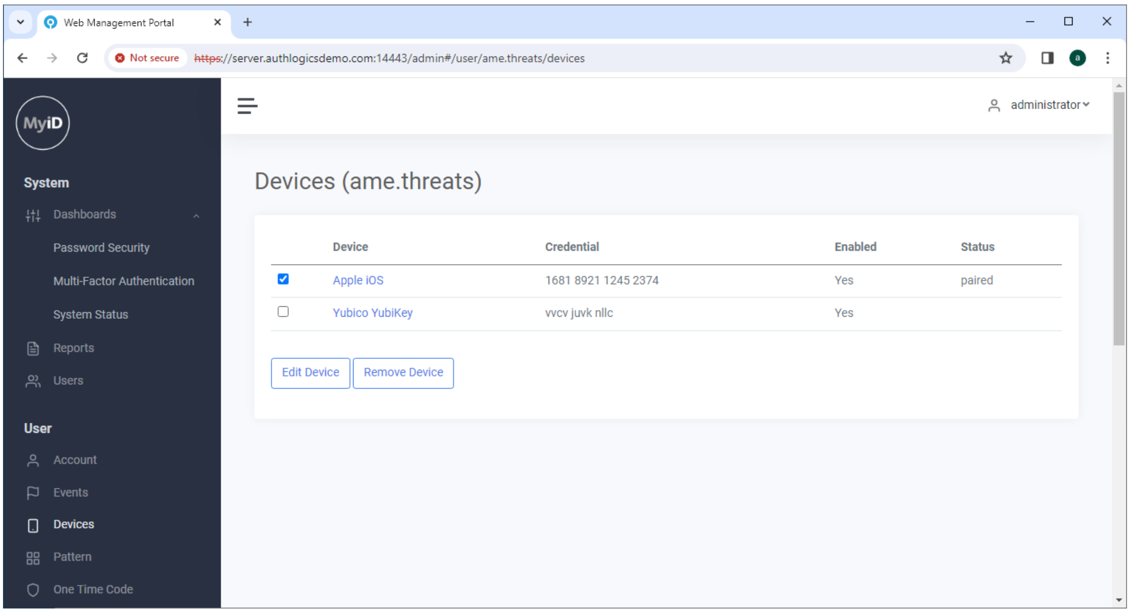


~~https~~://server.authlogicsdemo.com:14443/admin#/user/ame.threats/devices

Devices (ame.threats)

	Device	Credential	Enabled	Status
□	Apple iOS	1681 8921 1245 2374	Yes	paired
□	Yubico YubiKey	vvcv juvk nllc	Yes	

2. Tick the device to modify.



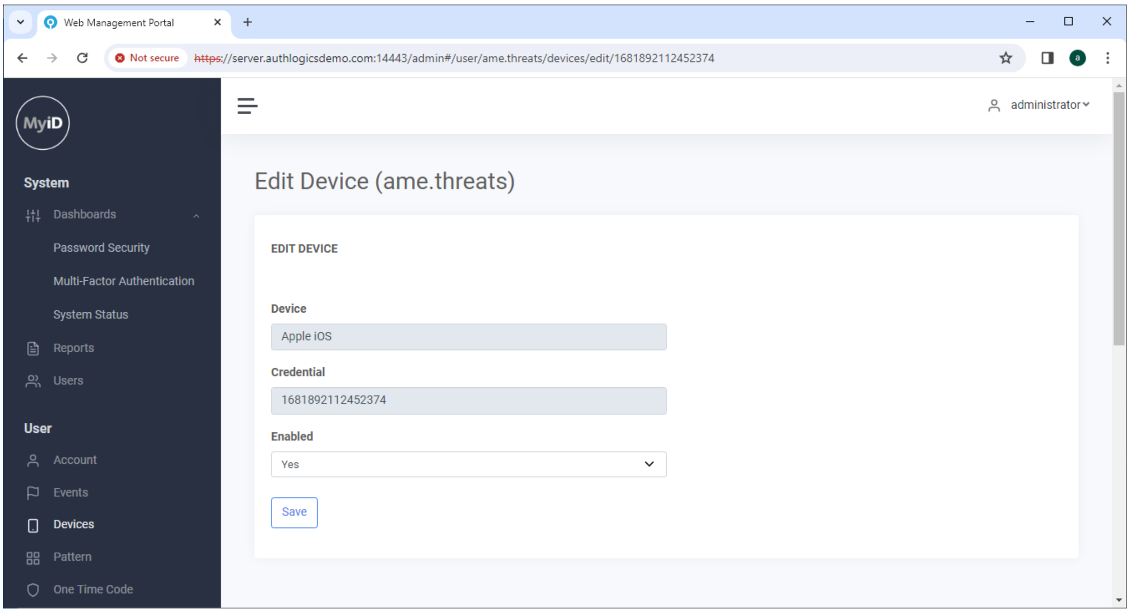
~~https~~://server.authlogicsdemo.com:14443/admin#/user/ame.threats/devices

Devices (ame.threats)

	Device	Credential	Enabled	Status
☑	Apple iOS	1681 8921 1245 2374	Yes	paired
□	Yubico YubiKey	vvcv juvk nllc	Yes	

Click *Edit*.

3. Select the Device to modify.



Edit Device (ame.threats)

EDIT DEVICE

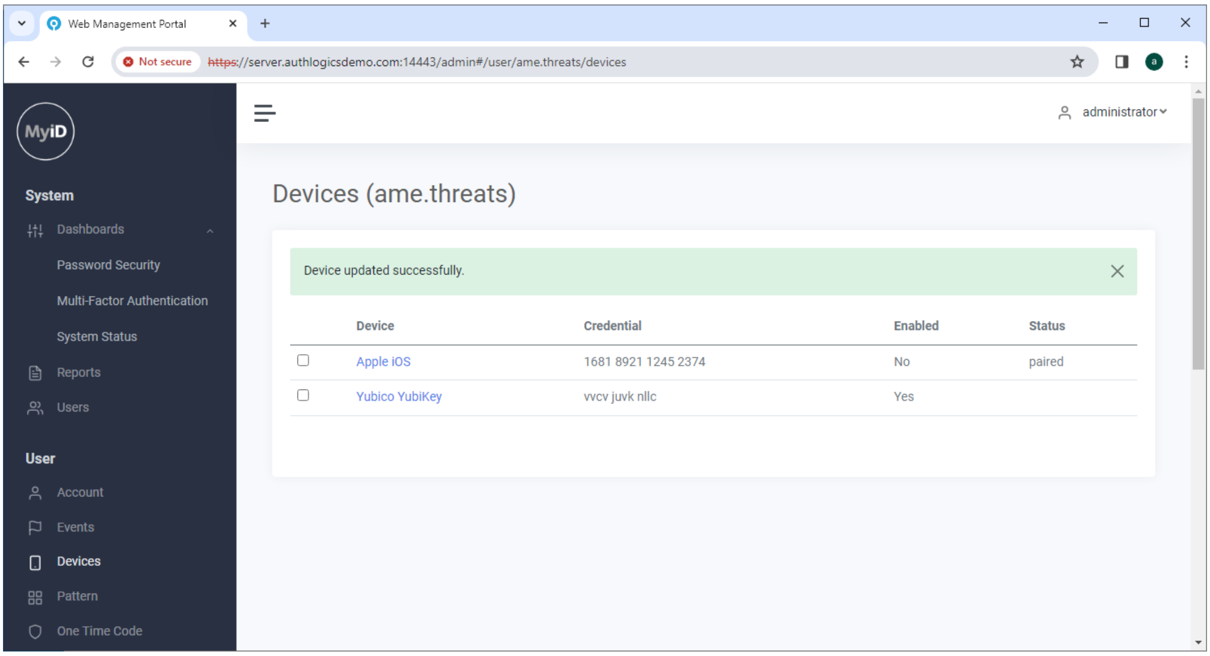
Device: Apple iOS

Credential: 1681892112452374

Enabled: Yes

Save

Set Enabled to *No* (conversely to re-enable a device, set Enabled to *Yes*) Click *Save*.



Devices (ame.threats)

Device updated successfully.

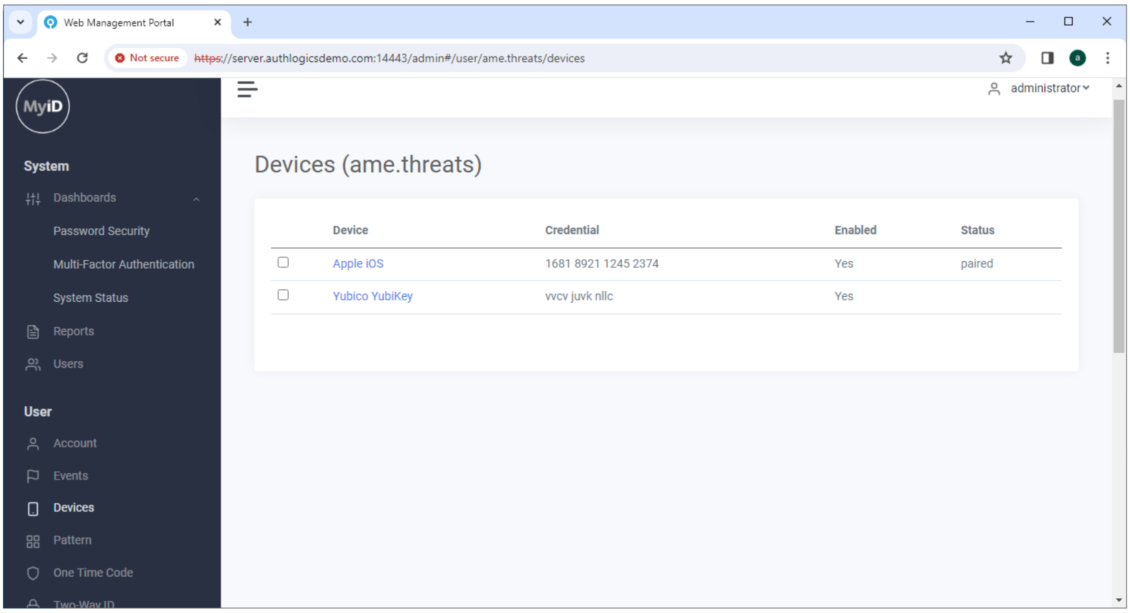
	Device	Credential	Enabled	Status
□	Apple iOS	1681 8921 1245 2374	No	paired
□	Yubico YubiKey	vvcv juvk nllc	Yes	

The device enabled state has now changed.

Removing a Token Device from a user account

If a user no longer possesses a device it can be removed from their account. These can be removed via the Web Management Portal, the MMC or the User Self Service Portal.

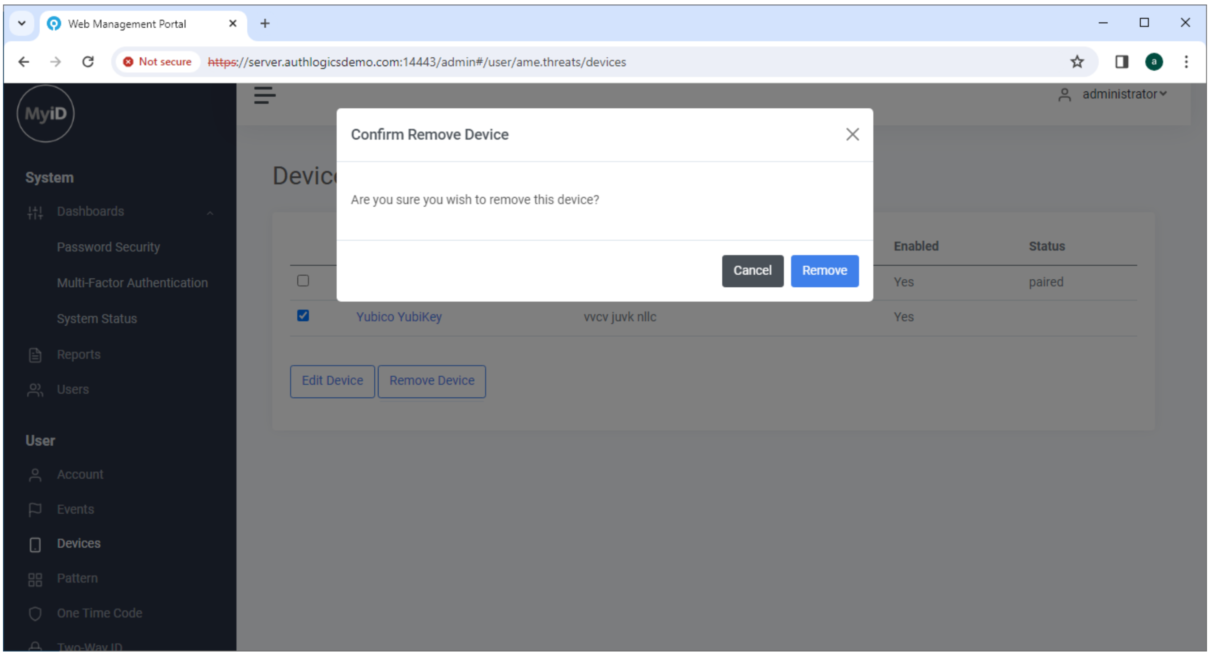
1. Select the user account to modify, then select the *Devices* tab.



Devices (ame.threats)

	Device	Credential	Enabled	Status
□	Apple iOS	1681 8921 1245 2374	Yes	paired
□	Yubico YubiKey	vvcv juvk nllc	Yes	

2. Tick the device you wish to remove and click the *Remove Device* button



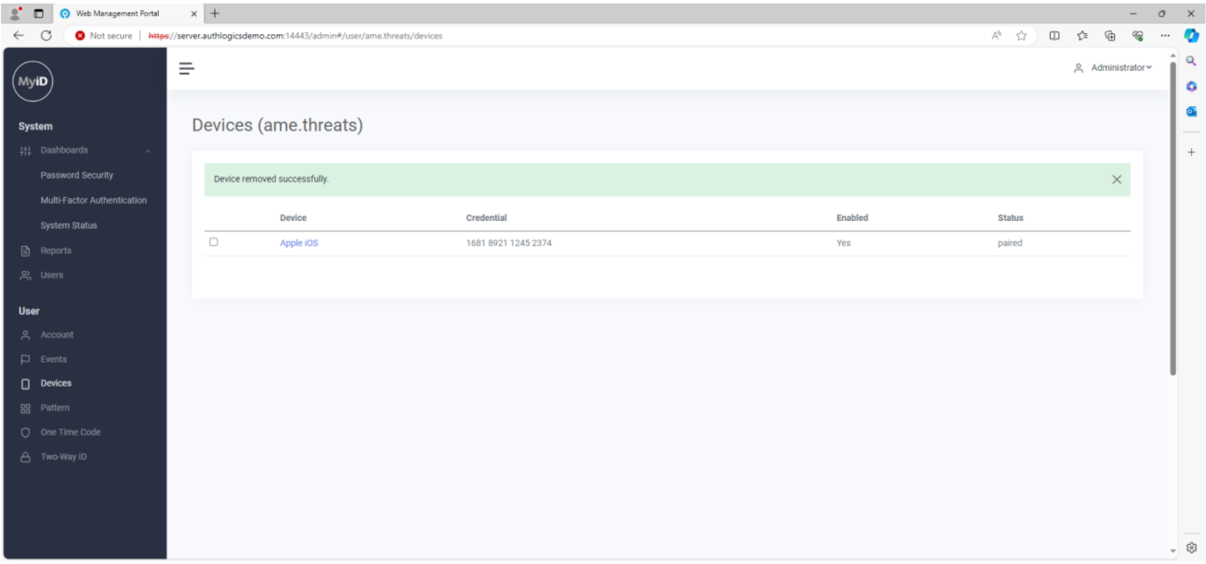
Confirm Remove Device

Are you sure you wish to remove this device?

Cancel Remove

			Enabled	Status
□			Yes	paired
☑	Yubico YubiKey	vvcv juvk nllc	Yes	

3. Click *Remove* to confirm the removal or *Cancel* to cancel the removal.



Devices (ame.threats)

Device removed successfully.

	Device	Credential	Enabled	Status
□	Apple iOS	1681 8921 1245 2374	Yes	paired

The device is now removed.

Web Management Portal Dashboards

The Dashboards are very simple to use. You start by selecting the Dashboards option under System in the Web Management Portal.

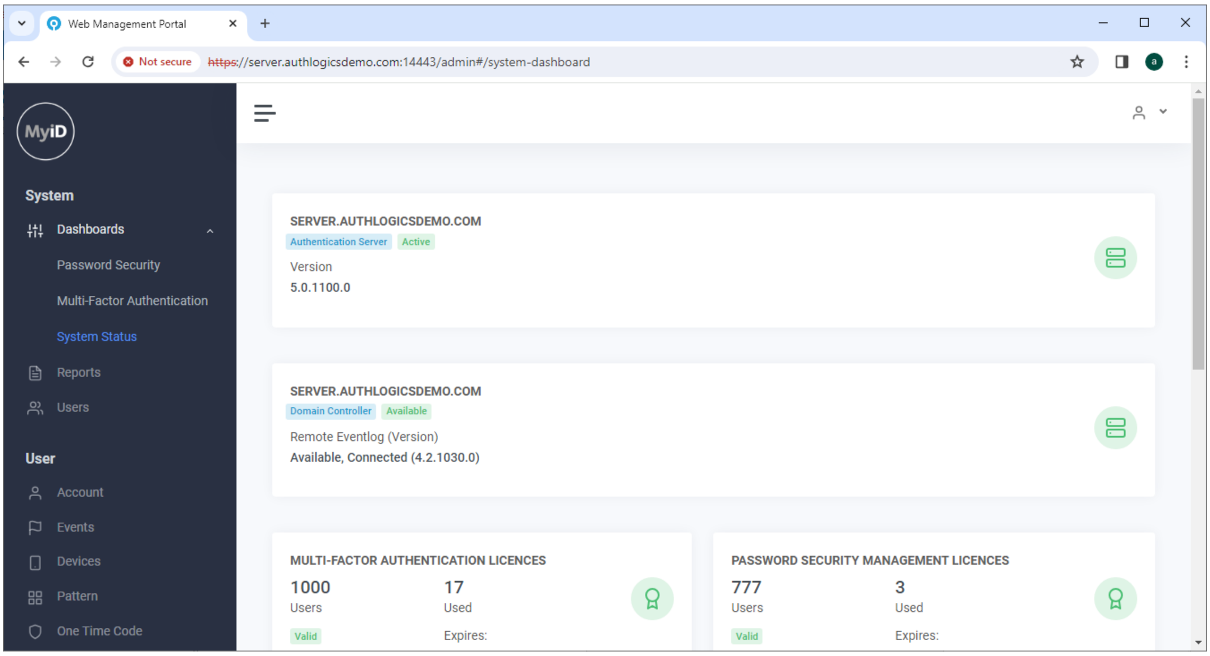
The Dashboard is broken into 3 categories; System Status, Password Security and Multi-Factor Authentication. The later 2 options will be available based on the applied MFA and PSM licences.

System Status

The System Status area of the Dashboards show all the MyID Authentication servers, Domain Controllers and applied Licences through the deployment.

Server listing shows the role of the server in the environment i.e. MyID Authentication Server and/or Domain Controller, the server's availability state and will also list MyID's ability to access the server's Windows Event Logs.

The licence component shows the applied licence, the validity of the licences, assigned and used quantities as well as the licence's expiry date.



SERVER.AUTHLOGICSDEMO.COM
Authentication Server Active
Version
5.0.1100.0

SERVER.AUTHLOGICSDEMO.COM
Domain Controller Available
Remote Eventlog (Version)
Available, Connected (4.2.1030.0)

MULTI-FACTOR AUTHENTICATION LICENCES
1000 Users 17 Used
Valid Expires:

PASSWORD SECURITY MANAGEMENT LICENCES
777 Users 3 Used
Valid Expires:

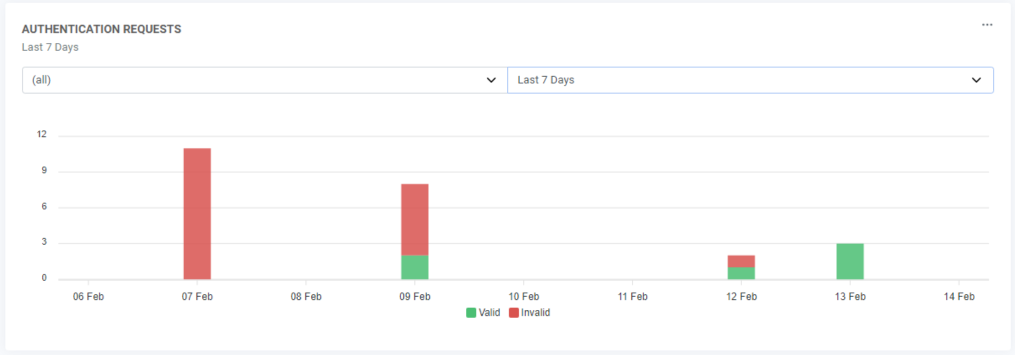
Multi-Factor Authentication

The Multi-Factor Authentication Dashboard shows a near-live view of:

- Authentication Requests
- Authentication Request By Type
- Users By Authentication Type
- Users By Device

Multi-Factor Authentication dashboards reflect the information across the AD forest or per domain over the selected period. All dashboard reports can be downloaded to SVG or CSV formats.

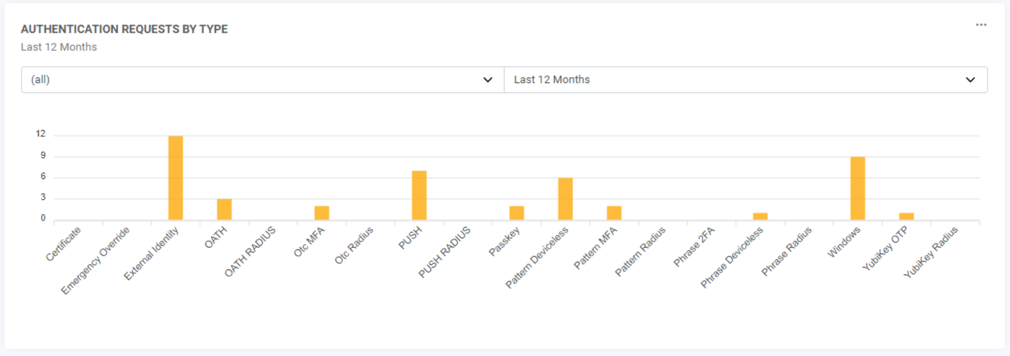
Authentication Requests module shows all valid and invalid MFA authentication requests over the selected period.



AUTHENTICATION REQUESTS
Last 7 Days

(all)
Last 7 Days

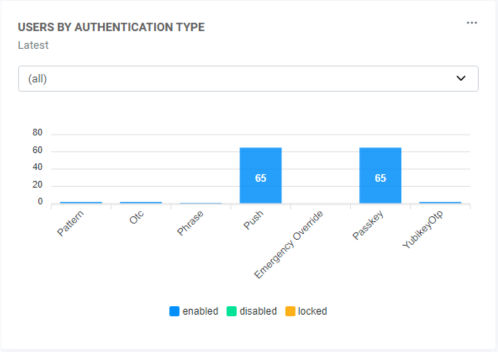
Authentication Requests By Type module shows the breakdown of successful authentication requests broken down by MyID MFA authentication type.



AUTHENTICATION REQUESTS BY TYPE
Last 12 Months

(all)
Last 12 Months

Users By Authentication Type module lists the total of users who have been provisioned to an MyID MFA authentication type.

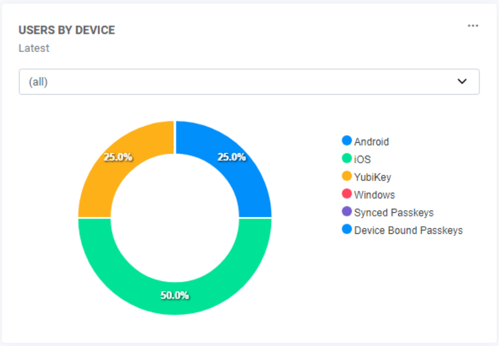


USERS BY AUTHENTICATION TYPE

Latest

(all)

Users By Device module lists the percentage of the device type which has been provisioned to users.



USERS BY DEVICE

Latest

(all)

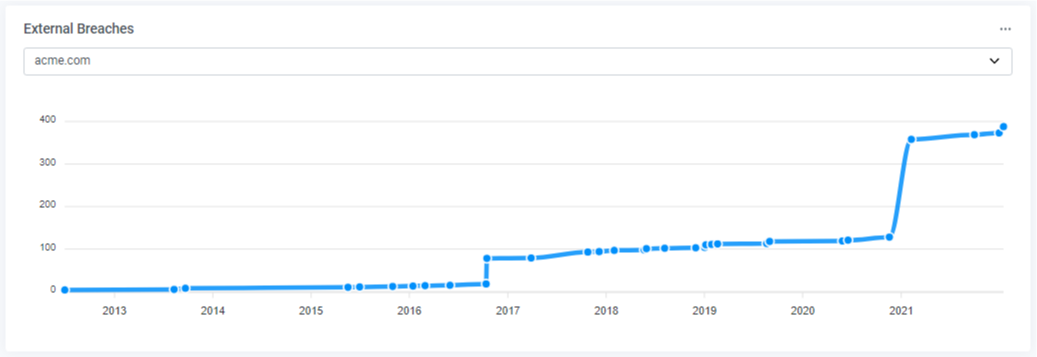
Password Security

The Password Security Dashboard shows a near-live view of:

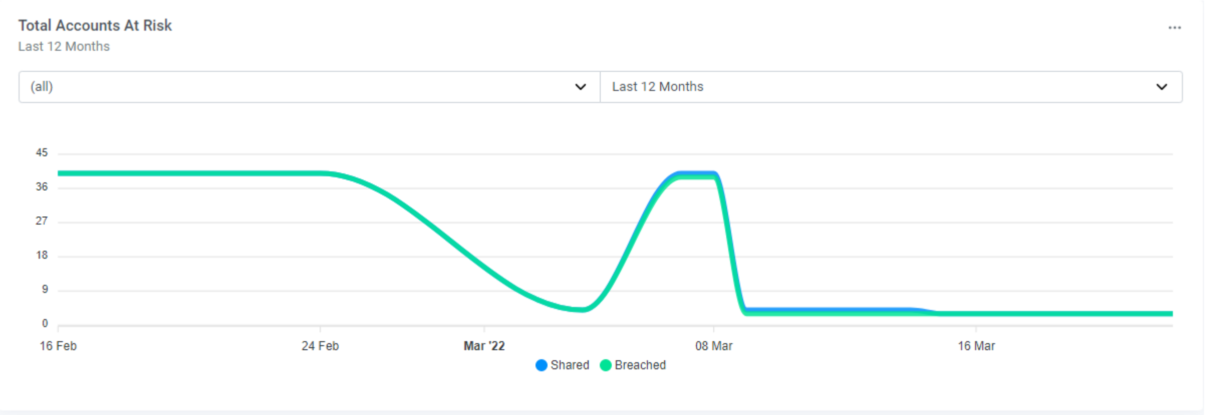
- External Breaches
- Total Accounts at Risk
- Failed Password Changes
- Users Accounts at Risk

Password Security dashboards reflect the information across the AD forest or per domain over the selected period. All dashboard results can be downloaded to SVG or CSV formats.

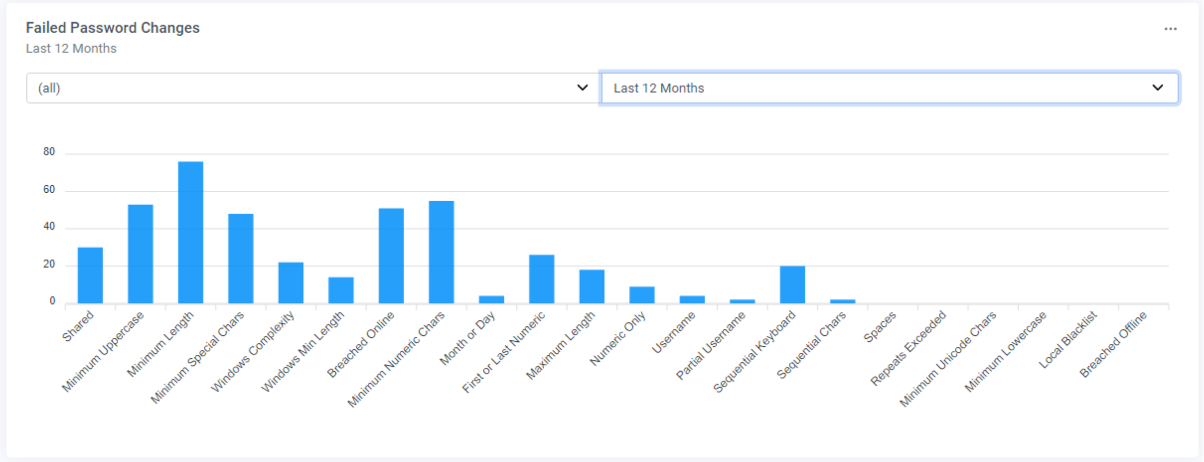
External Breaches module shows the breaches for the organisation as per the MyID Password Breach database.



Total Accounts At Risk Breaches module shows the number of accounts using breached or shared passwords as detected over the specified period.



Failed Password Changes module shows the failed password changes and the reason for the password rejection over the selected time period.

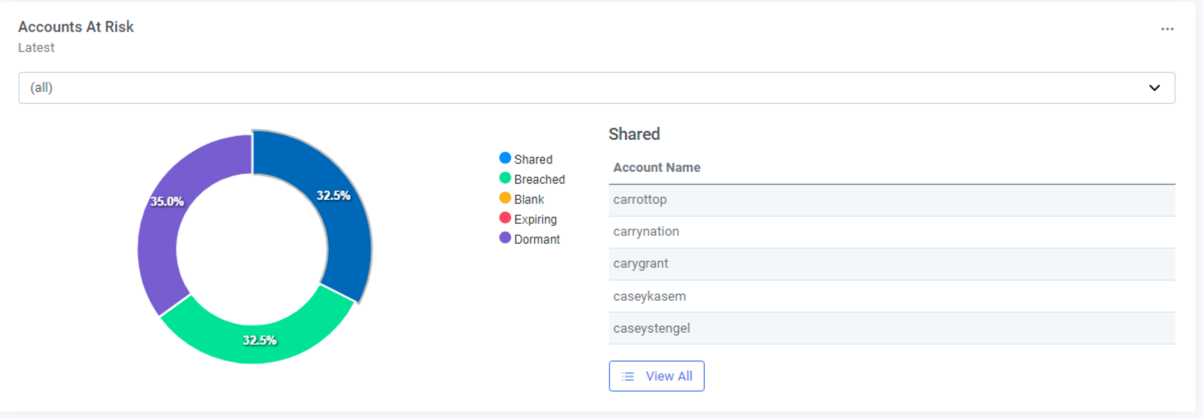


Failed Password Changes
Last 12 Months

(all)

Last 12 Months

Accounts at Risk module shows all the accounts which have passwords that are shared, breached, blank or soon to expire. This dashboard also shows dormant accounts.



Accounts At Risk
Latest

(all)

Shared

Account Name
carrottop
carrynation
carygrant
caseykasem
caseystengel

By selecting View All, all the accounts that fall under the highlighted category will be displayed.

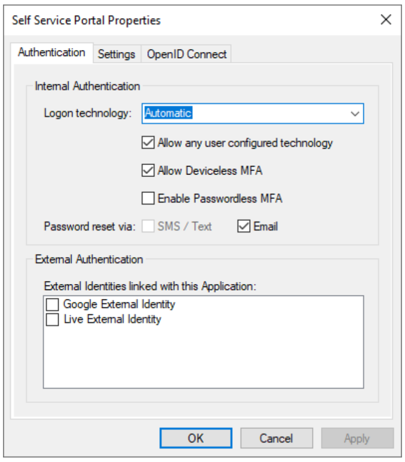
Web Portal customization

Authentication setting (Windows vs. Forms)

The Self Service Portal (SSP) and Web Management Portal (WMP) support both Windows Authentication and Forms bases Authentication.

A logon page can be displayed to require strong authentication via MyID supported MFA technologies or Password. The logon page can be set to use a specific technology only or set to auto to cater for all MFA technologies at once. In addition, the user's Active Directory password can be required on the logon page.

To change the Self Service Portal or Web Management Portal authentication type, on the Self Service Portal or Web Management Portal Applications settings- Authentication tab, select the required *Logon technology* from the dropdown list.



Self Service Portal Properties

Internal Authentication

Logon technology: Automatic

☑ Allow any user configured technology

☑ Allow Deviceless MFA

□ Enable Passwordless MFA

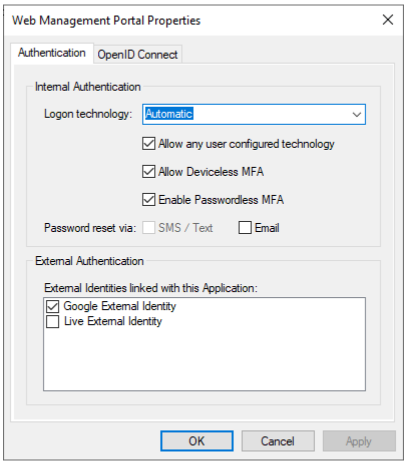
Password reset via: □ SMS / Text ☑ Email

External Authentication

External Identities linked with this Application:

□ Google External Identity

□ Live External Identity



Web Management Portal Properties

Internal Authentication

Logon technology: Automatic

☑ Allow any user configured technology

☑ Allow Deviceless MFA

☑ Enable Passwordless MFA

Password reset via: □ SMS / Text □ Email

External Authentication

External Identities linked with this Application:

☑ Google External Identity

□ Live External Identity

Using Deviceless OTP with Forms authentication

MyID Grid Pattern and Phrase questions can be displayed on the Forms Based Authentication login page to cater for Deviceless OTP authentication. If Deviceless OTP authentication is not required then the logon challenge can be disabled on the logon page. The authentication method is controlled via the *Allow Deviceless MFA* checkbox for each portal.

SSP Logon Page Customisation

The branding look of the Self Service Portal logon page can be easily customised by editing settings in the web.config file located at:

```
C:\Program Files\Authlogics Authentication Server\wwwroot\web.config
```

Item	Value	Detail
`Title`	`Self Service Portal`	Any custom text
`DisplayText`	`Self Service Portal`	Any custom text

LogoPath	/assets/img/logo-colour-transparent.png	A full or relative path to a graphic file such as a company logo.
UserGuideUrl	https://authlogics.com/download/authlogics-self-service-portal-user-guide-v5	A full or relative path to a downloadable user guide document.
PasswordLabelText	Password	Any custom text to help the user know which password is required, e.g. *Coprnet Password*

Note

Editing other values in the web.config file is not supported.

WMP Logon Page Customisation

The branding look of the Web Management Portal logon page can be easily customised by editing settings in the web.config file located at:

```
C:\Program Files\Authlogics Authentication Server\wwwroot\Admin\web.config
```

Item	Value	Detail
Title	MyID Self Service Portal	Any custom text
PasswordLableText	Password	Any custom text to help the user know which password is required, e.g. *Coprnet Password*

Note

Editing other values in the web.config file is not supported.

Advanced UI Customisation

Advanced customisation of the Self Service Portal is possible via CSS and JavaScript. The portal has two built-in customisation files where all customisations can be placed.

```
C:\Program Files\Authlogics Authentication Server\Web\SSP\wwwroot\css\custom.css
C:\Program Files\Authlogics Authentication Server\Web\SSP\wwwroot\js\custom.js
```

Some customisation of the Web Management Portal is possible via CSS. The portal has a built-in customisation file where customisations can be placed.

```
C:\Program Files\Authlogics Authentication Server\Web\Admin\wwwroot\css\custom.css
```

The web pages within the portal load the custom CSS and JS files automatically. The files are loaded last in the load order to allow custom code to override code in built-in functions if required.

Editing of any other files in the portal folder structure is NOT SUPPORTED. The custom files may be replaced by future updates/upgrades and existing customisations may not be compatible with future product versions. Intercede is unable to provide product support for any 3rd party code placed in the custom.css or custom.js files and any additions to the files are done so at your own risk.

Note

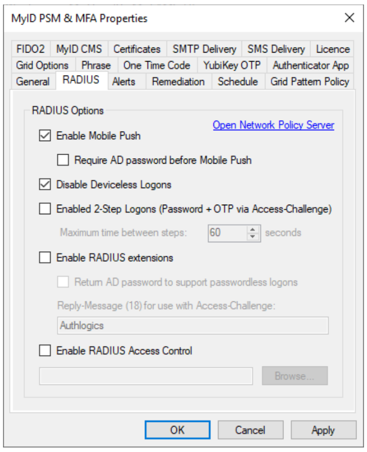
While the installer will attempt to retain your custom files, always keep a backup of your custom files to ensure they are not lost after an upgrade.

RADIUS Communication

MyID Authentication Server leverages the Windows Network Policy Server role to provide RADIUS connectivity. This is a high performance and robust RADIUS server which allows you to configure a flexible RADIUS policy; including RADIUS proxy capabilities which can simplify migrations from other token solutions.

The MyID RADIUS server only supports PAP authentication from RADIUS client devices.

RADIUS configuration is performed via the MyID MMC as well as the Microsoft Network Policy Server MMC.



RADIUS Options

☑ Enable Mobile Push

□ Require AD password before Mobile Push

☑ Disable Deviceless Logons

□ Enabled 2-Step Logons (Password + OTP via Access-Challenge)

Maximum time between steps: 60 seconds

□ Enable RADIUS extensions

□ Return AD password to support passwordless logons

Reply-Message (18) for use with Access-Challenge: Authlogics

□ Enable RADIUS Access Control

Mobile Push MFA

Mobile Push MFA via RADIUS can be enabled/disabled independently to other mechanisms if required.

When a RADIUS request is received containing only a user name the Authentication Server will trigger a Mobile Push to the users device, only if the user is configured for Mobile Push. It may be required that a username and password is required before a Mobile Push notification is triggered, in which case enable “Require AD password before Mobile Push”.

2-Step Logons (Access-Challenge)

RADIUS Access-Challenge is supported by some RADIUS clients. It allows for a 2-step logon process whereby the client will first send the username and password to the server for verification. The server will respond with either an Access-Challenge or Access-Reject. If the client supports Access-Challenge it will prompt the user for a 2nd set of credentials, e.g. an OTP and send it to the server. The server will then process the username and OTP and respond with an Access-Accept (only if an Access-Challenge preceded the request) or Access-Reject.

RADIUS Extensions

RADIUS extensions can be enabled to send metadata from the server back to the RADIUS client. This can also includes returning:

- The user's AD password to support single sign-on to certain applications such as Citrix Access Gateway.
- Custom reply text when using Access-Challenge for the RADIUS client to display (where supported by the RADIUS client).

RADIUS Server ports and protocols

The MyID RADIUS server uses the IANA assigned ports for authentication and accounting, as well as the unofficial ports for backward compatibility with legacy RADIUS clients.

- Authentication: UDP:1812 & UDP:1645
- Accounting: UDP:1812 & UDP:1645

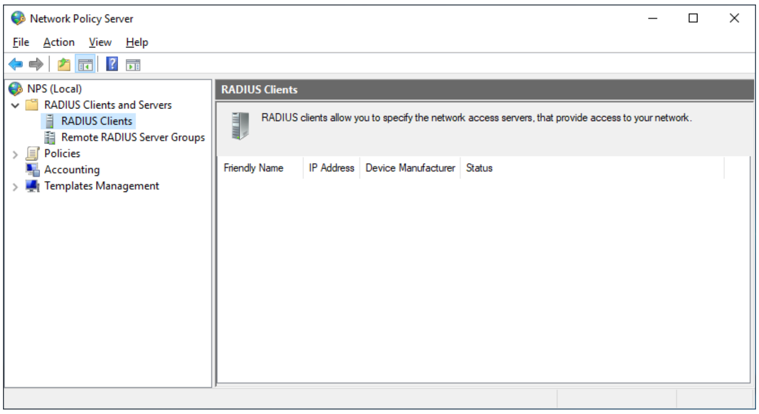
Both IPv4 and IPv6 are supported for communication with RADIUS clients.

Adding a RADIUS client

A RADIUS client device would typically be a VPN concentrator or remote access server, however, it could also be a wireless access point or a door access system. RADIUS is a common system used by a multitude of applications and platforms.

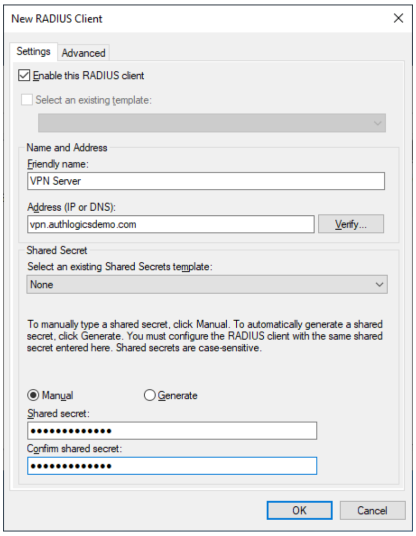
> **Note**
>
> This section of the installation process requires Local Administrator rights on the server. Domain rights are not required at this stage.

1. Open the *Network Policy Server* from the Administrative Tools start menu group.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

2. Select RADIUS Clients and Servers, then RADIUS Clients.
3. Right-click *RADIUS Clients* and select *New*.



New RADIUS Client

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: VPN Server

Address (IP or DNS): vpn.authlogicsdemo.com

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

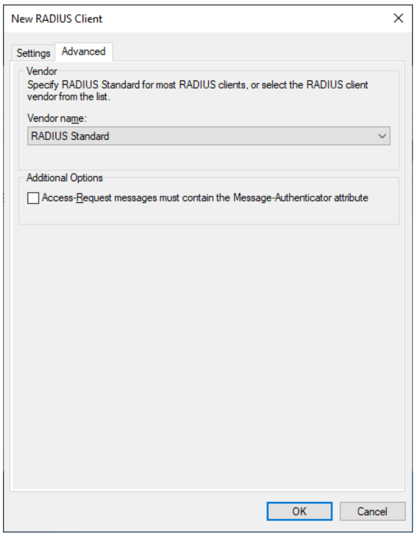
Shared secret: ••••••••••••••

Confirm shared secret: ••••••••••••••

4. On the *Settings* tab, enter values for:

   - “Friendly name” of the remote RADIUS client;
   - Address (IP address or DNS) of the RADIUS client. Use the Verify option to ensure that entered IP Address or DNS name is valid;
   - Enter and Confirm your Shared Secret. Ensure that the shared secret matches the secret entered on the RADIUS client device. You can also use the *Generate* option to generate a highly secure random secret.

   Ensure that the *Enable this RADIUS client* checkbox is ticked.



New RADIUS Client

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

5. Select the *Advanced* tab.

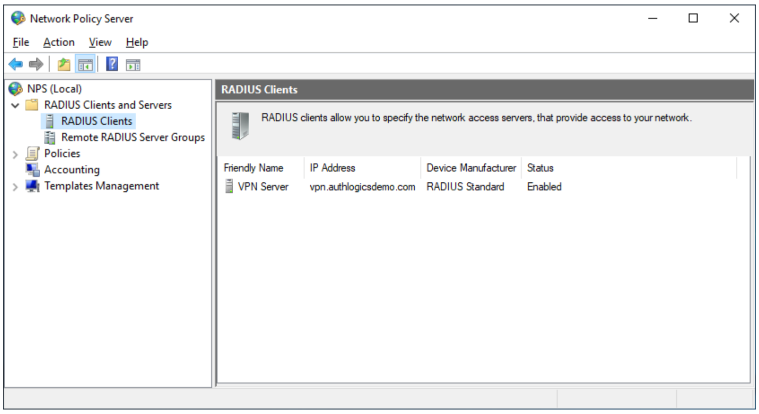
Ensure that the:

- Vendor name is set to *RADIUS Standard*.
- The *Access-Request messages must contain the Message-Authenticator attribute* is optional but must be set the same as on the RADIUS client device.

Note

Ensure that the Message-Authenticator attribute status is set to the same value on the RADIUS client devices as on the RADIUS server. They can either both be enabled or both disabled.

6. Click OK.



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	Status
VPN Server	vpn.authlogicsdemo.com	RADIUS Standard	Enabled

You may add as many RADIUS clients as required.

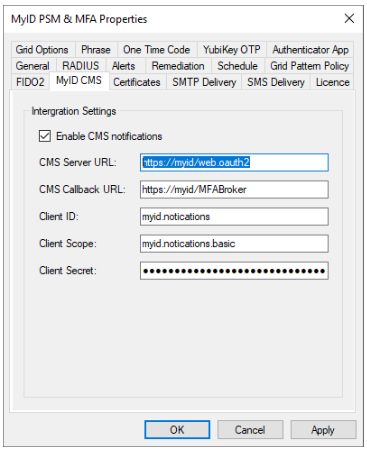
RADIUS Policies

The MyID Authentication Server installation automatically configures a Connection Request Policy within NPS which allows MyID to support configured RADIUS clients automatically. A Network Policy is not required as the MyID NPS plug-in will function without one.

If you need to modify the default Connection Request Policy it is recommended that you duplicate (Right-click, Duplicate Policy) the default policy as a backup and then disable it. Once complete you can modify the duplicated policy as needed.

Configuring MyID CMS Settings

Configuring the MyID CMS settings in the MyID Authentication Server is done via the MyID CMS tab in Global Settings.



Intergration Settings

☑ Enable CMS notifications

CMS Server URL: https://myid/web.oauth2

CMS Callback URL: https://myid/MFABroker

Client ID: myid.notications

Client Scope: myid.notications.basic

Client Secret: ••••••••••••••••••••••••••••••

The following information is required to complete the configuration:

- The MyID CMS OAuth2 Authentication Service URL
  - e.g. “https://myid/web.oauth2”
- The MyID CMS MFA Broker Service URL
  - e.g. “https://myid/MFABroker”.
- The MyID CMS Client ID used to authenticate
  - e.g. “myid.notifications”
- The MyID CMS Client Scope use to authenticate
  - e.g. “myid.notifications.basic”
- The MyID CMS Client Secret used to authenticate
  - e.g. “4116e8f9-92e2-48b1-8616-5fb3d130b91d”

Configuring the PSM Password Policy

Deploying the MyID PSM Password Policy involves the following step:

1. Create a MyID PSM Password Policy in Active Directory Group Policy
2. Deploy the Domain Controller Agent
3. Group Policy changes:
    - Assign the MyID Password Policy to the Domain Controllers OU
    - Assign the MyID Password Policy to the Authlogics Authentication Servers group
    - Modify the built-in *Default Domain Policy*

> **Note**
> Installing the MyID Domain Controller Agent does NOT modify the existing Windows password policy for the Domain.

Configuring the MyID Password Policy Settings

The MyID Authentication Server includes an AD Group Policy Template files `AuthlogicsPasswordPolicy.admx` and `AuthlogicsPasswordPolicy.adml` which are used to create policies. The *User Configuration* section of the GPO can be disabled as the settings only apply to the *Computer Configuration*.

The PSM Users role

The PSM Users role is disabled by default. To enable it you must assign an AD group to the role. See the *Managing the Password Security Management Users Role* section of this guide for more information.

If the PSM Users role is not enabled then all AD users will have the MyID Password Policy applied to them. If enabled, only members of this group will have the MyID Password Policy applied to them and non-members will have the “Exception Password Policy” applied to them which mirrors the equivalent default Windows password policy settings.

Main settings

These settings control the overall password policy behaviour.

Setting	Enable Authlogics Password Policy
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting enables the MyID Password Policy functionality on all Agents and Servers where this Group Policy is applied. If you enable this policy complexity and validity checks will be performed on the passwords. If you disable or do not configure this policy then no password processing will function as per the configured policy thus deeming all passwords as acceptable.	

Primary Password Policy

These settings control the MyID specific password policy. The default settings will work well in most scenarios and are NIST 800-63B compliant by default.

Setting	Disable Online Password Breach Database checking
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting prevents querying the MyID Password Breach Database in the Cloud consisting of billions of known previously breached passwords. If you enable this policy then no checks against the MyID Password Breach Database in the Cloud will be performed. If you disable or do not configure this policy a partial HASH of the password will be sent over SSL to Intercede for analysis. The password will be rejected if it is a known/previously breached password to comply with to comply with NIST SP 800-63B.	

Setting	Disable Offline Password Breach Database checking
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting prevents querying the offline MyID Password Breach Database installed on the MyID Authentication Server. If you enable this policy then no checks against the offline MyID Password Breach Database will be performed. If you disable or do not configure this policy passwords will checked against the offline database and will be rejected if it is found in order to comp with NIST SP 800-63B.	

Setting	Disable Custom Password Blacklist checking
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting prevents querying the custom Password Blacklist consisting of passwords entered by an administrator. If you enable this policy then no checks against the custom Blacklist file will be performed. If you disable or do not configure this policy then entered passwords will be compared with the contents of the custom blacklist file and is also be available for use by the heuristics engine. The password will be rejected if it is found on the custom blacklist to comply with NIST SP 800-63B.	

Setting	Disable Shared Password Protection
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting prevents checking if the password is already in use by another user account in the Domain. If you enable this policy then no checks against the Domain for shared passwords will be performed. If you disable or do not configure this policy the Domain will be checked and the password will be rejected if it is currently in use.	

Setting	Enable Passphrases
Values	(6 - 30)
Default	12
Description	
This policy setting enables the use of passphrases if a password is longer than the specified value. Passphrases not have to pass the following complexity checks if they are long enough: • Minimum Lowercase Characters • Minimum Uppercase Characters • Minimum Numeric Characters • Minimum Special Characters • Minimum Unicode Characters • Maximum Repeating Characters • Maximum Allowed Characters From Username If you enable this policy then the specified complexity checks will be skipped only if the password length is equal to or longer than the specified value. If you disable or do not configure this policy then users may find it difficult to set a passphrase as all configured complexity checks must pass.	

Setting	Override Password Policy for new User Accounts
Values	(1 - 30)
Default	5
Description	
This policy setting overrides password the password policy checks for accounts that have been created within a specified time period and will be accepted. If you enable this policy, specify the number of seconds from when an account has been created for it to be deemed as being a new account. If you disable or do not configure this policy then the password policy will apply to passwords specified during the Active Directory account creation process.	

Setting	Disable Heuristic Scanning
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting controls the heuristic scanning engine behaviour on password checks. Heuristic scanning will undergo a series of checks where known character replacements are detected and reverted to their original base value and then revalidated for compliance. For example, '@' reverts to 'a', '!' to 'i' etc. If you enable this policy the heuristic scanning engine will not be active for any checks. If you disable or do not configure this policy then heuristic scanning will be performed to comply with NIST SP 800-63B against the Offline Password Breach Database, Custom Password Blacklist, all or part of the username, and Month and Day names.	

Setting	Enable Cloud Heuristic Scanning
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting controls the heuristic scanning engine behaviour on passwords with the MyID Password Breach Database in the Cloud. Heuristic scanning will undergo a series of checks where known character replacements are detected and the various derivatives will the evaluated to see if they have been breached. For example, '@' reverts to 'a', '!' to 'i' etc. If you enable this policy the heuristic scanning will be used when checking the MyID Password Breach Database. Warning: By enabling this policy the full password HASH will be sent over the Internet to MyID as k-Anonymity cannot be used. If you disable or do not configure this policy then heuristic scanning will not be performed with the MyID Password Breach Database and k-Anonymity will still be used.	

Complexity Rules

These settings provide fine grain control of password complexity settings. Too many of these settings should not be used together otherwise it will make it too difficult for a user to choose a password and it may encourage them to write passwords down.

Setting	Disallow Incremental / Numeric-Only changes
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting prevents changing only a single digit, or appending a single digit compared to the existing password. If you enable this policy then users must change more than just a single digit compared to their old password. If you disable or do not configure this policy then entered passwords with a simple numeric change from the previous password will be allowed. Note: This check requires that the PSM Wizard has been run and enabled on the domain.	

Setting	Disallow First or Last Character being a number
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disallows passwords that start or end with a numeric character. If you enable this policy then users cannot use a password that begins or ends with a number. If you disable or do not configure this policy then passwords which start or end with a numeric character will be allowed.	

Setting	Disallow Month and Day names
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disallows the use of month and day names in the password. If you enable this policy a password will be rejected if a month or day name is found in an entered password. If you disable or do not configure this policy then the check will not be performed.	

Setting	Disallow spaces
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting disallows the use of a space character in a password. If you enable this policy a password will be rejected if a space is found in an entered password. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Password Length
Values	(4 - 127)
Default	8
Description	
This policy setting sets the minimum number of characters allowed for a compliant password. Setting this value too high may make the password too difficult for users to remember password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the length of the password is less than the value specified. Note: Consecutive space characters will be counted as a single space character as per NIST SP 800-63B guidance. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 8 will be used to comply with NIST SP 800-63B.	

Setting	Maximum Password Length
Values	(4 - 127)
Default	127
Description	
This policy setting sets the maximum number of characters allowed for a compliant password. Setting this value too low may stop users from selecting passphrases which are typically more secure than passwords. The password will be rejected if the length of the password is more than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 127 will be used to comply with NIST SP 800-63B.	

Setting	Minimum Lowercase Characters
Values	(1 - 127)
Default	2
Description	
This policy setting sets the minimum number of allowed lowercase characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of lowercase letters in the password is less than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Uppercase Characters
Values	(1 - 127)
Default	2
Description	
This policy setting sets the minimum number of allowed uppercase characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of uppercase letters in the password is less than the value specified. If you enable this policy then you must specify a value.	

If you disable or do not configure this policy then the check will not be performed.

Setting	Minimum Numeric Characters
Values	(1 - 127)
Default	2
Description	
This policy setting sets the minimum number of allowed numeric digits a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of numeric digits in the password is less than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Special Characters
Values	(1 - 127)
Default	2
Description	
This policy setting sets the minimum number of allowed special characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of special characters in the password is less than the value specified. The following are recognised as special characters ! " # % & ' ( ) * , - . / : ; ? @ [\ ] _ { }' If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Minimum Unicode Characters
Values	(1 - 127)
Default	2
Description	
This policy setting sets the minimum number of allowed Unicode characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of Unicode characters in the password is less than the value specified. Unicode characters are non-printable characters that are not punctuation or alphanumeric characters. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Maximum Repeating Characters
Values	(0 - 126)
Default	8
Description	
This policy setting sets the maximum number of times a character can be repeated anywhere within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if a character is repeated in the password more times than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed to comply with NIST SP 800-63B.	

Setting	Maximum Consecutive Repeating Characters
Values	(0 - 126)
Default	3
Description	
This policy setting sets the maximum number of times a character can be repeated anywhere within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if a character is repeated in the password more times than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed to comply with NIST SP 800-63B.	

Setting	Maximum Sequential Characters
Values	(0 - 127)
Default	3
Description	
This policy setting sets the maximum number of times a sequence of characters can be used within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of characters in a sequence is more than the value specified. Sequential characters are both forward and backwards i.e. ABC and CBA are deemed to be sequential. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed to comply with NIST SP 800-63B.	

Setting	Maximum Sequential Keyboard Characters
Values	(0 - 5)
Default	2
Description	
This policy setting sets the maximum sequential keyboard characters allowed within a compliant password. The password will be rejected if the number of keyboard layout characters in sequence is more than the value specified. Sequential characters are both forward and backwards i.e. "qwerty" and "ytrewq" with both be deemed to be sequential. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Maximum Allowed characters from User Account name
Values	(1 - 127)
Default	3
Description	
This policy setting sets the maximum number of characters from a user account name that are allowed in a password. Passwords will be rejected if the number of characters from the user account name in a password is more than this value specified. e.g. If the user account name is Robert and the value is 3 then passwords containing "robe", "ober" and "bert" will be rejected. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the check will not be performed.	

Setting	Allow Full User Account name in password
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting allows the use of the full user account name within the password. If you enable this policy a password will not be blocked if the full user account name is found within the entered password. If you disable or do not configure this policy then the password may not contain the full user account name to comply with NIST SP 800-63B.	

Dynamic Password Expiry

These settings dynamically control the maximum age of a password depending on its length. This allows for passwords to be used for longer the longer they are. This encourages users to create longer, and thus more secure passwords.

A password is matched to the highest zone possible depending on the length of the password. When MyID detects that a password has dynamically expired the user account will be configured to change password at next logon.

There are 5 password expiry zones with each consisting of a minimum password length and maximum password age in days. A 6th zone can be used to configure accounts to never expire if they are over the specified length.

Setting	Password Expiry Default Zone
Values	Maximum Age in days: (1 - 999)
Default	42
Description	
This policy setting configures the default password expiry period. If a password length is unknown or less than what is required by any other Zone then the Default Zone will apply. Note: If a password was created prior to installing MyID its length will be unknown and the Default Zone will apply. Once the password has been changed the length will be known and other Zones may then apply. If you enable this policy you must specify the Maximum Age in days until the user account's password will be set to expire. If you disable or do not configure this policy then the setting will not take effect.	

Setting	Password Expiry Zone 1
Values	Minimum Password Length: (6 - 100)
Default	8
Values	Maximum Age in days: (1 - 999)
Default	60
Description	
This policy setting configures the dynamic password expiry period for this zone. If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account’s password will be set to expire. If you disable or do not configure this policy then the zone setting will not take effect.	

Setting	Password Expiry Zone 2
Values	Minimum Password Length: (6 - 100)
Default	9
Values	Maximum Age in days: (1 - 999)
Default	90
Description	
This policy setting configures the dynamic password expiry period for this zone. If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire. If you disable or do not configure this policy then the zone setting will not take effect.	

Setting	Password Expiry Zone 3
Values	Minimum Password Length: (6 - 100)
Default	10
Values	Maximum Age in days: (1 - 999)
Default	180
Description	
This policy setting configures the dynamic password expiry period for this zone. If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire. If you disable or do not configure this policy then the zone setting will not take effect.	

Setting	Password Expiry Zone 4
Values	Minimum Password Length: (6 - 100)
Default	11
Values	Maximum Age in days: (1 - 999)
Default	270
Description	
This policy setting configures the dynamic password expiry period for this zone. If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire. If you disable or do not configure this policy then the zone setting will not take effect.	

Setting	Password Expiry Zone 5
Values	Minimum Password Length: (6 - 100)
Default	12
Values	Maximum Age in days: (1 - 999)
Default	365
Description	
This policy setting configures the dynamic password expiry period for this zone. If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire. If you disable or do not configure this policy then the zone setting will not take effect.	

Setting	Password Never Expires Zone
Values	Minimum Password Length: (6 - 100)
Default	20
Description	
This policy setting configures the dynamic password expiry period for this zone. If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect. If you disable or do not configure this policy then the zone setting will not take effect.	

Exception Password Policy

These settings control the exception settings to the Primary Password Policy. The default settings mirror the equivalent default Windows password policy settings.

These settings will only apply to the users who are not members of the **PSM Users** role if a group has been configured.

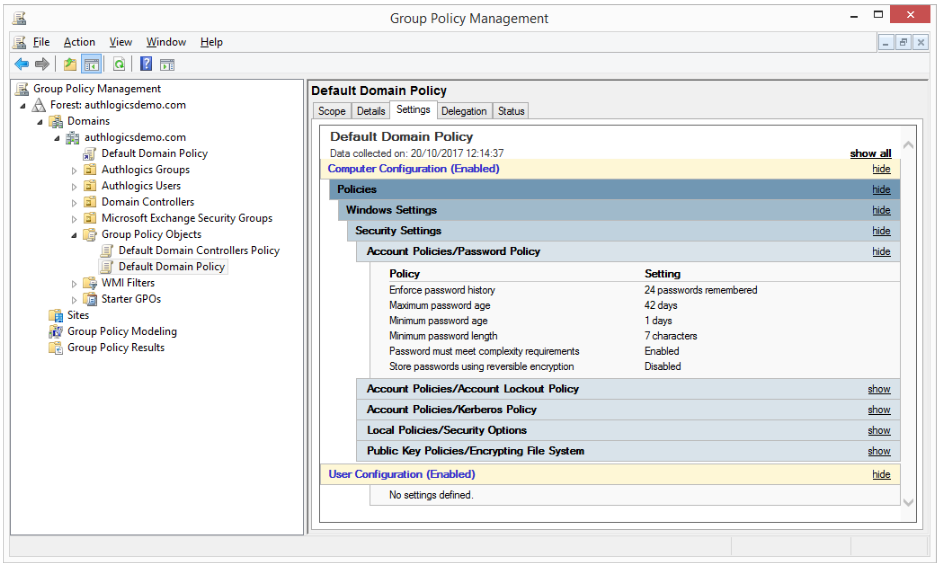
Setting	Maximum Password Age
Values	Maximum Age in days: (1 - 999)
Default	42
Description	
This policy setting configures the maximum password age for accounts that are NOT a member of the PSM Users Role. If you enable this policy you must specify the Maximum Age in days until the user account's password will be set to expire. If you disable or do not configure this policy then the setting will not take effect.	

Setting	Minimum Password Length
Values	(1 - 127)
Default	7
Description	
This policy setting sets the minimum number of characters allowed for a compliant password for accounts that are NOT a member of the PSM Users Role. Setting this value too high may make the password too difficult for users to remember password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the length of the password is less than the value specified. If you enable this policy then you must specify a value. If you disable or do not configure this policy then the default value of 7 will be used as per Windows password policy.	

Setting	Mirror Windows 'Password Complexity' requirements
Values	Enabled / Disabled
Default	Disabled
Description	
This policy setting mirrors the Windows built in 'Password must meet complexity requirements' restriction for accounts that are NOT a member of the PSM Users Role. This check ensures that a password does not contain the username, that it contains a minimum of 3 of the following character types: uppercase, lowercase, numeric, non-alphabetic/special characters. If you disable or do not configure this policy then the check will not be performed.	

Modifying the Default Domain Policy

The following password settings apply to the Default Domain Policy by default:



Default Domain Policy

Data collected on: 20/10/2017 12:14:37 show all

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy show

Account Policies/Kerberos Policy show

Local Policies/Security Options show

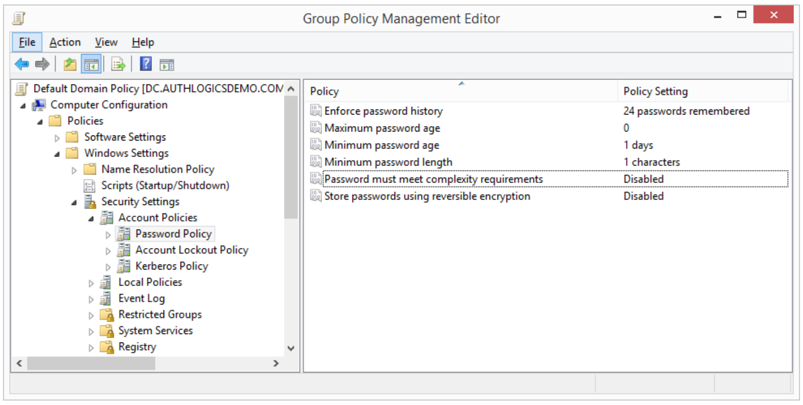
Public Key Policies/Encrypting File System show

User Configuration (Enabled) hide

No settings defined.

The following password settings for the Default Domain Policy must be changed so that the built-in Windows policy does not conflict with the MyID Password Policy and NIST guidance:

- **Maximum password age: 0**
  - This should be set to 0 when MyID PSM "Dynamic Password Complexity" is used or to comply with NIST SP 800-63 which states that passwords should not periodically expire.
- **Minimum password length: 1**
  - This should be set to 1 so that it does not conflict with MyID PSM "Minimum Password Length" complexity rule setting.
- **Passwords must meet complexity requirements: Disabled**
  - This should be set to Disabled to allow the MyID PSM policy to function or to comply with NIST SP 800-63B which states that passwords should not be forced to contain complexity rules.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	0
Minimum password age	1 days
Minimum password length	1 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Warning

DO NOT set these settings to *Not Configured* as this will not achieve the desired goal as Windows will revert to default settings.

Configuring Custom Password Blacklist checking

MyID PSM provides administrators with the ability to add their own unwanted passwords to a blacklist text file. The blacklist allows for the rejection password based on full passwords as well as those matching wildcard characters “*” and “**#**”. Furthermore, the heuristics engine will add further protection to the file by substituting ‘@’ to ‘a’, and ‘5’ to ‘s’ etc.

To enable the local Password Blacklist, modify the contents of the following text file:

```
C:\Program Files\Authlogics Authentication Server\blacklist.txt
```

Once a blacklist file has been updated it must be copied to all MyID Authentication Servers. The file is not required to be placed on Domain Controllers.

The custom blacklist can be disabled by emptying the contents of the file or by disabling the check via Group Policy.

Wildcard Usage within Local Blacklist

To enforce password rejection, full words and wildcards characters “*” and “**#**” can be added to the local blacklist file. If a password matches what is defined in the local blacklist file, the password will be rejected. How a password is processed is dependent on the positioning of the wildcard i.e. front, middle, back.

The wildcard “*” refers to any character for any length, if a “*” is entered on its own, all passwords will be rejected.

The wildcard “**#**” refers to a single numeric number and translates to 9 i.e. **##** = 99. Numeric numbers within passwords will be converted to a numeric and then, if less than the restricted value, the password will be rejected.

The following table shows examples of how MyID Authentication Server will process a password based on the blacklist entry:

Blacklist Entry	Description	Password	Result
Authlogics	Direct matches to a restricted word will be rejected	Authlogics	Rejected
		Authlogics01	Accepted
Auth*	Passwords starting with ***Auth*** will be rejected	Authlogics	Rejected
		HelloAuthlogics	Accepted
Auth	Passwords with ***Auth*** in the middle will be rejected	Authlogics01	Accepted
		heloAuth123	Rejected
*Auth	Passwords ending with ***Auth*** will be rejected	heloAuth123	Accepted
		Authlogics	Accepted
		helloAuth	Rejected
Authlogics##	Reject any Password starting with word ***Authlogics*** ending in 2 digits	Authlogics12	Rejected
		Authlogics12	Rejected
		Authlogics112	Accepted
		Hellowworld12	Accepted
##Authlogics	Reject any Password starting with 2 digits and ending with the word ***Authlogics***	12Authlogics	Rejected
		123Authlogics	Accepted
##*	Reject any password starting with 2 digits	12Authlogics	Rejected
		Authlogics12	Accepted
		1Authlogics	Accepted
		123Authlogics	Rejected
*##	Reject any password ending with 2 digits	12Authlogics	Accepted
		Authlogics12	Rejected
		Authlogics123	Accepted
##	Reject any password with 2 consecutive digits in the middle of the password.	12Authlogics	Accepted
		Authlogics12	Accepted
		Auth12logics	Rejected
		Authlogics123logics	Accepted

Advanced Configuration

Advanced configuration options for MyID are controlled via the Windows registry. The following entries are created during the installation of MyID server components and typically most of them should only be changed if instructed by an Intercede support engineer.

> **Note**
> After changing a registry key on the MyID Server the IIS components must be restarted by running `IISRESET` from an elevated admin command prompt.

Specifying Active Directory Domain Controllers

The MyID Authentication Server will automatically locate domain controllers as needed. In environments where network segmentation exists not all DC's may be contactable by the MyID Authentication Server. This can cause connectivity problems and logon delays.

In these environments, you can specify which Domain Controllers (DCs) and Global Catalog Servers (GCs) should be used via registry keys. There are two keys which can be configured and each can contain one or many server names (FQDN recommended) separated by commas.

```
HKLM\SOFTWARE\Authlogics\Authentication Server\DomainGCs
```

Default Value: `{blank}`

Used by components: MyID Authentication Server; Management Console

The MyID Authentication Server will use attempt to connect to each specified GC and then remain connected to the server that responds to LDAP queries the quickest.

```
HKLM\SOFTWARE\Authlogics\Authentication Server\DomainDCs
```

Default Value: `{blank}`

Used by components: MyID Authentication Server; Management Console

The MyID Authentication Server will use attempt to connect to each specified DC and then remain connected to the server that responds to LDAP queries the quickest. The MyID Authentication Server will initially find the names of all the Domains in the Forest, and the DC's in each Domain by querying the Global Catalog. It will then map the results against the DC list in the registry to calculate which server to use for each Domain. If a Domain does not have a DC specified then one will be selected automatically.

Adding a trusted SSL certificate for secure connections

To replace the self-signed SSL certificate on the MyID server with an alternative from a trusted root authority.

1. The Common Name (CN or SAN) in the certificate must match the DNS value use by MyID agents or make use of a wide card certificate.
2. The certificate must be trusted by all systems that connect directly to the MyID server.
3. Using Internet Information Services (IIS) Manager, edit the HTTPS IIS bindings for the MyID web site and select the new SSL certificate.

Active Directory Timing

```
HKLM\SOFTWARE\Authlogics\Authentication Server\DomainAccessTimeout
```

Default Value: `60`

Accepted Values:

```
0 = Disabled, indefinite timeout
1 to 120 = Timeout in seconds
```

The time taken in seconds before a connection to a Domain Controller times out.

```
HKLM\SOFTWARE\Authlogics\Authentication Server\DomainControllerRefeshTime
```

Default Value: `15`

Accepted Values:

```
1 to 9999 = Timeout in minutes
```

The time taken in minutes before a new search is done to locate the quickest GC and DC.

Diagnostics Logging

```
HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingEnabled
```

Default Value: `0`

Accepted Values:

```
0 = Disabled
1 = Enabled
```

Notes: When this value is enabled various log files will be created in the logging folder. These logs may be requested by an Intercede support engineer.

```
HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingFolder
```

Default Value: `C:\Program Files\Authlogics Authentication Server\Log`

Notes: This Value may be changed to an alternative valid local folder with the same NTFS permissions as the default folder.

Other settings

Changing other registry values is NOT supported unless instructed by Intercede Support.

Integration with external systems

Intercede provide integration guides for various external systems which may include step-by-step instructions or custom integration components.

The MyID Authentication Server Developers Guide should be used when planning to programmatically access the MyID Authentication Server for automation, scripting or app integration. Extensive provisioning and workflow integration can be achieved by utilising the Web Services APIs to create, delete, enable, disable accounts etc.

Integrating MyID Authentication Server with any other external or 3rd party systems can be done using Web Services or RADIUS, or a combination of the two.

If you are using Multi-Factor Authentication with an SSL VPN no logon screen customisation is required as a logon challenge will not be displayed on a login screen. In this scenario either a soft token, hardware token or a SMS/TEXT token must be used and the SSL VPN can use RADIUS to validate login requests.

If you are using deviceless authentication with an SSL VPN you will need to modify the login page of the SSL VPN to display a challenge. The SSL VPN can simply request the image from the MyID server using the GetToken.ashx web service with little coding effort. The SSL VPN can still use RADIUS to validate login requests but may alternatively use Web Services if supported by the SSL VPN vendor.