Installation and Configuration Guide

Multi-Factor Authentication and Password Security Management

Product Version: 4.2.1040.0

Publication date: May 2023

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

Email us: sales@authlogics.com

Table of Contents

Introduction

Authlogics 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:
  - PINgrid - Pattern Based Authentication
  - PINphrase - Random Character Authentication
  - PINpass - OATH (TOTP) Compliant Authentication
  - YubiKey – Yubico YubiKey hardware token support

Considerations

System Requirements

The supported operating systems for Authlogics Authentication Server are:

- Windows Server 2022 *
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

> **Note: Windows Server 2022 Update Requirement**
> The Authlogics 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: 4.8

The hardware requirements for Authlogics 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 Authlogics 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 Authlogics.

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

Password Breach Databases

Authlogics has 3 versions of its Password Breach Database:

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

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

(3) Cloud Password Breach Database
- An Internet hosted database containing over 5 billion breached credentials.
- Regularly updated.

The Authlogics 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 Authlogics Cloud Password Breach Database will also be checked.

A full Offline Password Breach Database containing over 5 billion breached passwords is available as a separate addon download from https://authlogics.com/downloads/. When the full database is installed it may be possible to disable Cloud Password Breach Database lookups.

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

High Availability

Authlogics 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 Authlogics data.

To ensure high availability of the Authlogics 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 Authlogics 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 (WSAPI) please see the Authlogics Authentication Server Developers Guide.

Language Requirements

Authlogics 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, Authlogics specific text is in English only.

Internet Connectivity

The Authlogics 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 Authlogics 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 Authlogics Cloud Password Breach Database lookups are enabled, the Authlogics 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 Authlogics 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 Authlogics 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 Authlogics 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

Authlogics solutions are licensed on a per-user basis with each user requiring a licence. A licence must be installed onto each instance of an Authlogics Directory. Contact licencing@authlogics.com for any licencing enquires.

To install an Authlogics licence simply run the Licence Configuration Wizard within the Authlogics Authentication Server Management Console.

Licence functionality

The functionality available in the Authlogics 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

Authlogics 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

Authlogics 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

Authlogics 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 Authlogics 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 Authlogics Authentication Server including SMS/Text message, email, offline OTP (pattern or OATH), Mobile Push, biometrics and YubiKey hardware tokens.

Authlogics Authentication Server has been designed to integrate with a multitude of remote access solutions and applications. The core of Authlogics is the Authentication Server which provides a Web API and a RADIUS interface. Authlogics also provides agents for various 3rd party systems to allow for direct integration, e.g. Windows Desktop, Active Directory Federation Services, Exchange Server etc.

Any remote access concentrator or application that can interact with Web Services (SOAP, HTTP Get or HTTP Post) 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.

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

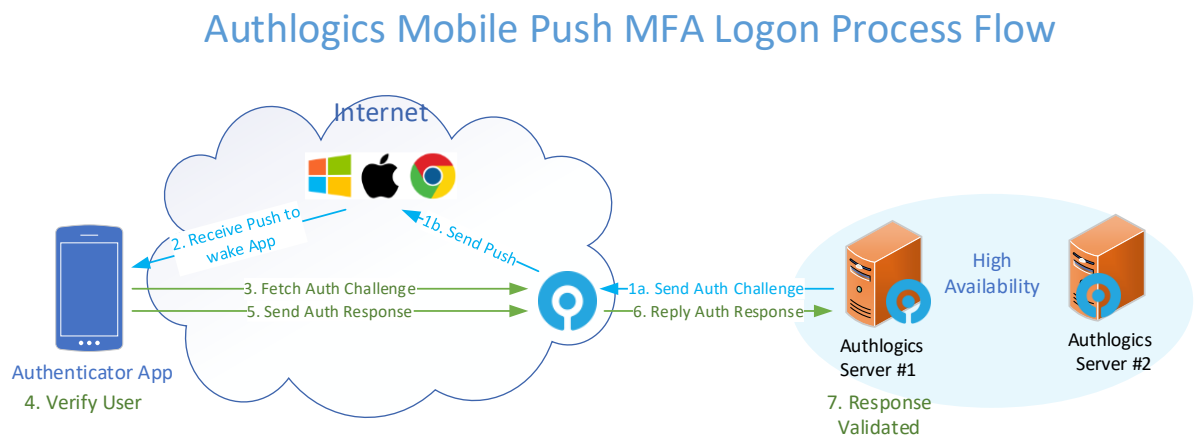
For high-availability deployment scenarios with numerous users, user information can be stored across multiple domains in an Active Directory forest. Multiple Authlogics servers can be deployed within an Active Directory forest for multiple points of presence, or in the same location with built-in Network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

Mobile Push Authentication

Overview

Authlogics 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.



Public Push Networks

App notifications via Microsoft, Apple & Google Public Push Networks can be unreliable and they are not a guaranteed delivery service. Authlogics 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 Logon.

Passwordless for Windows

The Authlogics 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 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 Authlogics Server Password Vault

The Authlogics 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.

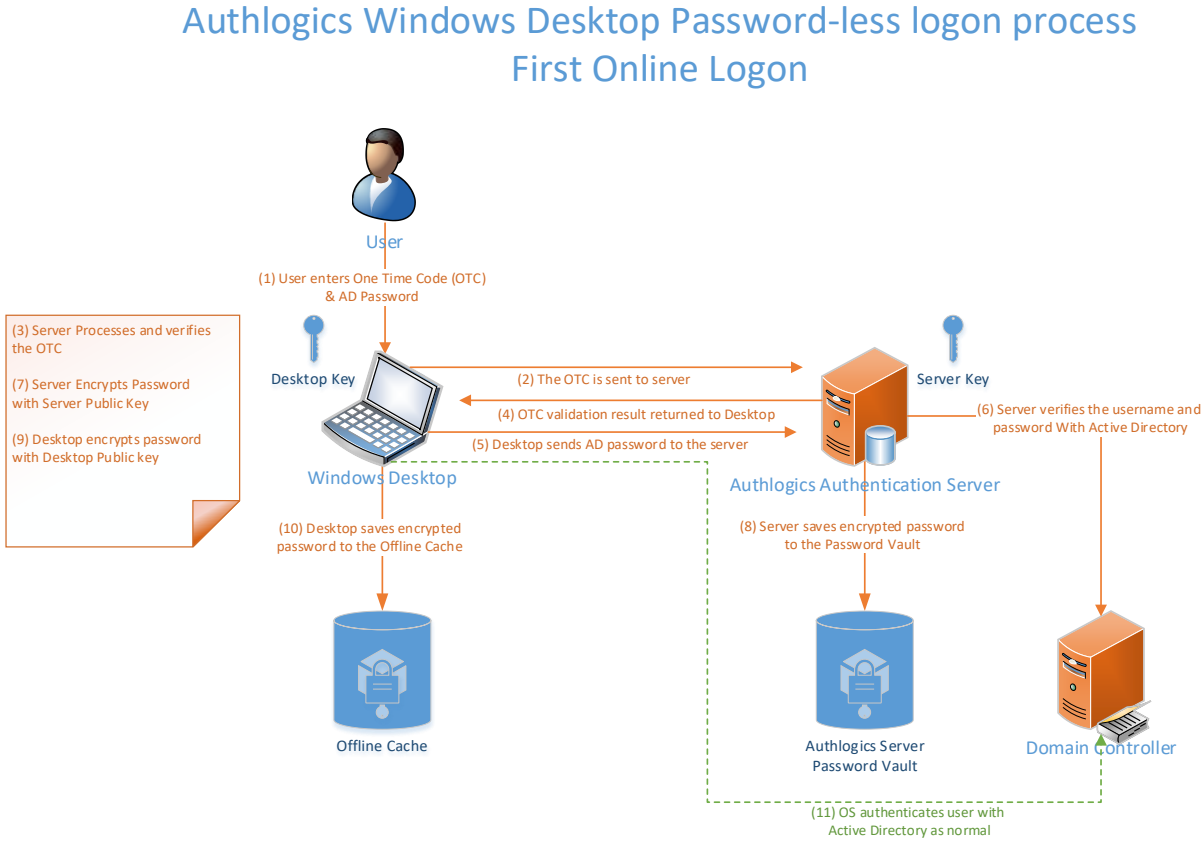
During the Authentication Server installation, a unique certificate is generated with an RSA 2048bit key pair which is used to encrypt the password data. This certificate can be replaced at any time by running the Certificate Configuration Wizard on the server which will re-encrypt the data with the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

The Windows Desktop Agent

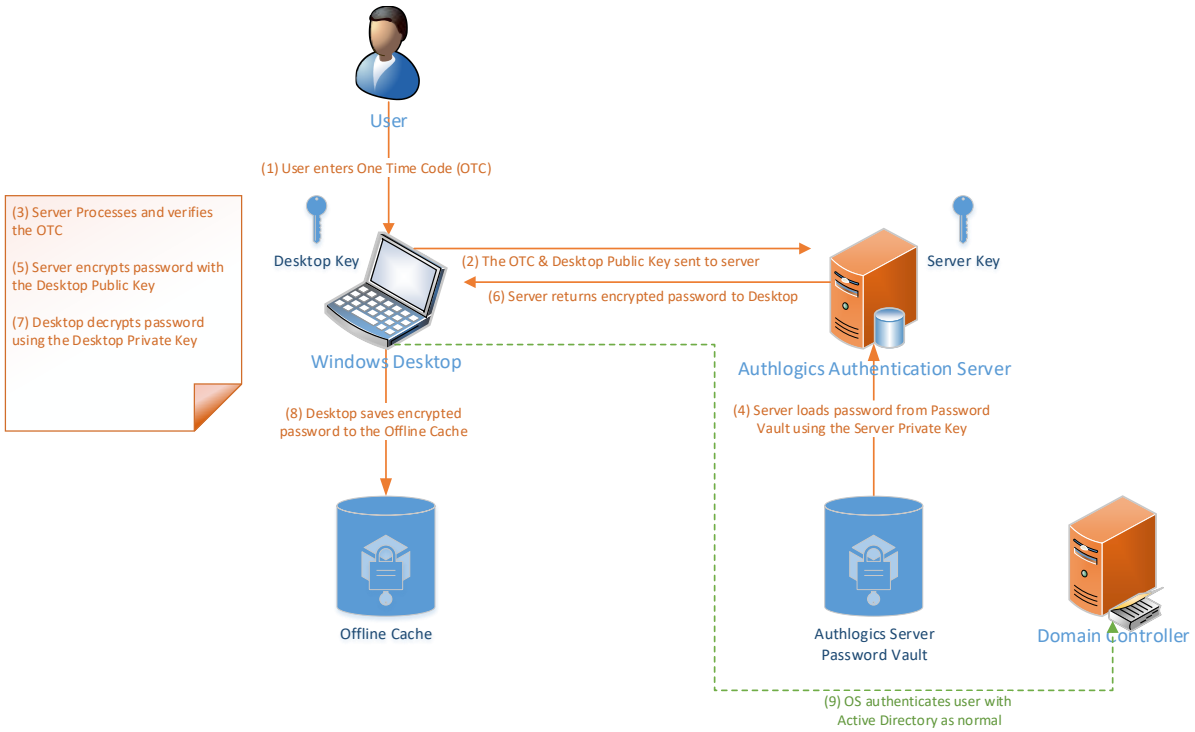
The Windows Desktop Agent is designed run on a Windows desktop/server machine to provide Multi-Factor Authentication security and Passwordless logons. The agent is fully managed and deployable via Active Directory group policy for easy and granular administration.

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

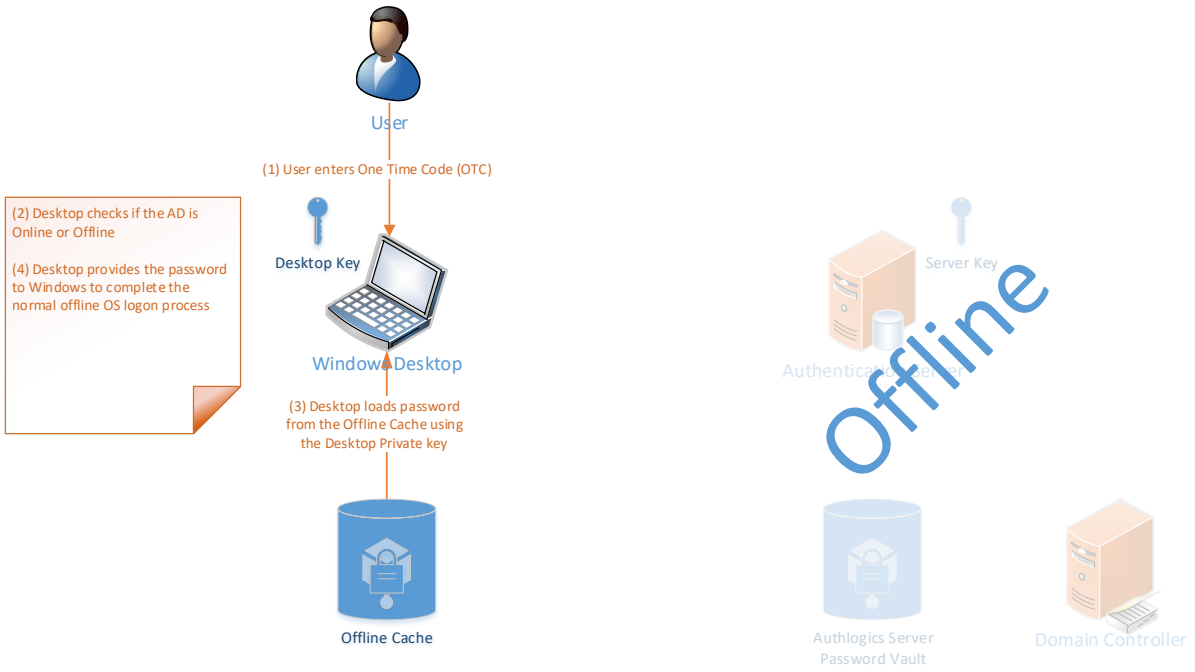
See the Authlogics Windows Desktop Agent Integration Guide for further information.



Authlogics Windows Desktop Password-less logon process
Regular Online Logon

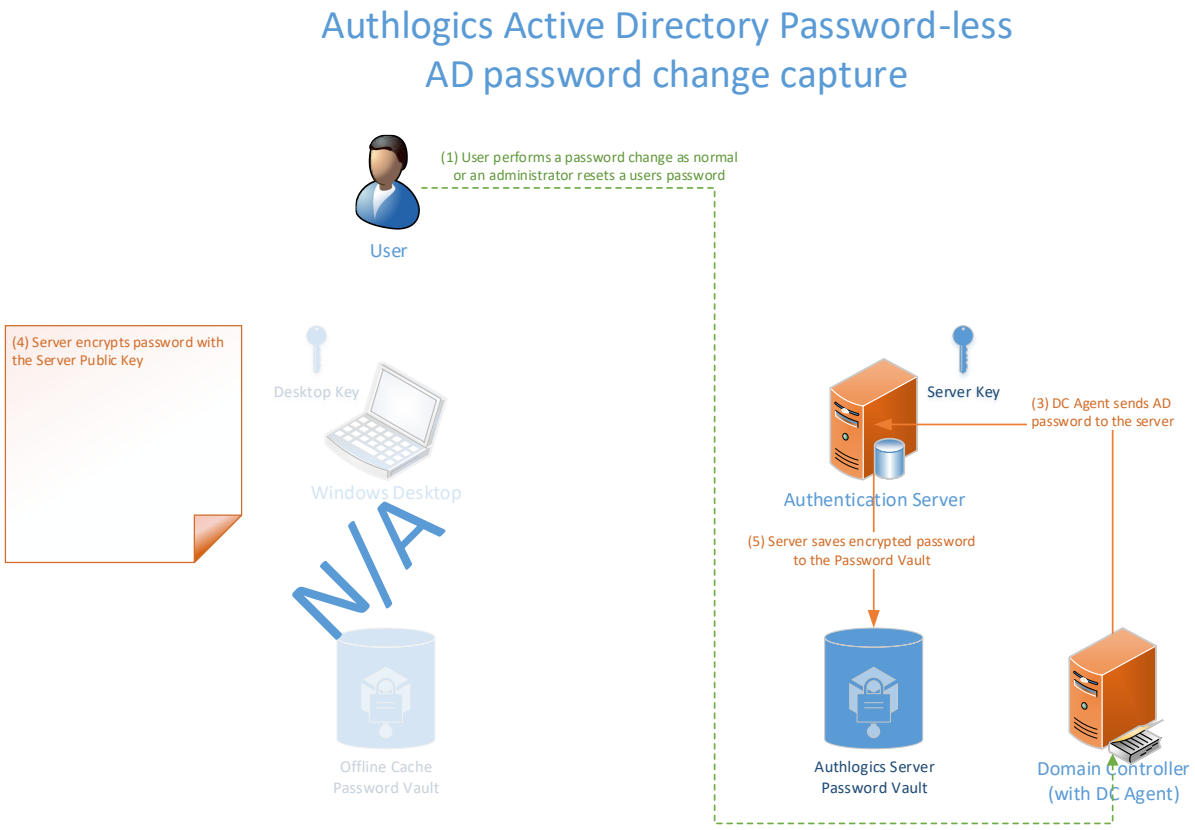


Authlogics Windows Desktop Password-less logon process
Regular Offline logon



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 Authlogics Server Password Vault. This ensures that all new passwords comply with the latest NIST SP 800-63 guidance and it keeps the AD password database and the Authlogics 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.



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 Authlogics 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…
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.

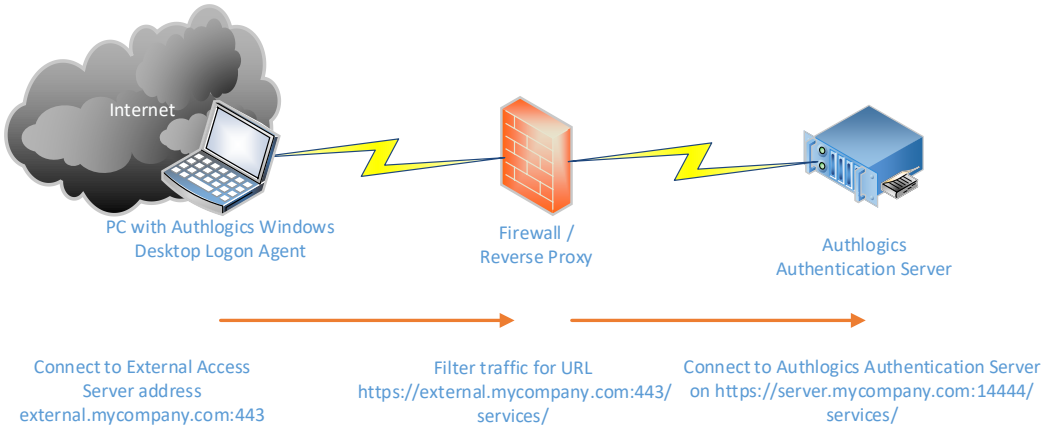
For information regarding granular application of rights within AD please contact support@authlogics.com

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

External Access Server role for Windows Desktop Agent

The External Access Server role is an optional component on the Authlogics Authentication Server which runs on a dedicated port and IIS web site. It is designed to be Internet facing to provide connectivity to the Windows Desktop Agent without exposing access to the Self Service Portal and main Web API. The role is installed during the server installation and can be configured to use a different SSL certificate to the Self Service Portal if required.

It is recommended to use a reverse proxy server or SSL capable firewall to allow Internet access to the External Access URL of the Authlogics Authentication Server.



Note

Authlogics Desktop Agents older than version 4.1.3200.0 are unable to use the dedicated External Access Server role and must be configured to connect to the main Web API. It is recommended to upgrade the Desktop Agents to 4.1.3200.0 or higher and utilise the External Access Server role.

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 2012 or higher OS on which to install Authlogics Authentication Server. *Recommended: Windows Server 2019*	
3	Internet Connectivity (HTTPS) from Authlogics 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 Authlogics Authentication Servers. *Recommended: Use the policy defaults where possible.*	
9	Plan which MFA technology to provision users for. *Recommended: PINgrid 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 Authlogics 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 Microsoft ADFS with the Authlogics ADFS Agent.*	

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.

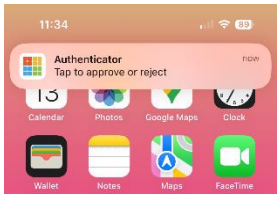
The increase of security provided by multi-factor (typically 2-factor) is that users must now "have something" and "know something" in the authentication process. The "have something" usually takes the form of a physical hardware device, like a key fob, which generates a specific unique One Time Pin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

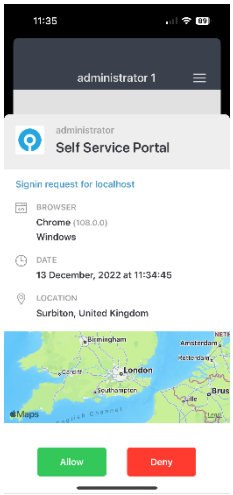
Although these hardware token devices have improved security significantly, they do have certain limitations and incur a costing overhead in both their implementation as well as on-going maintenance. Furthermore, they typically still need to be used together with a password and don't provide a path towards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

Authlogics 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

Authlogics 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.





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 Authlogics 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".

Authlogics 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.

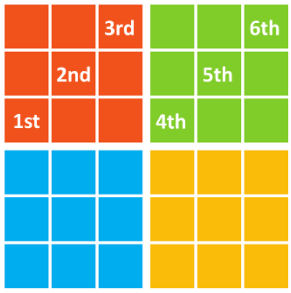
PINgrid Technology

PINgrid technology 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 PINgrid is that the user also needs to know a unique pattern to extrapolate an OTP.

To thwart automated brute force attacks, Authlogics 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. PINgrid even mitigates the threat of keylogging, screen scraping and shoulder surfing attacks.

PINgrid 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?



User pattern

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, PINgrid 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.

PINphrase Technology

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.

PINphrase 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 PINphrase ideal for both a deviceless and Multi-Factor Authentication. PINphrase 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 PINphrase 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:

```
PINphrase: 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 Authlogics PINphrase 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, PINphrase 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.

PINpass Technology (including YubiKey)

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

PINpass 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, PINpass can be used offline via the Authlogics Authenticator in the App Store.

If hardware tokens are required, PINpass works with YubiKey tokens from Yubico. YubiKey's 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 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 PINpass 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.

Authentication Technology vs Factor type

Technology	Knowledge	Possession	Inherent
Password (NIST)	X		
PINgrid	X	X	
PINphrase	X	X	
PINpass	X	X	
Mobile App		X	X
YubiKey		X	

Deployment

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

Overview

To fully deploy the Authlogics Authentication Server:

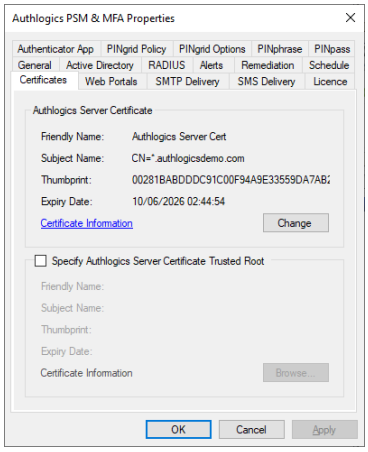
(1) Install the Authentication Server on a Windows Server.
(2) Provision users in the Authlogics Directory.
(3) Install Plug-ins, configure 3rd party integrations or setup RADIUS clients. Authlogics plug-ins have separate Integration guides which should be followed.
(4) Optional: Deploy additional Authentication Servers for High Availability.

High Availability and Certificates

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

Prior to installing an additional Authlogics Authentication Server, the Authlogics Server Certificate must be exported from the primary Authlogics 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 check the certificates tab in the Authlogics Management Console:



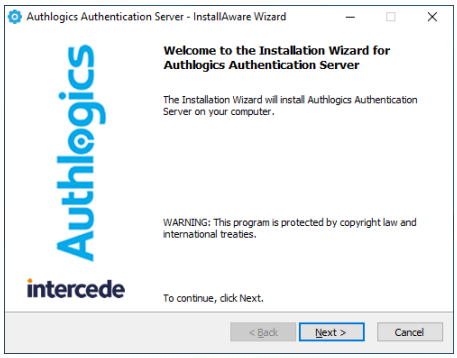
Follow the Certificate Export and Import section later in this guide for setup by step details.

Installing Authlogics Authentication Server

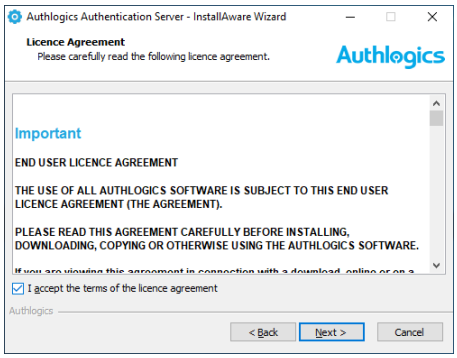
The Authlogics Authentication Server is responsible for processing logon requests and other core activities. This Authlogics Authentication Server should be set up before any other component.

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

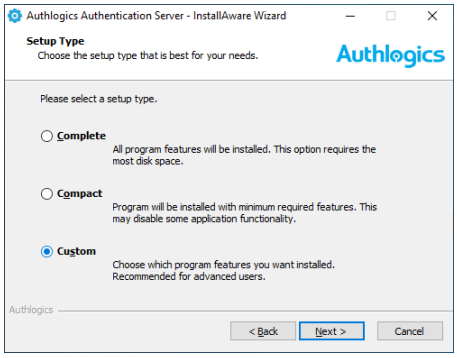
1. To start the Authlogics Authentication Server installation, run the *Authlogics Authentication Server xxxxx.exe* installer. Click *Next* to automatically uninstall the previous version.



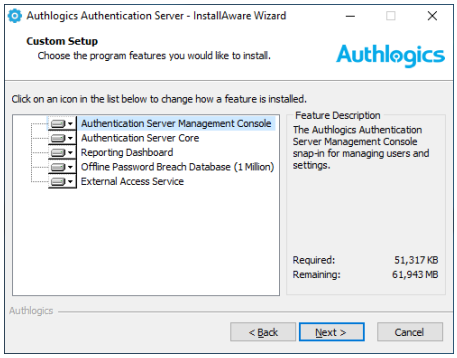
2. Click *Next* to continue.



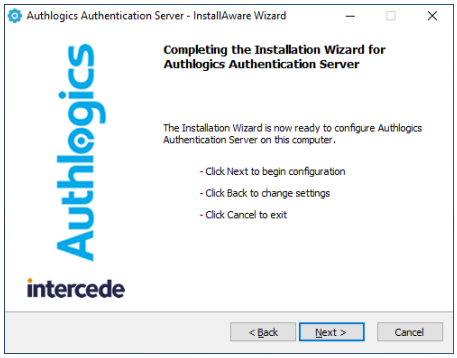
3. After **reading** the licence agreement click *I accept the terms in the terms in the Licence Agreement* if you agree to the terms, then click *Next* to continue.



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

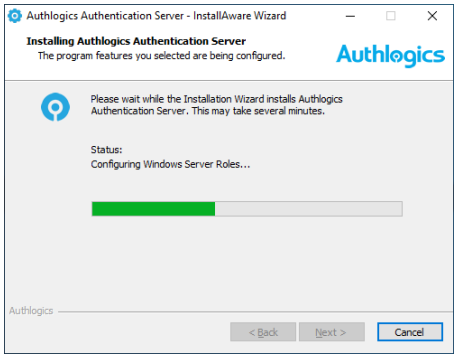


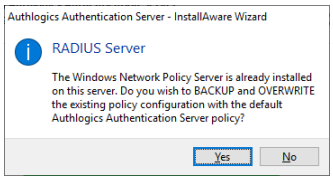
5. As a minimum ensure to select the *Authentication Server core* and the *Authentication Server Management Console* features for installation. Click *Next* to continue.



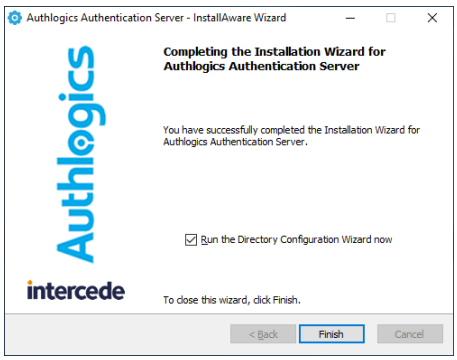
6. Click *Next* to continue.

The installation is being performed.





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

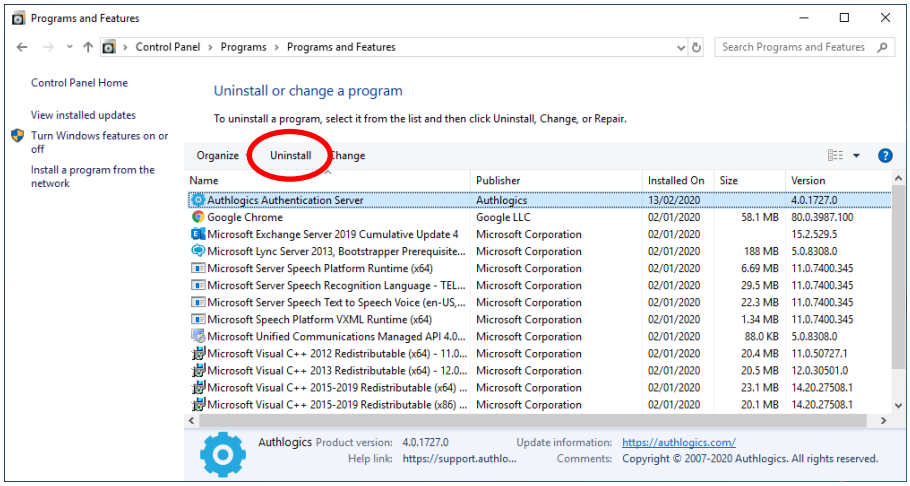


8. All necessary Authlogics Authentication Server files have been installed on your server. Select *Run the Directory Configuration Wizard now* if you wish to set up the directory immediately.

   Click *Finish* to complete the installation process.

Uninstalling Authlogics Authentication Server

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



Active Directory metadata

Uninstalling Authlogics does NOT remove the metadata from user accounts in the Active Directory. If you are planning to completely remove Authlogics 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 Authlogics information from it.

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

Installing a new version of Authlogics 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.

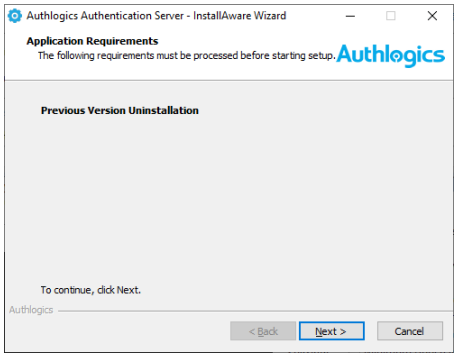
A product Upgrade is a major new version which will include fixes but is mainly designed to deliver new features and functionality. Upgrades are not released regularly. Upgrades may require additional planning before they are installed. Always review the Installation and Configuration Guide of the new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

Installing an Update

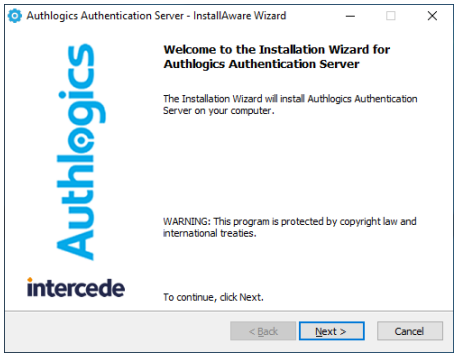
The installation program of an Update can be used for a full clean install, or to perform an in-place update of an existing installation.

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. All directory settings, registry settings and supported web portal customisations are retained during an update.

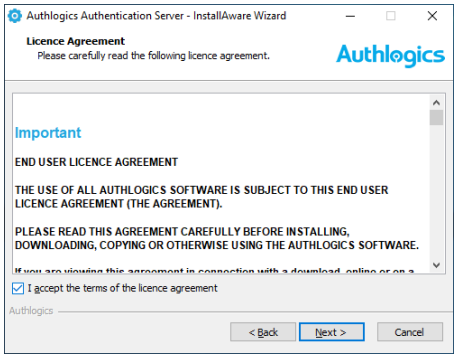
1. To start the Authlogics Authentication Server installation, run the *Authlogics Authentication Server xxxxx.exe* installer.



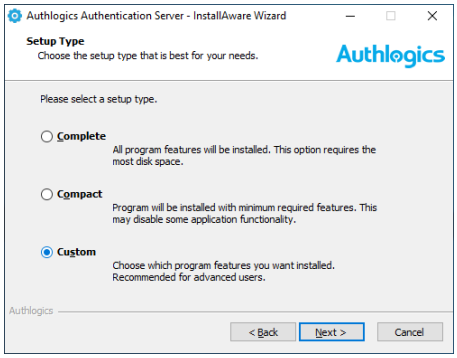
2. Click *Next* to automatically uninstall the previous version.



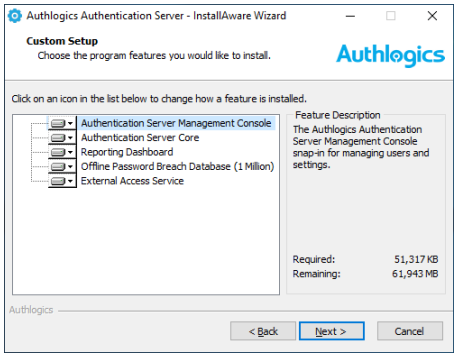
3. Click *Next* to continue.



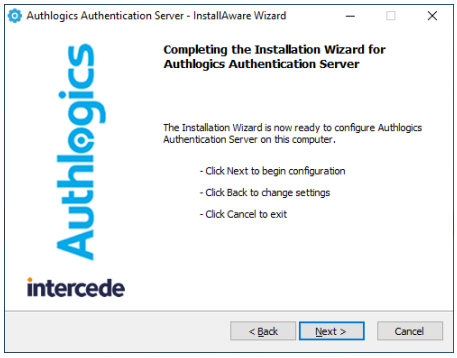
4. After **reading** the licence agreement click *I accept the terms in the terms in the Licence Agreement* if you agree to the terms, then click *Next* to continue.



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

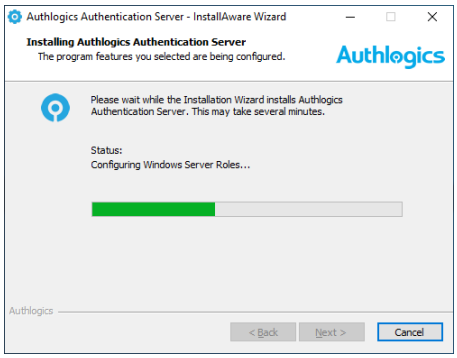


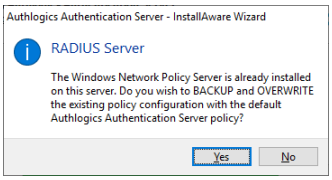
6. As a minimum ensure to select the *Authentication Server core* and the *Authentication Server Management Console* features for installation. Click *Next* to continue.



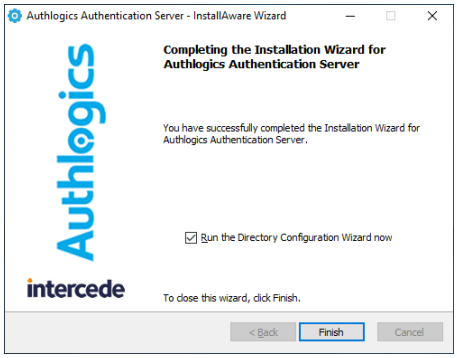
7. Click *Next* to continue.

The installation is being performed.





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



9. All necessary Authlogics 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 3.x

Authlogics Authentication Server 4.2 supports upgrading from version 4.0 and higher. To upgrade from 3.x you must first upgrade to 4.1, and then to 4.2, there is no direct upgrade path.

> **Important – Desktop Logon Agent**
>
> If the Authlogics Desktop Logon Agent version 3.x is deployed the **Authlogics Desktop Agent MUST be upgraded to version 4.2 before the Authlogics Authentication Server is upgraded**. The Authlogics Desktop Agent 4.2 is backwards compatible with version 3.0 and higher servers. See the Authlogics Windows Desktop Agent Integration Guide for further details.

Upgrading from Version 4.x

Authlogics Authentication Server 4.2 supports upgrading from version 4.0 and higher.

> **Important – Desktop Logon Agent**
>
> If the Authlogics Desktop Logon Agent version 4.x is deployed the **Authlogics Desktop Agent MUST be upgraded to version 4.2 before the Authlogics Authentication Server is upgraded**. The Authlogics Desktop Agent 4.2 is backwards compatible with version 4.0 and higher servers. See the Authlogics Windows Desktop Agent Integration Guide for further details.

Process overview:

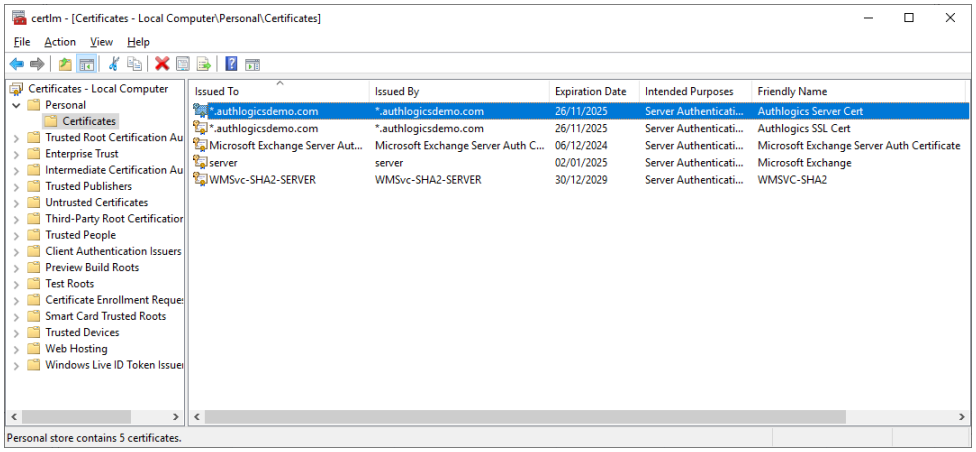
(1) If multiple Authlogics Authentication Servers running 4.0/4.1 are deployed then all but one server must be uninstalled. If all servers are already running a previous 4.2 release then a simple in place upgrade can be performed on each server.
(2) On the last remaining Authlogics Authentication Server run the setup for version 4.2 to in-place upgrade the server. This will automatically remove version 4.0/4.1.
(3) Complete the Directory Configuration Wizard to upgrade the version 4.0/4.1 user metadata.
(4) Review the Authlogics Authentication Server settings, noting new features which may be required.
(5) Test user logons and general functionality post upgrade.
(6) Deploy additional Authlogics Authentication Servers if needed.
    a. Review the *Certificate Export and Import* section of this document prior to installing additional Authlogics Authentication Servers.

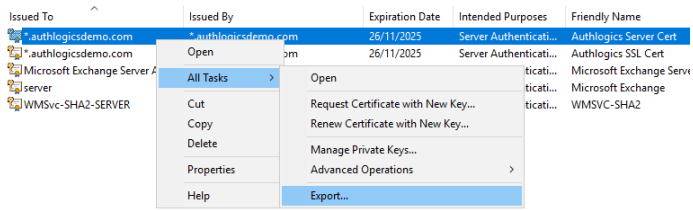
Certificate Export and Import

This section details the process of exporting the Authlogics Authentication Server directory encryption certificate to a file so it can be imported onto another server where the Authlogics Authentication Server software will be installed.

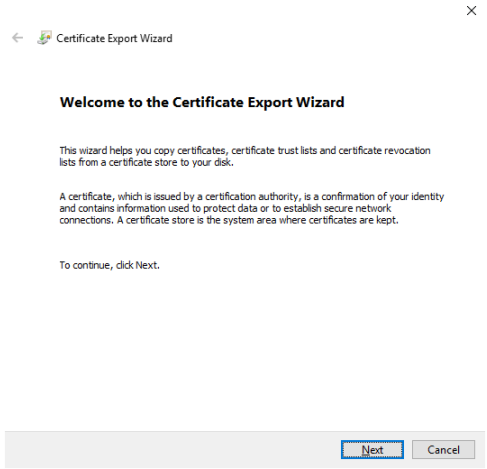
Export Certificate from existing Authlogics Authentication Server

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

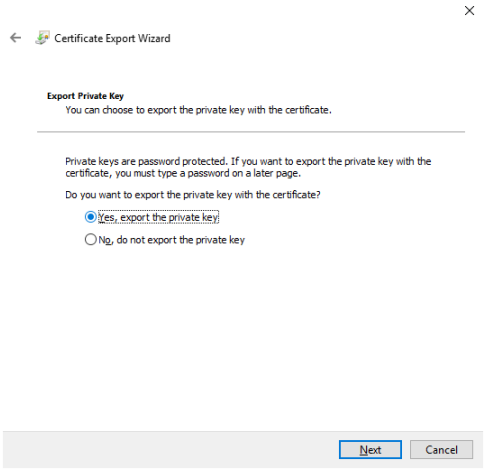




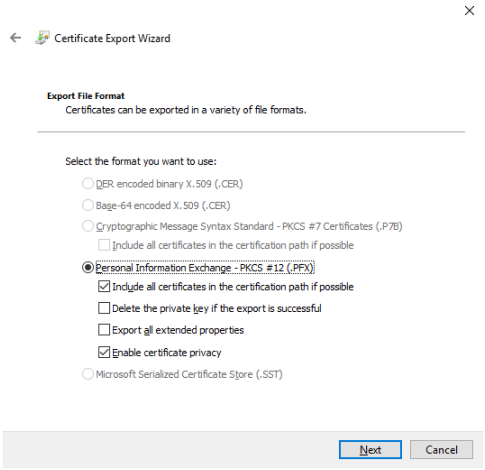
2. Right-click the Authlogics Server Certificate being used, select *All Tasks*, *Export*…



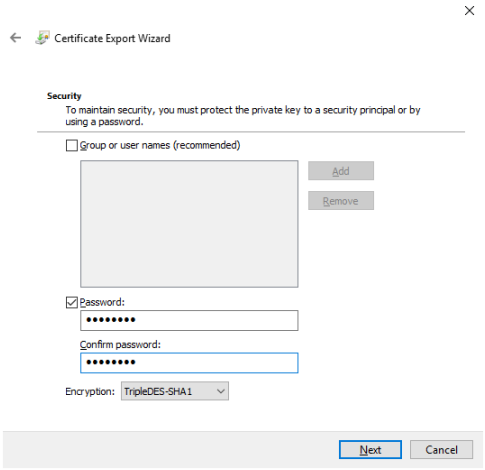
3. Click *Next* to continue.



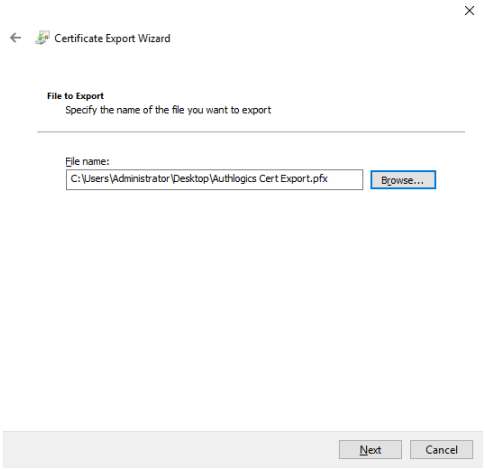
4. Select *Yes, export the private key* and click *Next* to continue.



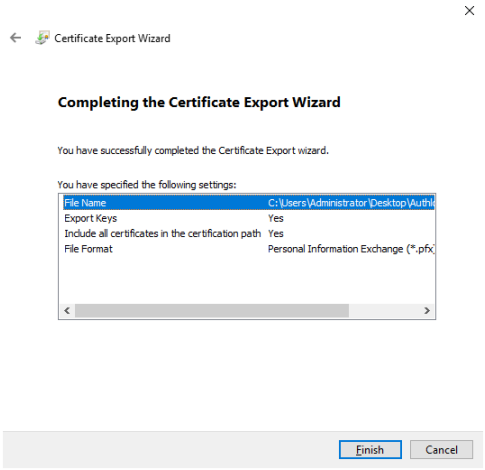
5. Click *Next* to continue.



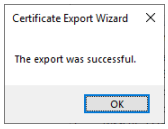
6. Select *Password* and enter a password twice to confirm. Click *Next* to continue.



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



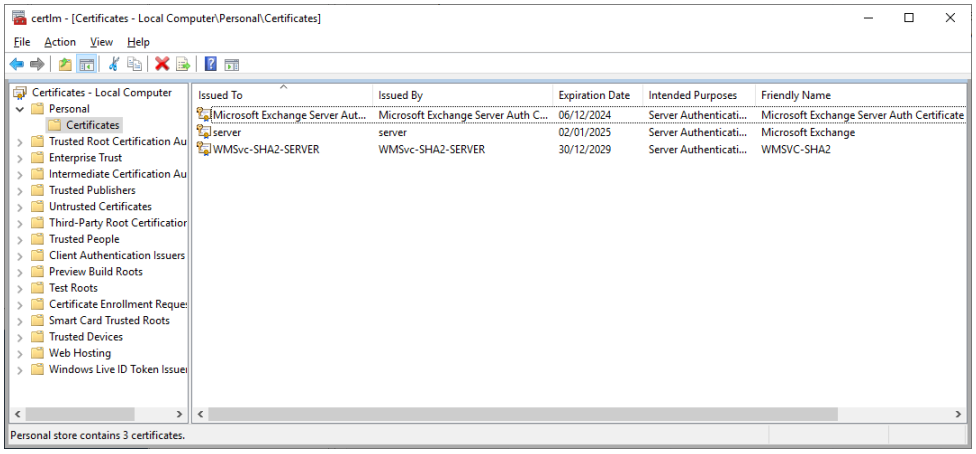
8. Click *Finish*.

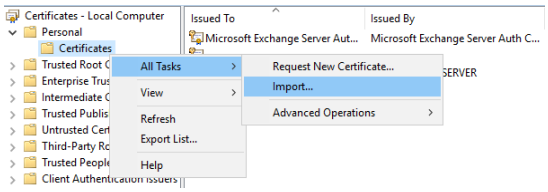


9. Click *Ok* to close the wizard.

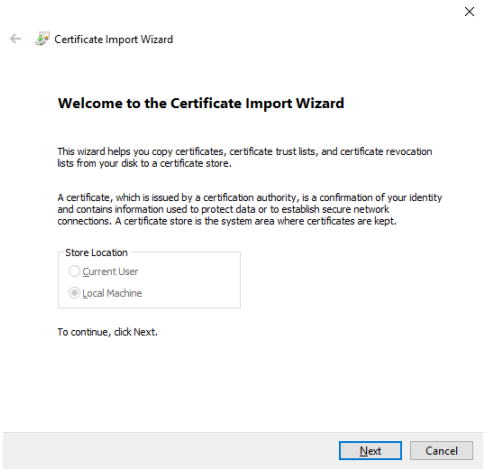
Import Certificate to new Authlogics Authentication Server

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

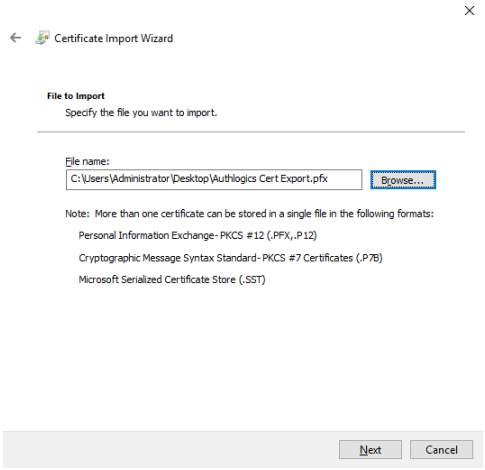




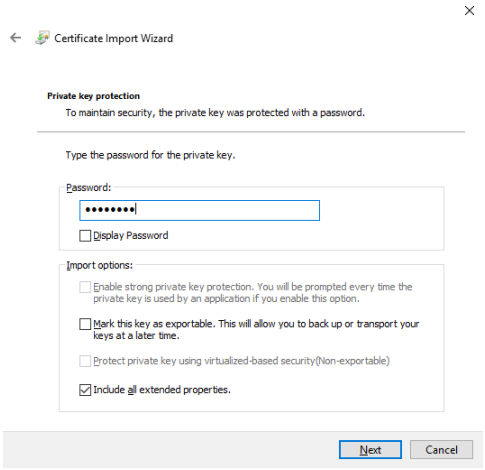
2. Right-click *Certificates* in the *Personal* store, select *All Tasks*, *Import…*



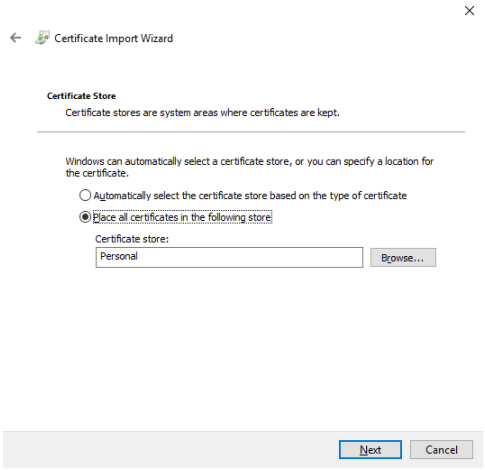
3. Click *Next* to continue.



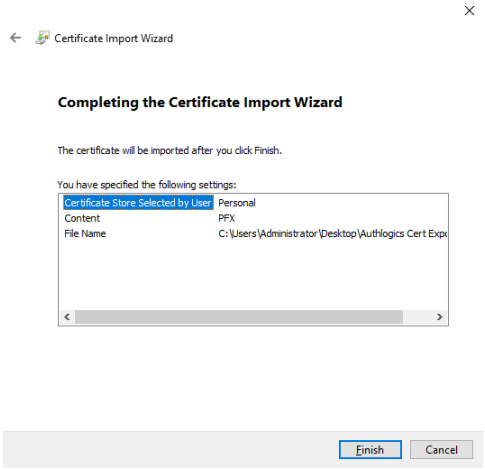
4. Enter the path to the file previously exported. Click *Next* to continue.



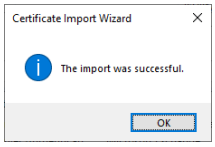
5. Enter the password used when exporting the certificate. Click *Next* to continue.



6. Click *Next* to continue.



7. Click *Finish*.



8. Click *Ok* to close the wizard.

Authlogics Authentication Server Directory Configuration

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

Directory Configuration Wizard

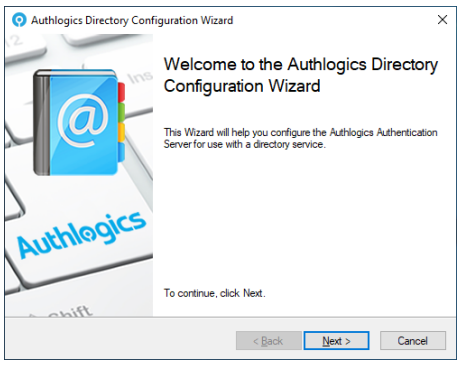
This section should be performed on the server running the Authlogics Authentication Server.

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

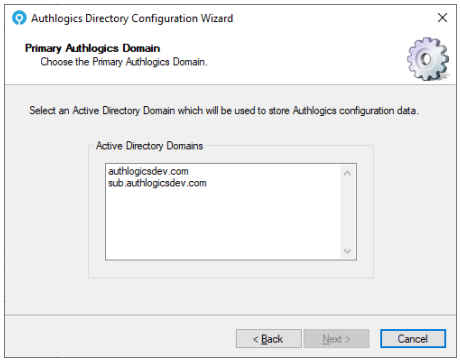
1. Start the Authlogics Directory Configuration Wizard from the Windows Start menu:

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

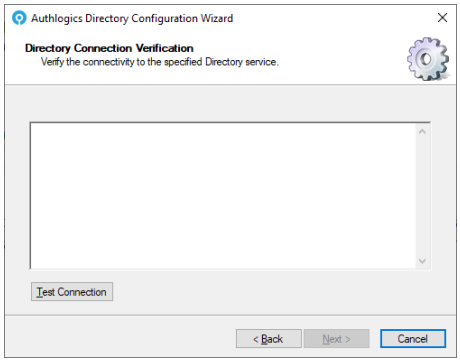
> **Note**
>
> Ensure that you are logged on with domain administrator account and not a local administrator account.



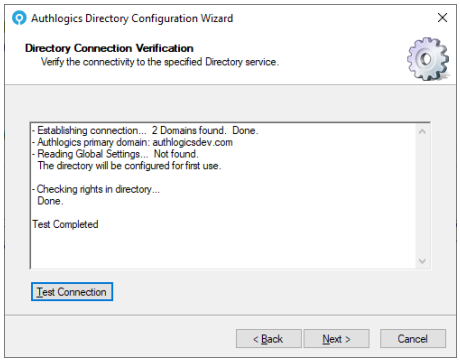
2. Click *Next* to start the Authlogics Authentication Server Configuration Wizard.



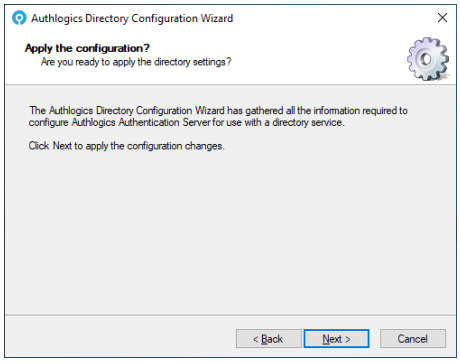
3. If the AD forest contains more than 1 domain and this is the first time the directory is being configured, choose which AD Domain you want to use to store Authlogics configuration data in and click *Next*.



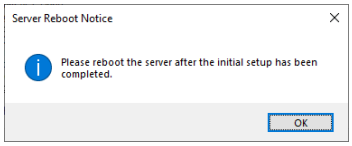
4. To ensure that the Authlogics Authentication Server can access the specified directory click the *Test Connection* button.



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.



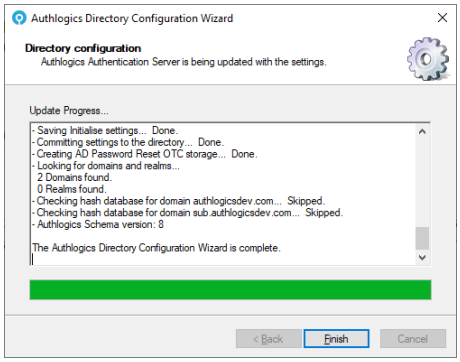
6. Click *Next* to apply the configuration changes.



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

Important!

After configuring the Authlogics Authentication server for use with Active Directory you **MUST reboot the server** otherwise authentication services **will fail**.



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.

Authlogics Licence Configuration

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

Authlogics 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 Authlogics 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, Authlogics 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 licencing@authlogics.com for further information.

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

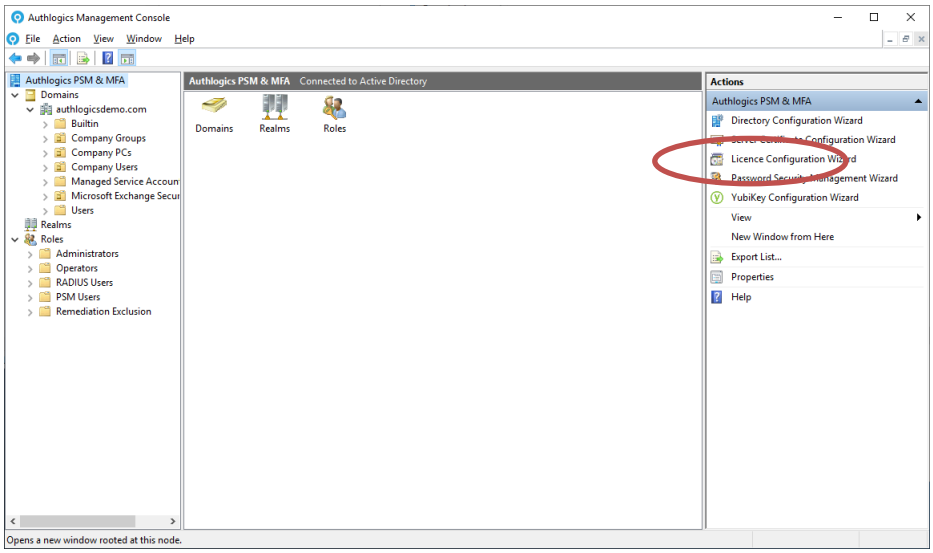
Authlogics provides a free licence for up to 10 users. The free licence does not include our standard product support and assistance and we will only be able to provide email assistance on a best-effort basis. However, access to our knowledge base and community site is freely available: https://support.authlogics.com/.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

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

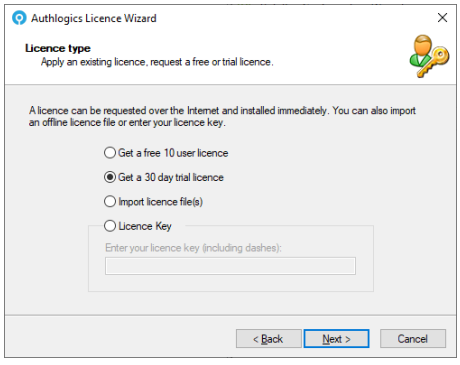
A free or trial licence is installed instantly so you can evaluate at your own pace, however, it does require Internet connectivity (HTTPS) to install and will be activated. If Internet connectivity is not available on the authentication server please contact Authlogics for support.

Licence Configuration Wizard

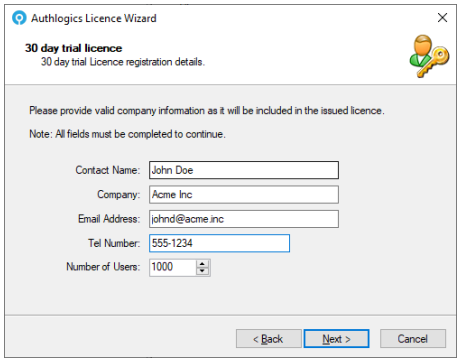
1. The Licence Configuration Wizard will start automatically when the Authlogics Management Console is first loaded. The wizard can also be started from the MMC as follows:



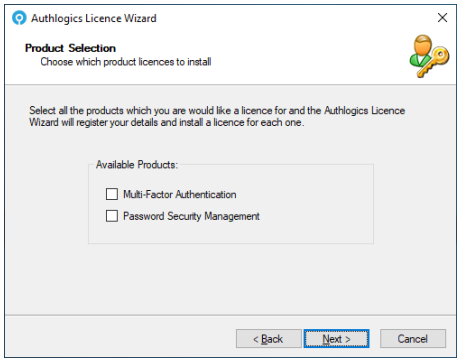
2. Click *Next* to start the Authlogics Licence Configuration Wizard.



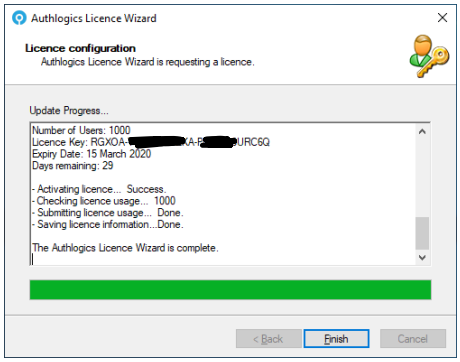
3. Select Get a free 10 user licence or Get a 30-day trial licence. Click Next to continue.



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



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



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

   Click *Finish* when done.

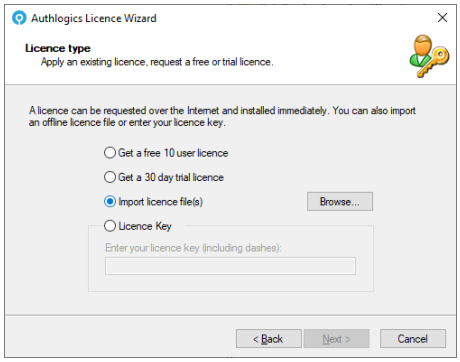
Importing an offline licence file

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

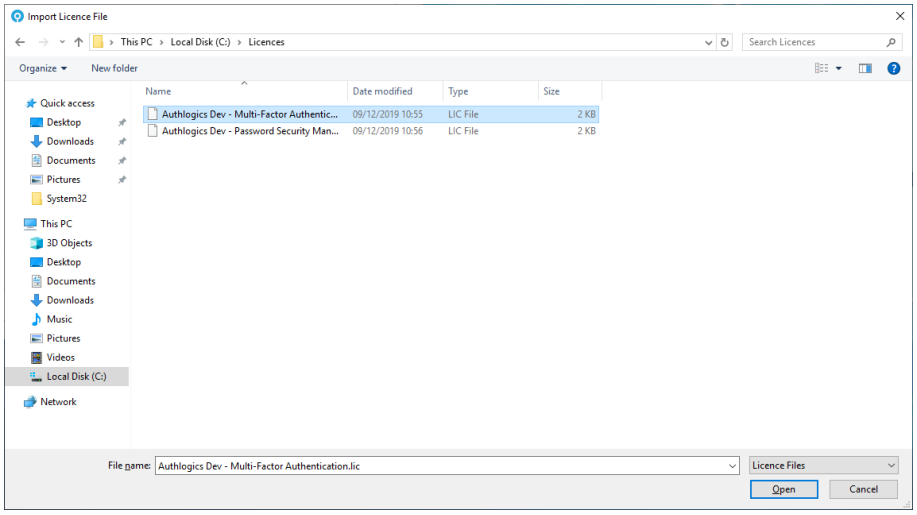
If you have multiple licences files they need to be added one at a time. Simply run the wizard again to add the second licence file.

1. Start the Licence Configuration Wizard

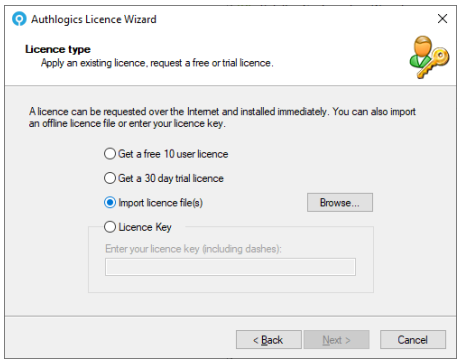
2. Click *Next* to start the Authlogics Licence Configuration Wizard.



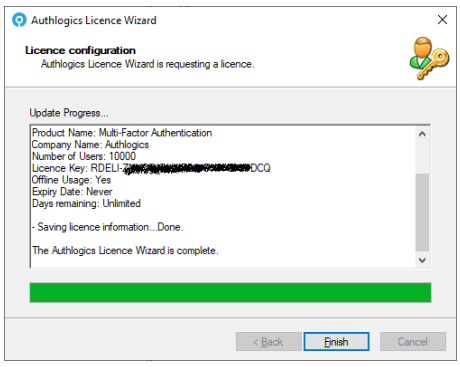
3. Select Import licence file(s) and click Browse…



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



5. Click *Next* to continue.



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

   Click *Finish* when done.

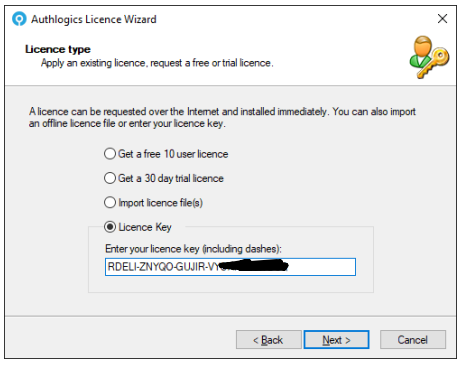
Entering an existing licence key

A licence key is issued by Authlogics 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 Authlogics.

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.

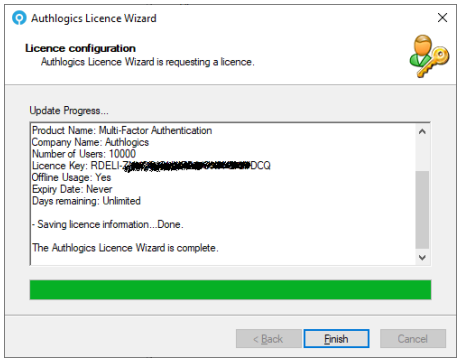
1. Start the Licence Configuration Wizard

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



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

   Click *Next* to continue.



4. The licence will be installed and activated.

   Click *Finish* when done.

Authlogics 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 Authlogics Authentication Server is responsible for doing all retrospective protection, remediation and alerting work required by the scheduled.

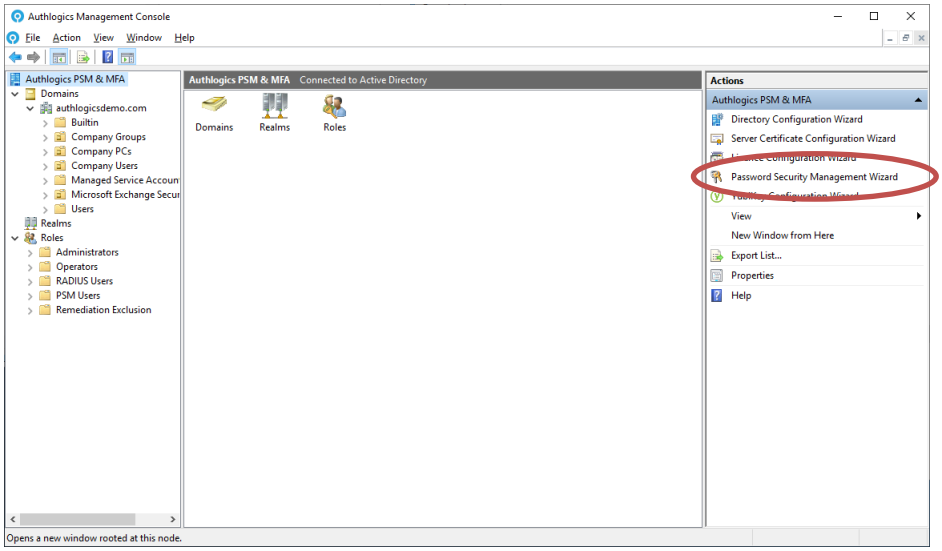
Real-Time Protection: The Authlogics Authentication Server works in conjunction with Authlogics Domain Controller Agent (DCA) to provide real-time protection of Active Directory passwords. The Domain Controller Agent will intercept password changes at the DC as they happen and query the Authlogics Authentication 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 Authlogics Authentication Servers for the policy to take effect.
>
> See the *Configuring the Authlogics Password Policy* Settings section for further information.

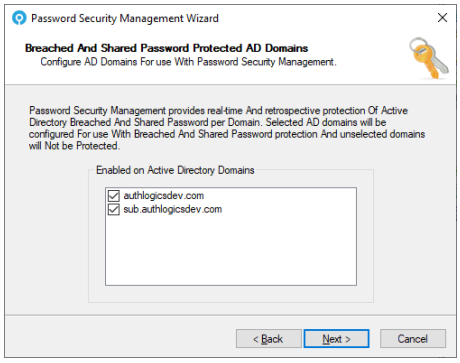
The Authlogics Authentication Server requires Internet access to query the Authlogics Password Breach Database in the Cloud. See the *Internet Access for breach password lookups* section for further information. A fully offline copy of the Authlogics Password Breach Database can be installed on the Authlogics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

Starting the Password Security Management Wizard

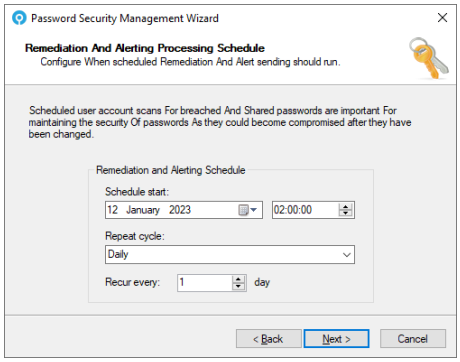
1. The wizard can be started from the MMC as follows:



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

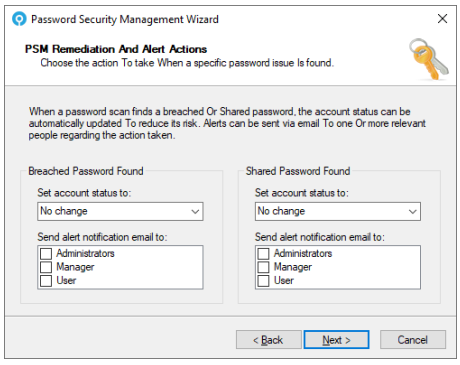


3. Select the domain or domains to which you wish to enable PSM password protection on. Click *Next* to continue.



4. Authlogics 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.



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.

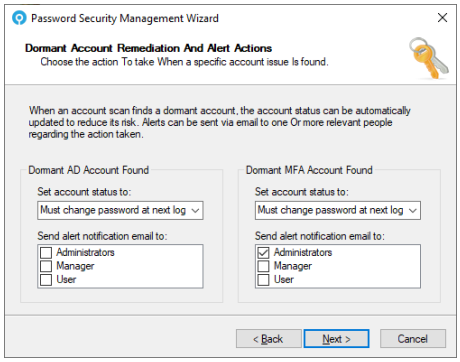
    Set account status for detected Breached Passwords and Shared Passwords to:

    - 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.



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.

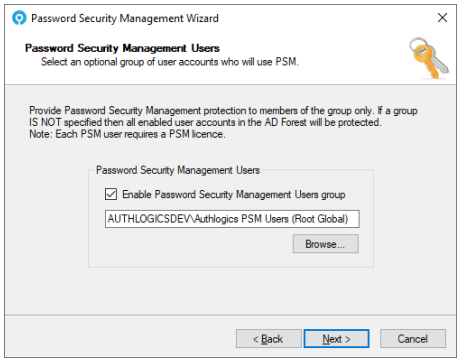
    Set account status for detected dormant AD or MFA accounts to:

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

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

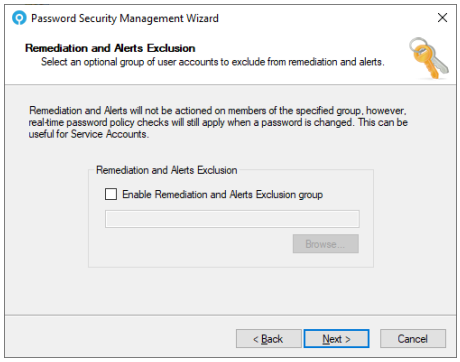
    - Administrators
    - Managers
    - Users

    Click *Next* to continue.



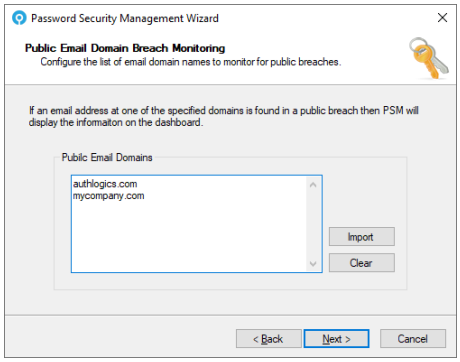
14. To limit which users will use PSM (and thus require a licence) check *Enable Password Security Management Users group* and then click *Browse…* to select an AD Group containing the user accounts to include.

    Click *Next* to continue.



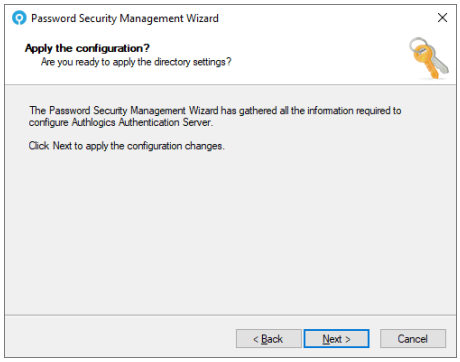
15. To exclude users from PSM remediation and alerting check *Enable Remediation and Alerts Exclusion group* and then click *Browse…* to select an AD Group containing the user accounts to exclude.

    Click *Next* to continue.



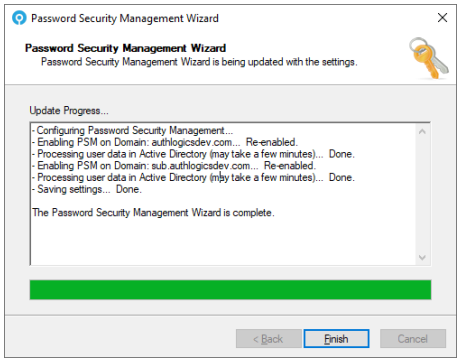
16. To monitor and display data breaches based on email addresses for your organisation on the Web Management Portal Dashboard enter all public email domain names. Authlogics will auto detect any email domain names configured within Microsoft Exchange.

    Click *Next* to continue.



17. Click *Next* to continue.

Password Security Management will be configured.



18. Click *Finish* when done.

YubiKey Configuration Wizard

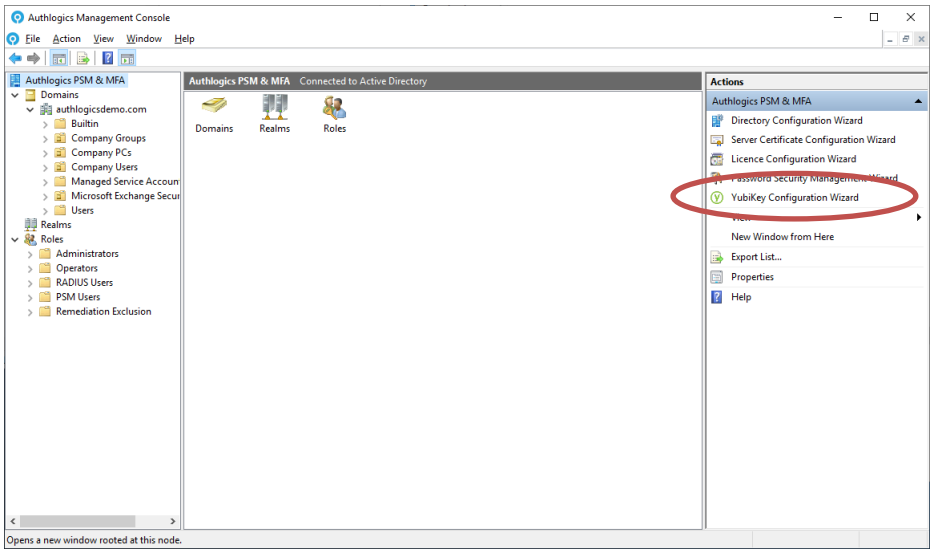
The YubiKey Configuration Wizard is responsible for managing reprogrammed YubiKey tokens so that YubiKey OTPs are processed by the Authlogics Authentication Server and access to the Internet-based YubiKey servers is not required for validation.

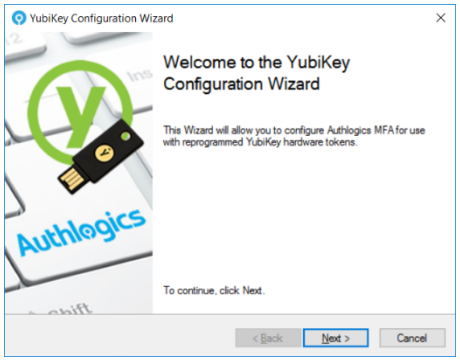
Should you wish to still validate YubiKey OTPs using the Internet-based YubiKey servers for tokens that have not been reprogrammed then the Authlogics Authentication Server still requires Internet access.

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

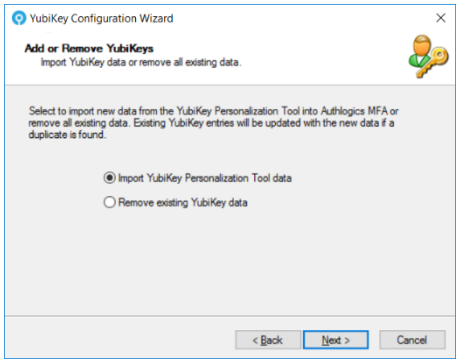
Starting the YubiKey Configuration Wizard

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

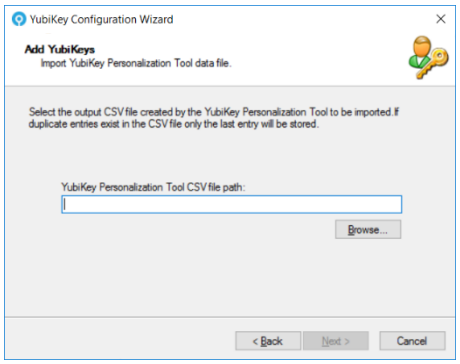




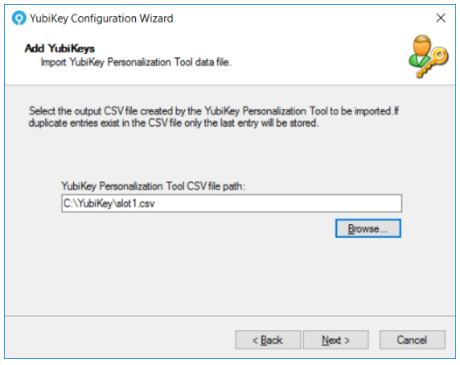
2. Click *Next* to start the Authlogics YubiKey Configuration Wizard.



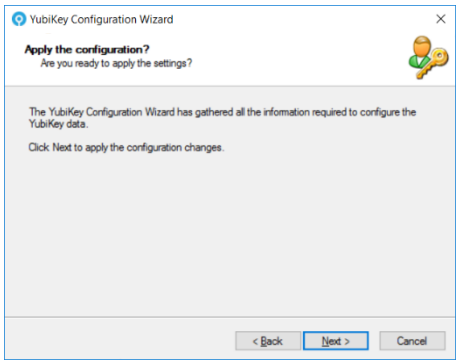
3. Select Import YubiKey Personalisation Tool data. Click *Next* to continue.



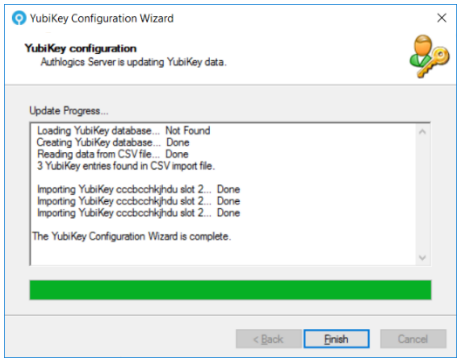
4. Select *Browse* to select the YubiKey Personalisation Tool generated CSV file.



5. Click *Next* to continue.



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



7. The YubiKey database has been imported.

   Click *Finish* when done.

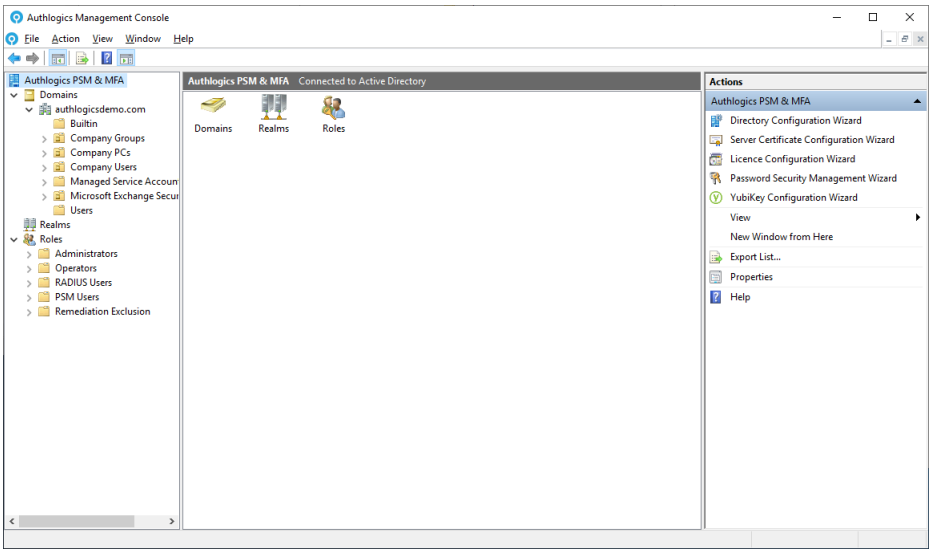
Administering Authlogics Authentication Server

The Authlogics Management Console

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

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

- Directory Configuration
- Authlogics Global Settings
- Authlogics Users in Domains or Realms
- User Roles



Authlogics Management Console Views

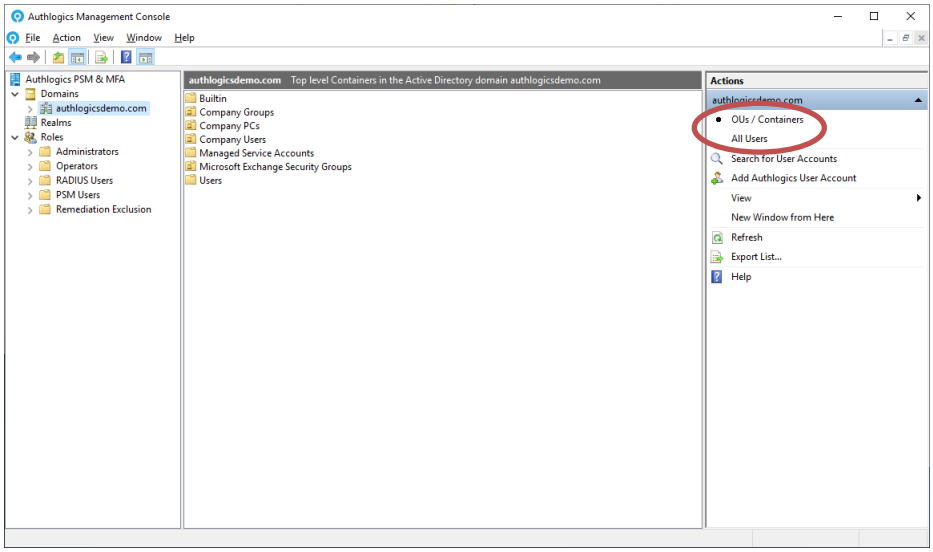
The Authlogics Management Console displays both the MFA and PSM users.

PSM user only icon: 

MFA user icon: 

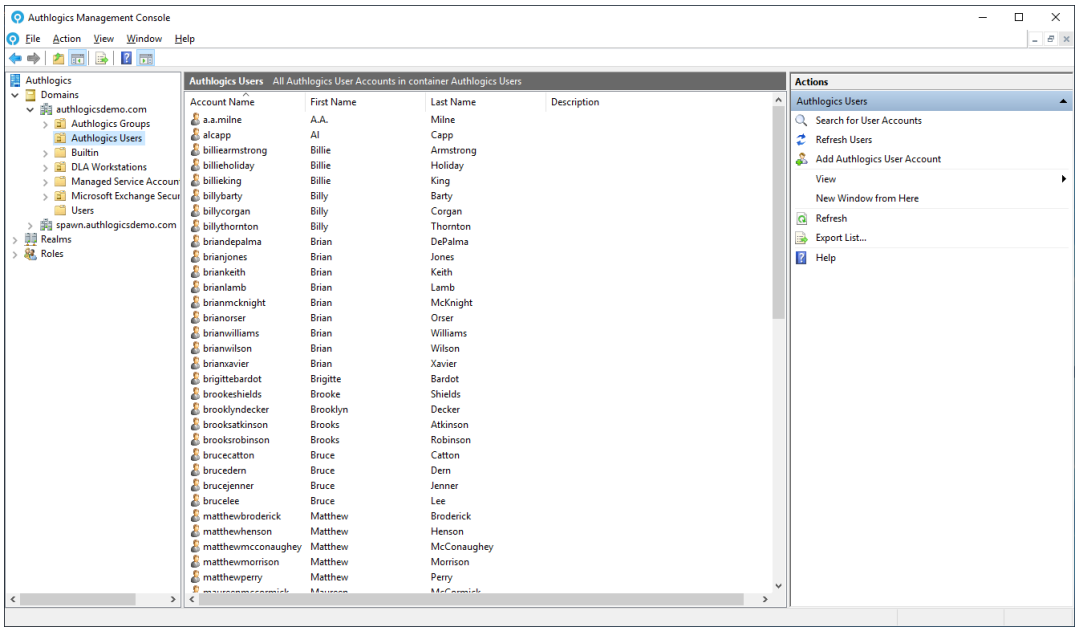
The Authlogics Management Console is suited to small deployments and also scales to very large Active Directory environments. This is achieved by utilising the “OUs / Containers” and the “All Users” view for Active Directory Domains, and a Realms view for External users.

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



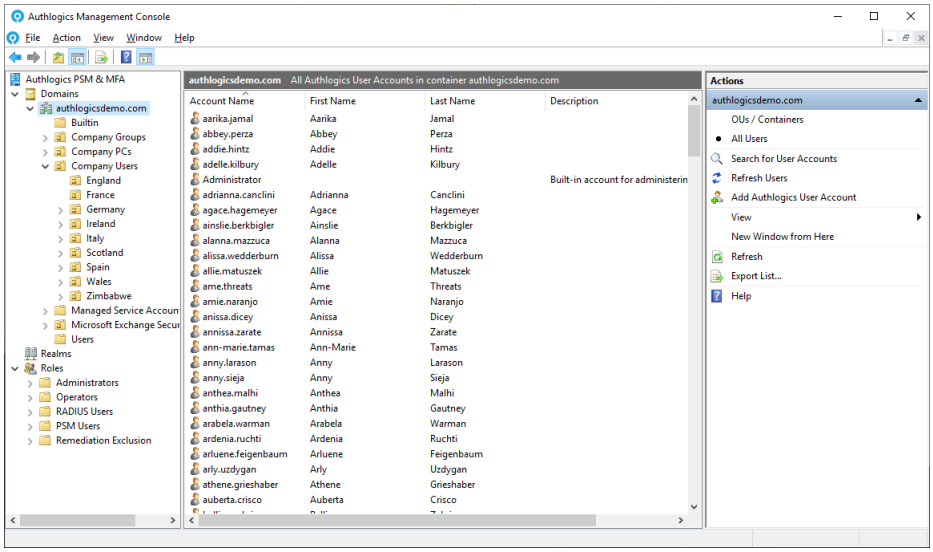
OUs / Containers View

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 “*”.



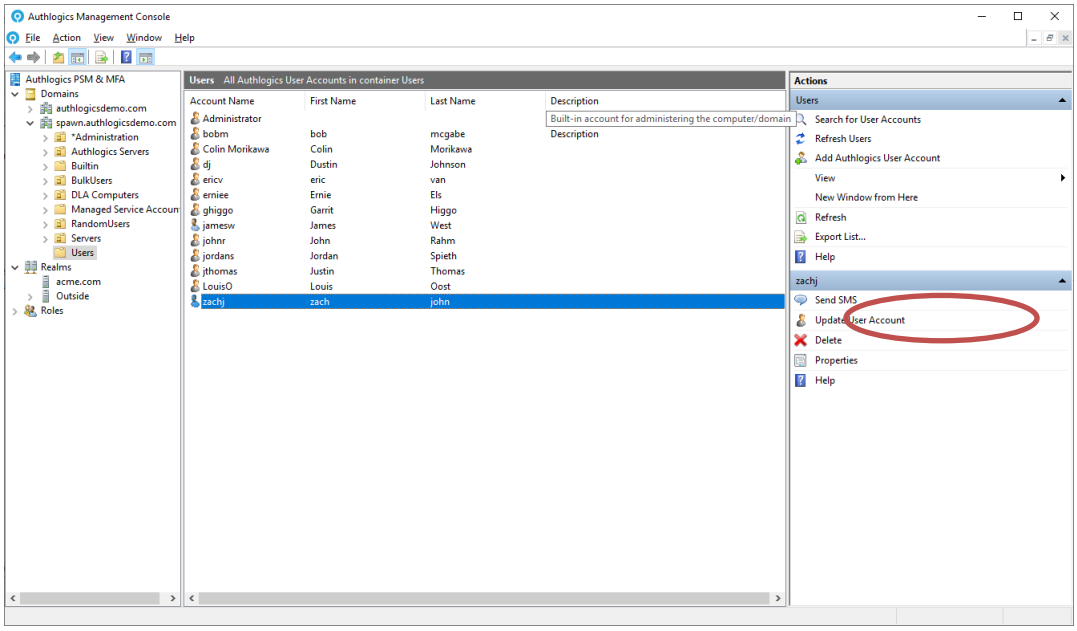
All Users View

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.

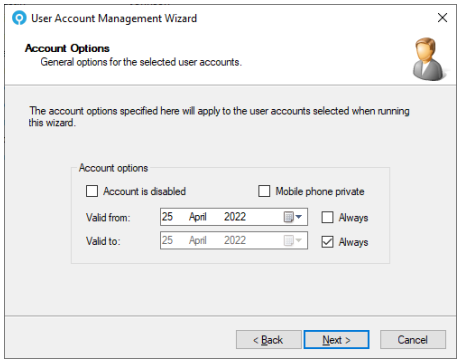


Updating PSM Users

PSM users are automatically added to the Authlogics Management Console when the user interacts with Authlogics 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.

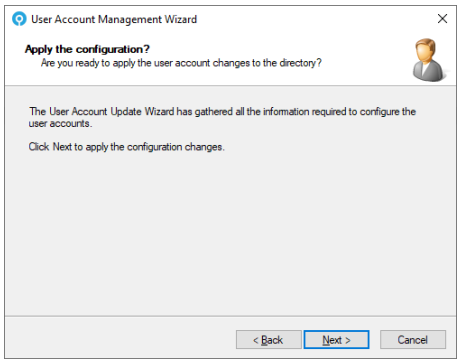


1. Click *Next* to start the User Account Update Wizard.

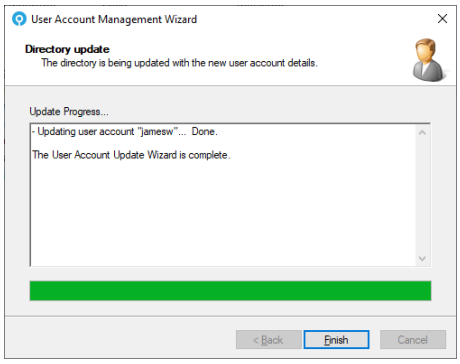


2. Account options determine the user's initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use. The mobile phone privacy setting can also be specified. Make any required changes and click Next

to continue.



3. Click Next to Apply the configuration changes.



4. The User Account has been updated.

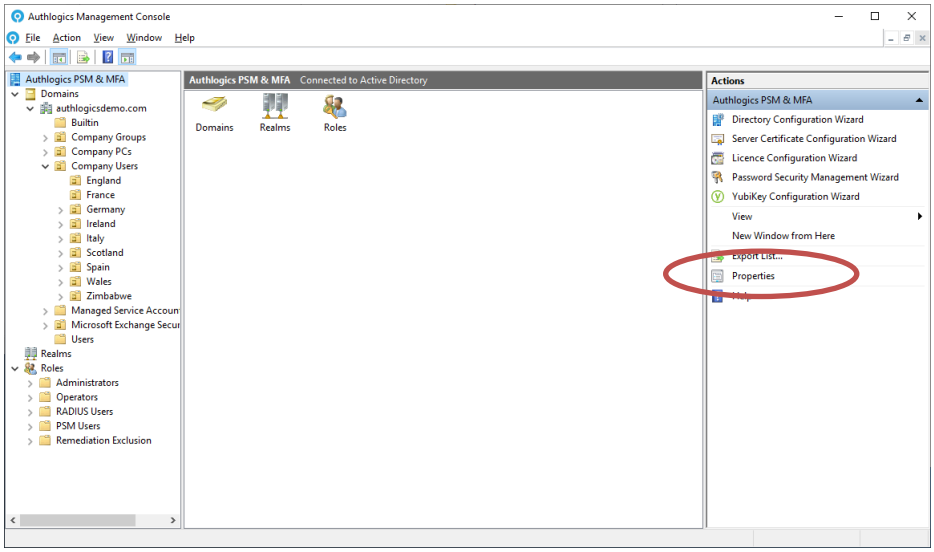
   Click *Finish* when done.

Global Settings walkthrough

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

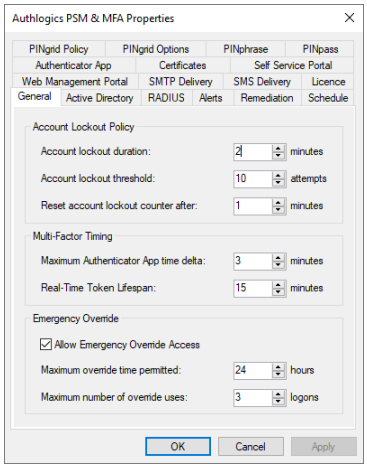
1. Open the Authlogics Authentication Server Management Console.
2. Highlight the high-level **Authlogics** node. The node name will include the product name based on the installed licences, e.g. PSM and/or MFA).

   Click *Properties* in the Actions pane.



The General Tab

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



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 Authlogics server.

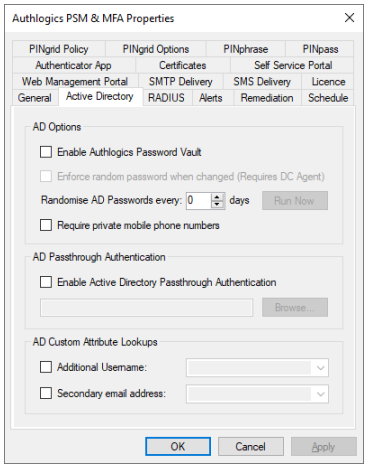
Real-time Token Lifespan provides the number in minutes that a Real-Time token can be used for before it expires. After this period has exceeded, the token will no longer be able to be used.

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.

The Active Directory Options Tab

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



The *Authlogics 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 Authlogics 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 Authlogics 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 Authlogics to use a custom LDAP attributes on a user account when looking up a user account name or secondary email address.

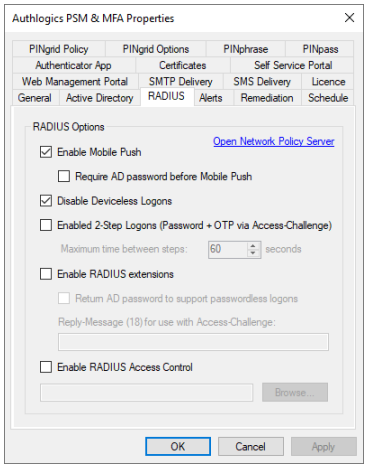
The *Additional Username* option may be useful to locate a user account via an employee number instead of an AD account name. If the employee number is stored in "extensionAttribute1" in AD then you can configure Authlogics to also look in the specified attribute. The custom field is used as a secondary 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 Authlogics should search.

The RADIUS Tab

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



Authlogics 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 PINgrid and PINphrase 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.

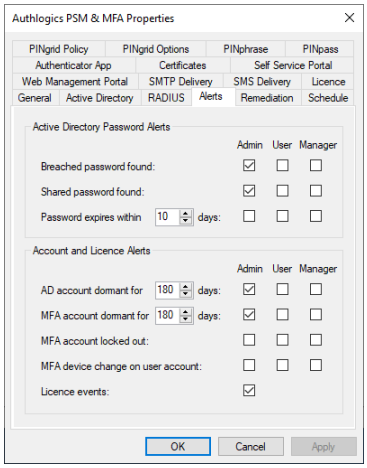
> **Step 1:** If the AD password is valid then Access-Challenge will be returned to tell the RADIUS client to request an OTP. If the AD password is invalid then an Access-Reject will be returned.
>
> **Step 2:** If the OTP is received within the allowed time (60 seconds by default) and it is valid an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

The Alerts Tab

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



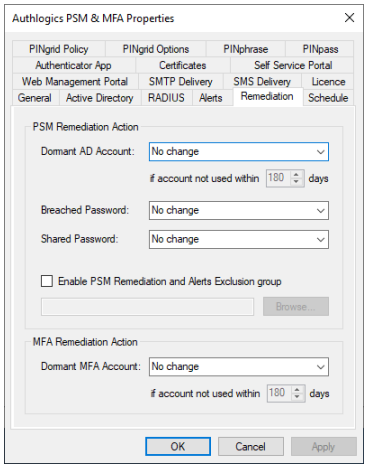
> **Note**
>
> Alerts are sent via SMTP and cannot be configured unless an SMTP server is configured first. The options available are dependent on which licence types are installed and which PSM policies are configured.

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.

The Remediation Tab

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



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:

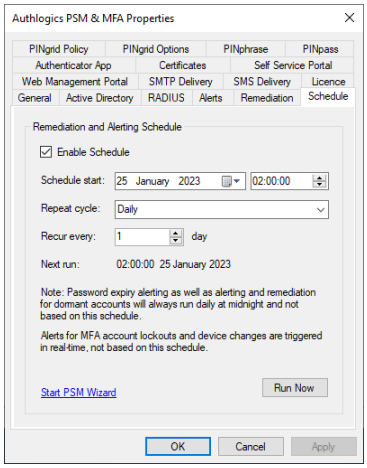
- No change
- Must change at next logon
- Account is disabled

“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”.

The Schedule Tab

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



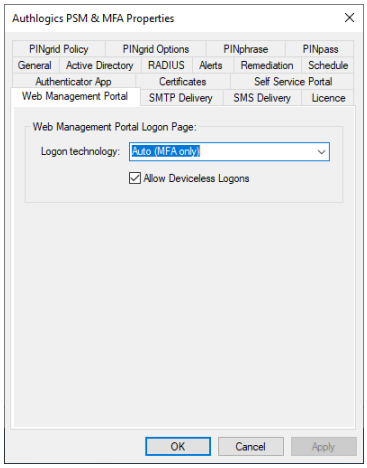
It is recommended to run the schedule daily out of hours, however, this can be customised as required. The processing work is ONLY performed on the primary Authlogics Server.

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.

The Web Management Portal Tab

The Web Management Portal tab contains the customisation options for the Web Management Portal.



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

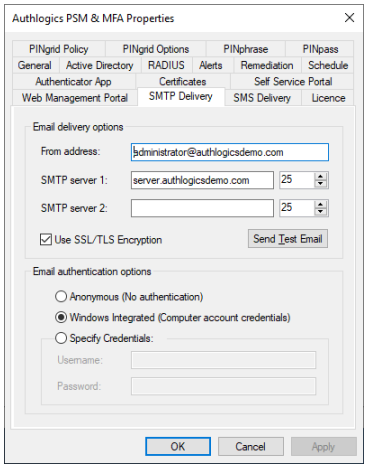
- Auto (MFA only)
- Mobile Push
- PINgrid
- PINphrase
- PINpass
- Password (Active Directory password)
- Windows Authentication (pass-through authentication)

PINgrid and PINphrase both support Deviceless authentication, check the "Enable Deviceless Logons" box to enable this support. If this is not enabled, then MFA will always be required.

When an MFA licence is installed the default logon option 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.

The SMTP Delivery Tab

When users provisioned using the Authlogics 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. The SMTP Delivery tab allows administrators to set the SMTP host and port for the email server for email message delivery.

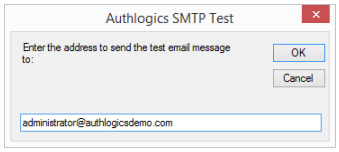


The *From address* setting specifies the email address which delivered mail will be received from.

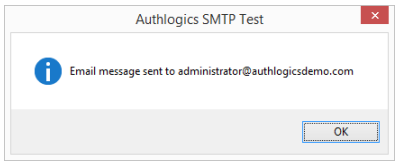
A primary SMTP must be specified to send an email. A secondary SMTP may be specified for redundancy purposes. The secondary server is only used if the sending fails via the primary server. Enter the *SMTP server 1* and *SMTP server 2* DNS names or IP addresses and corresponding port numbers. If the servers 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 a test email address and click OK.



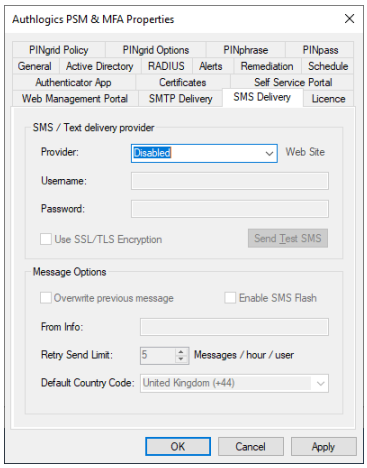
A confirmation that the message has been sent is displayed is the send was successful; if not an error stating the SMTP issue is displayed.

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

The SMS Delivery Tab

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

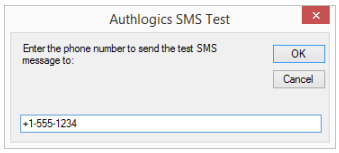
The administrator can also send notification or broadcast messages to one or many users via the MMC by right-clicking an account and selecting the *Send SMS* menu option.



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 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*.

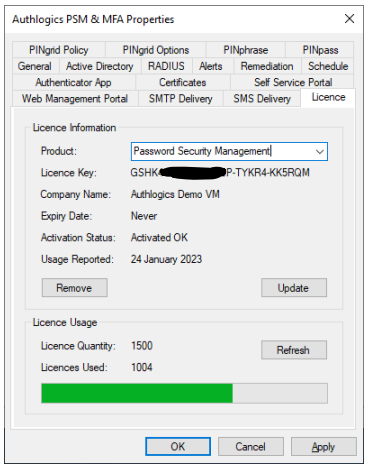
Enter the number that all messages will appear to be delivered from.

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.

The Licence Tab

The Licence tab displays the loaded licence information.



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.

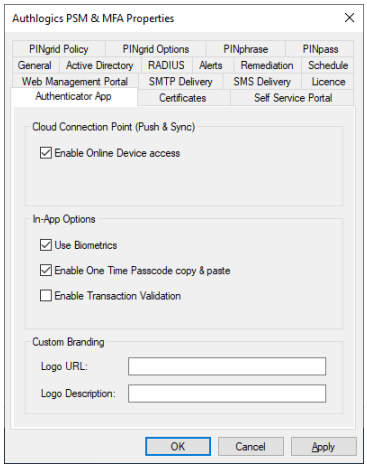
Licences can be removed by clicking the *Remove* button, which will be replaced by an *Add* button. Clicking the *Add* button starts the Licence Configuration Wizard.

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 Authlogics.

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

The 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.



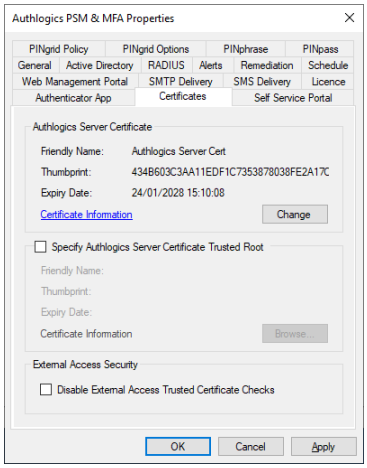
To allow the Authenticator App to perform an online pairing and Mobile Push authentication ensure the "Enable Online Device access" option is checked.

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.

The Certificates Tab

The Certificates tab allows you to change the Authlogics Server Certificate which is used to secure the Authlogics data stored in Active Directory as well as the Server Password Vault. By default, the installation program will generate a self-signed certificate. This is NOT the certificate used by IIS for HTTPS (SSL) connections to the server.



The Authlogics 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 Authlogics 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 Authlogics data stored in Active Directory.

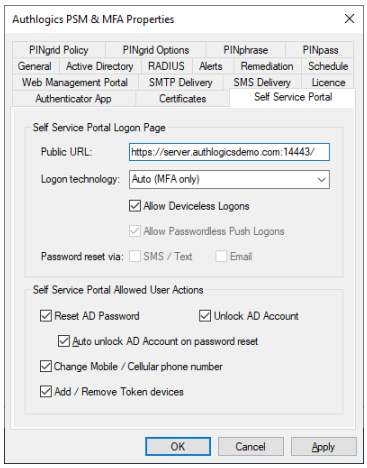
If using Windows Desktop Agent you can select an *Authlogics Server Certificate Trusted Root* certificate. If there is an enterprise CA available then a CA root certificate can be specified. This will require all Authlogics Desktop Agent machines to have a certificate installed on them which was issued 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 *Authlogics Server Certificate Trusted Root* certificate is not configured then the default Self Signed Certificates will be used.

Desktop Logon Agents connecting to the Authlogics Authentication Server using the External Access Server role must have a trusted certificate installed on it so that it have be validated by the Authlogics 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.

The Self Service Portal Tab

The Self Service Portals tab 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 PINgrid pattern, 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.



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.

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

- Auto (MFA only)
- Push
- PINgrid
- PINphrase
- PINpass
- Password (Active Directory password)
- Windows Authentication (pass-through authentication)

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.

PINgrid and PINphrase 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.

If Push authentication is selected, the option of "Allow Passwordless Push Logons" will be available. When enabled, a password is not required before a Push notification is sent to a user's device.

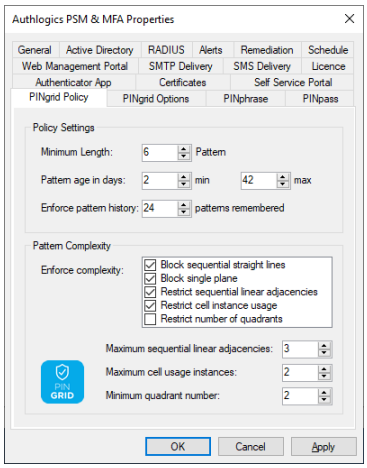
When only a PSM licence is installed the Self Service Portal can still issue One Time Codes via SMS/Text or Email for Active Directory Password reset purposes. To use this feature the logon type must be set to *Password* and either *SMS / Text* or *Email* must be checked.

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

The PINgrid Policy Tab

This tab configures the pattern policy and complexity settings.



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.

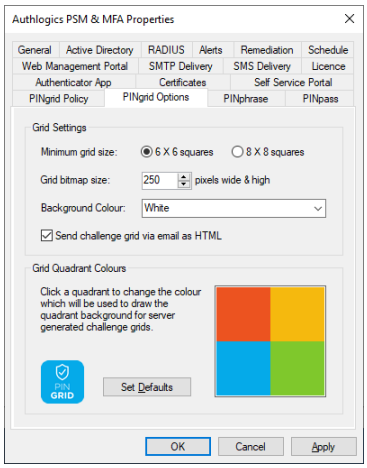
By enabling *enforce pattern history* an administrator can prevent users from re-using previously used patterns. Specify how many previous patterns are remembered.

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.

The PINgrid Options Tab

This tab configures generic and visual elements of PINgrid.



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 PINgrid grid.

Available Background Colours:

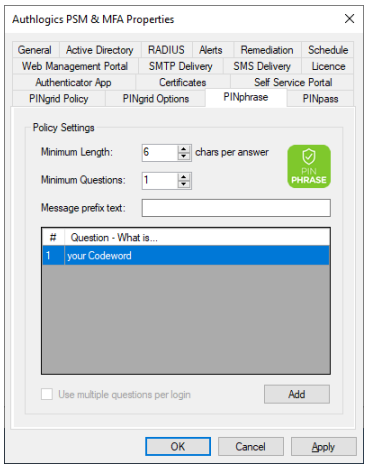
- Black
- Transparent
- White

When PINgrid 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.

The PINphrase Tab

This tab configures the standard PINphrase policy settings.



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 PINphrase. PINphrase allows administrators to create multiple questions and allow a user to select a subset of those questions to answer.

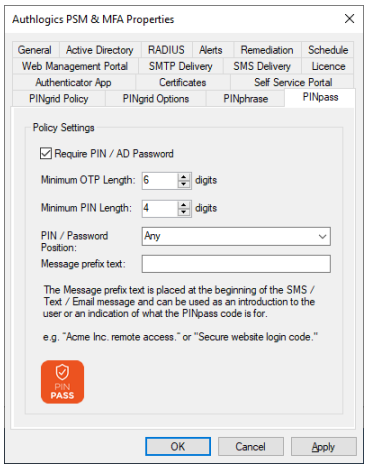
Set the *Message prefix text* that will precede all PINphrase challenges which are sent to mobile devices.

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 PINphrase challenge questions, Click *Add*.

Enable the *Use multiple questions per login* option to make PINphrase 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.

The PINpass Tab

This tab configures the standard PINpass policy settings.



PINpass can be used as a single or Multi-Factor Authentication solution. To enforce Two Factor Authentication with PINpass check the *Require PIN / AD Password* box so the user must enter a PIN code or Password along with an OTP when authenticating. This option is typically disabled when PINpass 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 PINpass token challenges.

Managing Users

As Authlogics 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 Authlogics 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 can not 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 Authlogics 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 and devices.

Adding a New Authlogics Realm

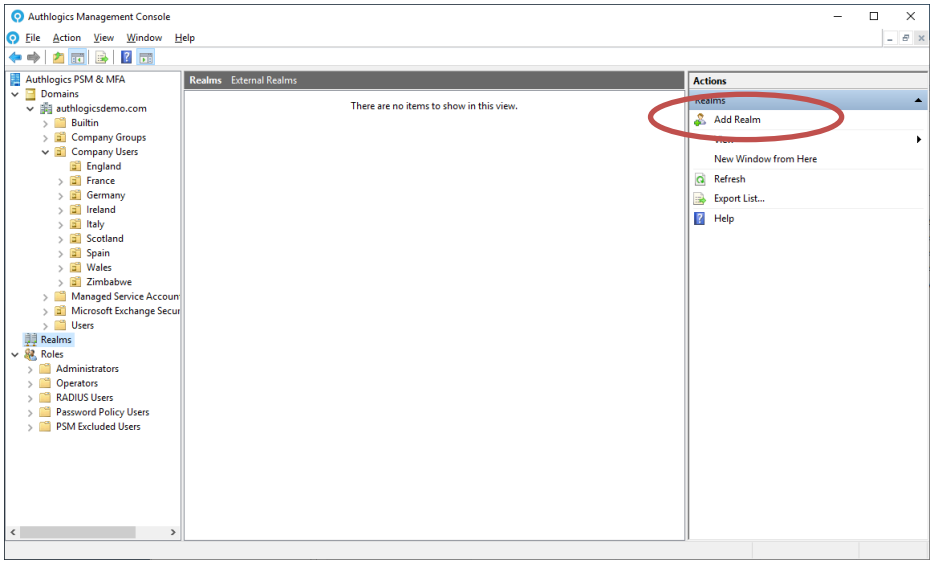
An Authlogics Realm is a container to store External User accounts. Each account within a Realm must have a unique name. Realms and account names can be renamed when needed.

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

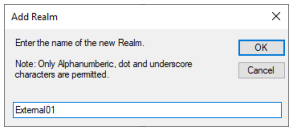
The Realm name forms part of the user logon name. A user would enter their logon names as follows:

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

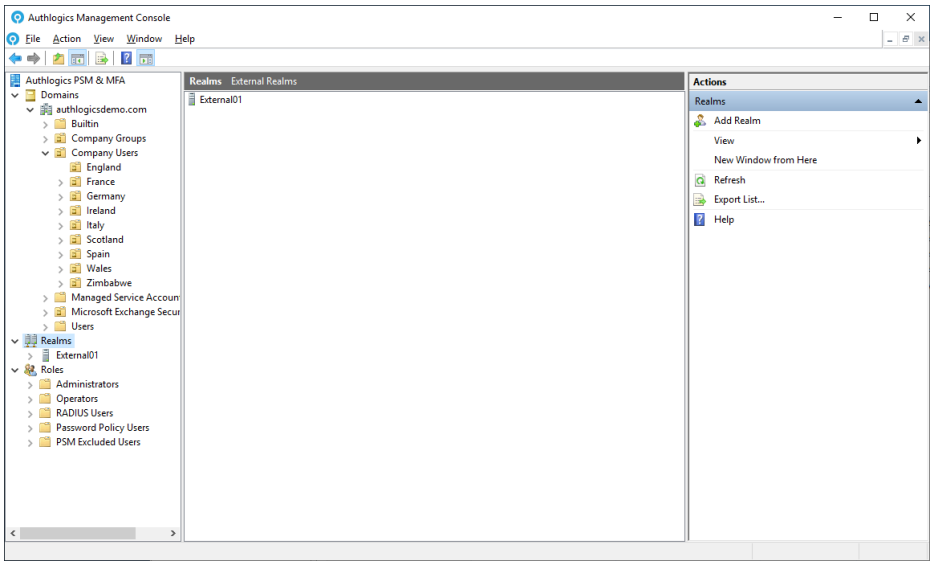
1. Select Realms in the Management Console.



2. Click Add Realm.



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.

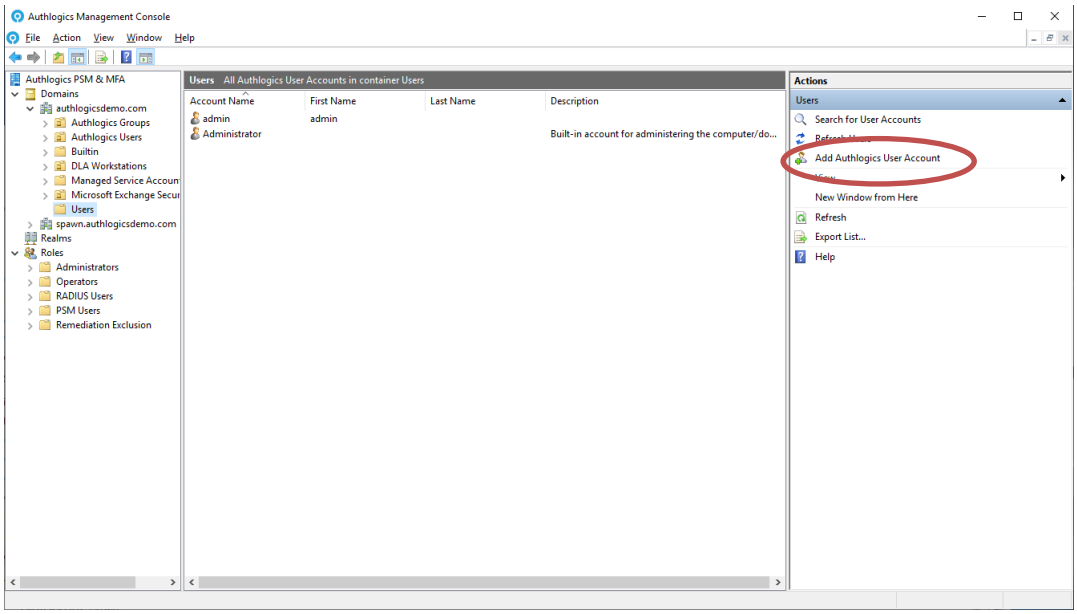
If only a PSM licence is installed then users can be created with PSM self-services features only. PSM users can access the Self Service Portal to change reset their password with One Time Codes. PSM users cannot be provisioned for use with Multi-Factor Authentication.

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.

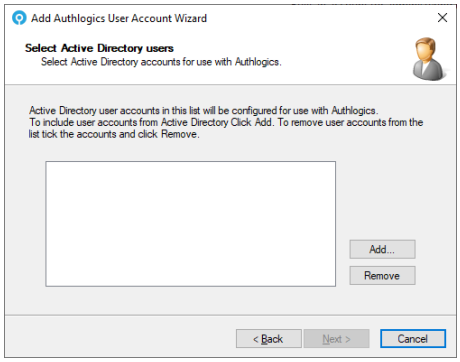
Adding a New Authlogics User Account

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



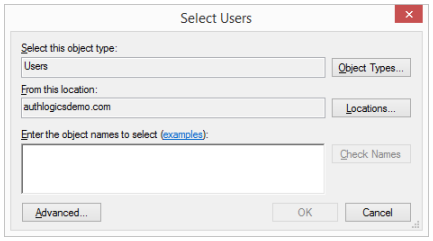
2. Click Add Authlogics User Account.

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

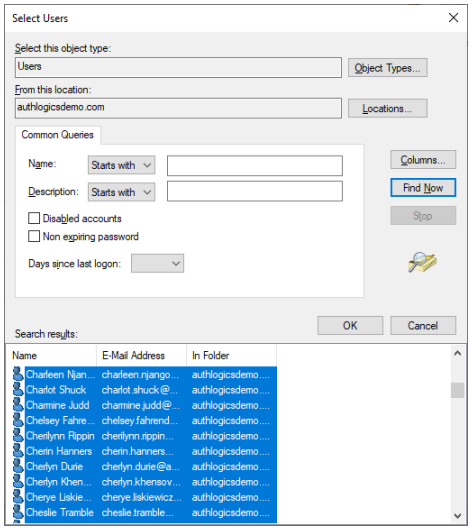


4. To add existing Active Directory users click *Add*.

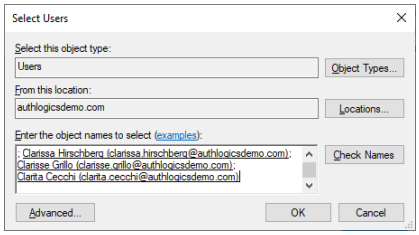
> **Note**
> This process does not create user accounts in the Active Directory Domain, it simply adds Authlogics metadata to an existing account. Ensure that the domain accounts exist before adding them to the Authlogics MMC.



5. Click Advanced… then click Find Now



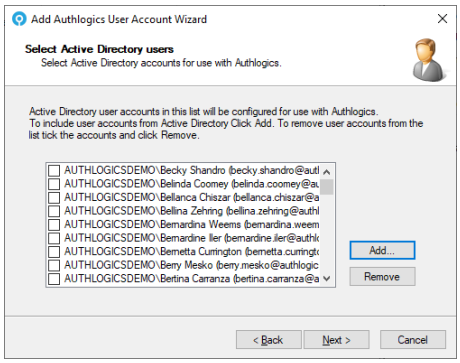
6. Select the required users from Active Directory and click *OK*.



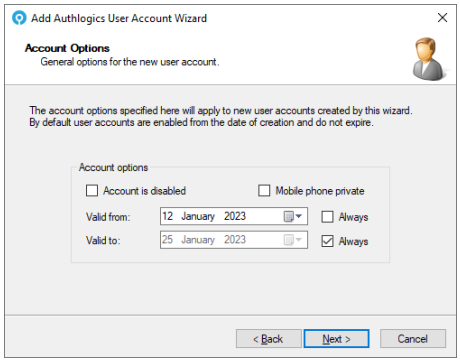
7. Click *OK*.

Tip

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

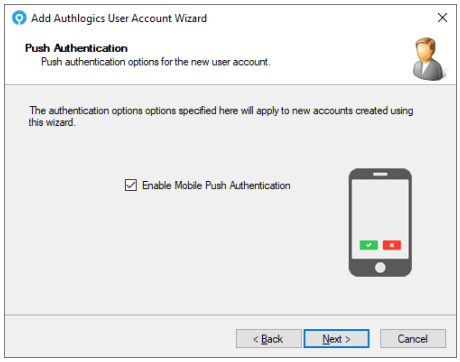


8. Click *Next*.

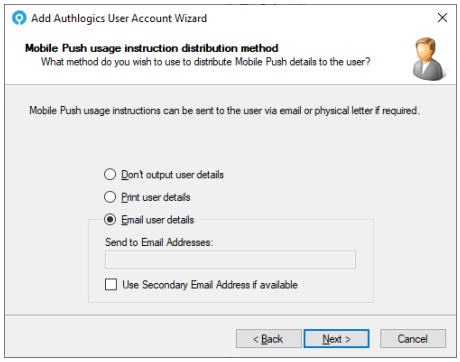


9. Account options determine the user's initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use.
   The mobile phone privacy setting can also be specified.

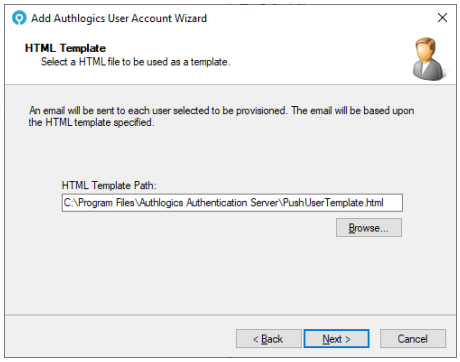
   Make any required changes and click *Next*.



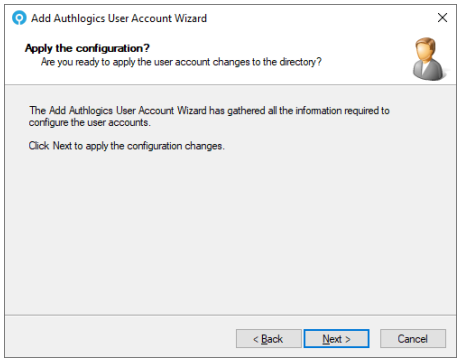
10. Choose if the users should be enabled for Mobile Push authentication or not and click *Next*.



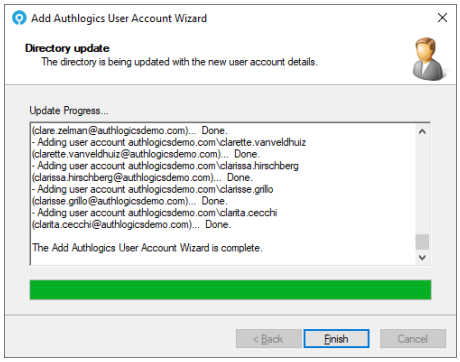
11. Choose how and if the users will receive a welcome email with instructions on how to setup their device for Mobile Push and click *Next*.



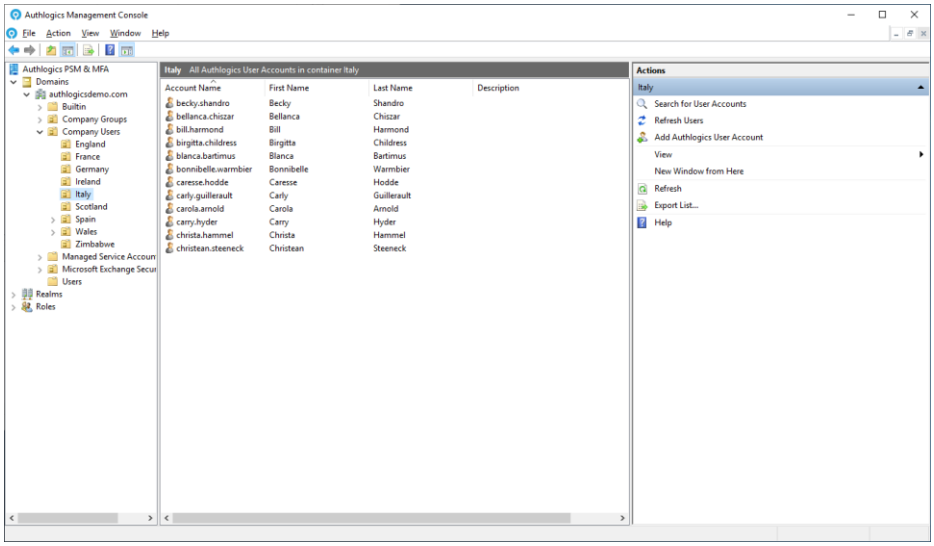
12. Select the HMTL template file to use for the letter and click *Next*.



13. Click *Next*.



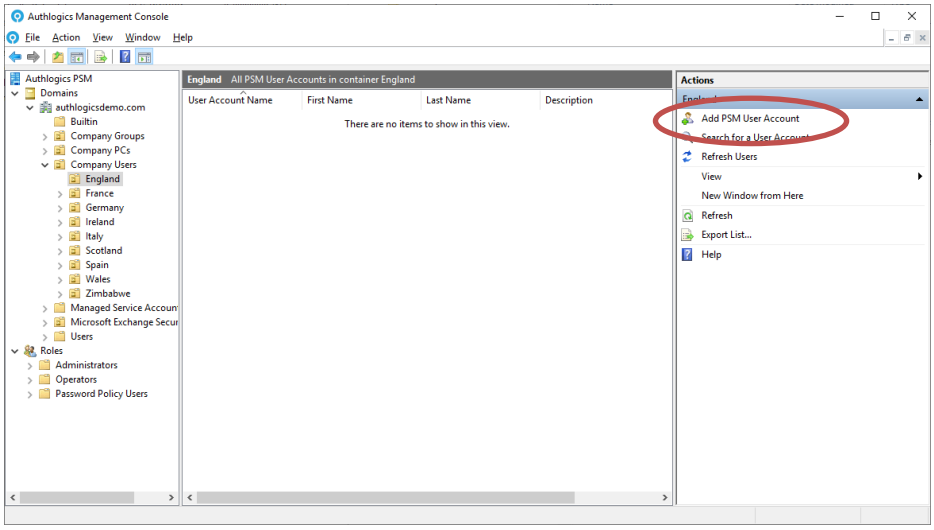
14. The New User Account(s) has/have been created.
    Click *Finish*.


Authlogics Management Console
File Action View Window Help
Authlogics PSM & MFA
Domains
authlogicsdemo.com
Builtin
Company Groups
Company Users
England
France
Germany
Ireland
Italy
Scotland
Spain
Wales
Zimbabwe
Managed Service Accoun
Microsoft Exchange Secur
Users
Realms
Roles
Italy All Authlogics User Accounts in container Italy
Account Name
First Name
Last Name
Description
becky.shandro Becky Shandro
bellanca.chiszar Bellanca Chiszar
bill.harmond Bill Harmond
birgitta.childress Birgitta Childress
blanca.bartimus Blanca Bartimus
bonnibelle.warmbier Bonnibelle Warmbier
caresse.hodde Caresse Hodde
carly.guillerault Carly Guillerault
carola.arnold Carola Arnold
carry.hyder Carry Hyder
christa.hammel Christa Hammel
christean.steeneck Christean Steeneck
Actions
Italy
Search for User Accounts
Refresh Users
Add Authlogics User Account
View
New Window from Here
Refresh
Export List...
Help

Adding a New Authlogics PSM User Account

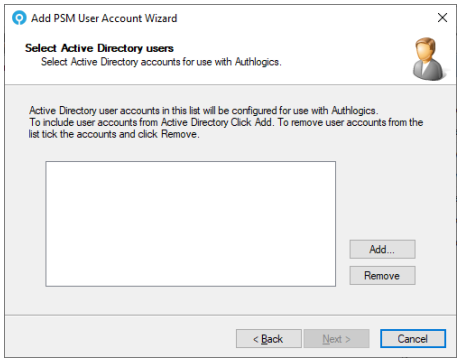
PSM user account can be manually added if required, however PSM users will automatically apprear when a user changes their password or logs onto the Self Service Portal.

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



2. Click Add PSM User Account.

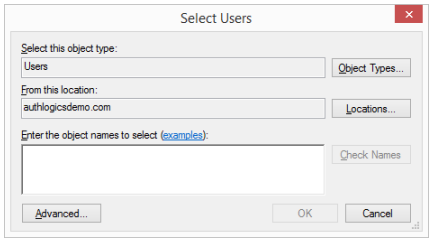
3. The Add PSM User Account Wizard starts. Click *Next*.



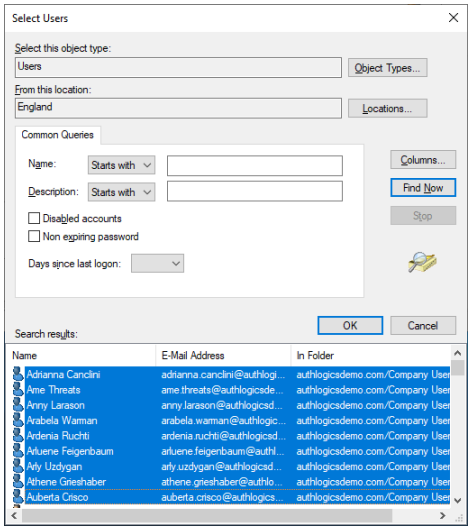
4. To add existing Active Directory users click *Add*.

Note

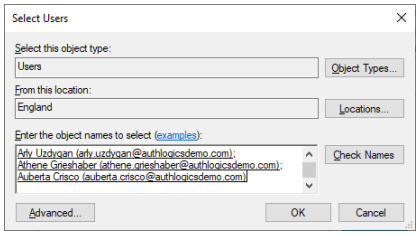
This process does not create user accounts in the Active Directory Domain, it simply adds Authlogics metadata to an existing account. Ensure that the domain accounts exist before adding them to the Authlogics MMC.



5. Click Advanced… then click Find Now



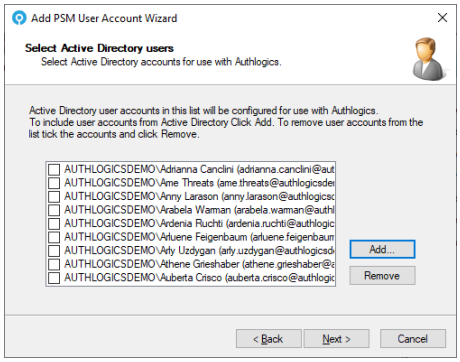
6. Select the required users from Active Directory and click *OK*.



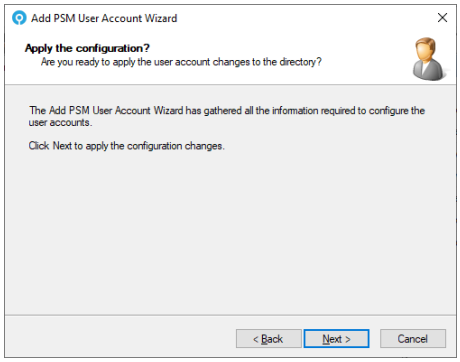
7. Click *OK*.

Note

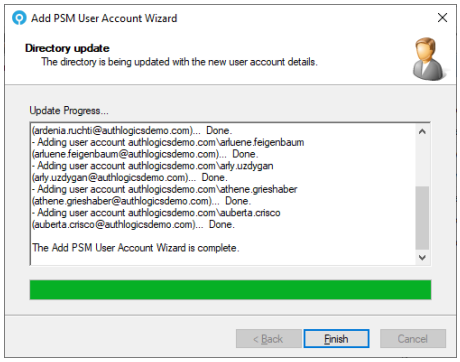
To remove accounts from the list, check the box next to the name and click *Remove*.



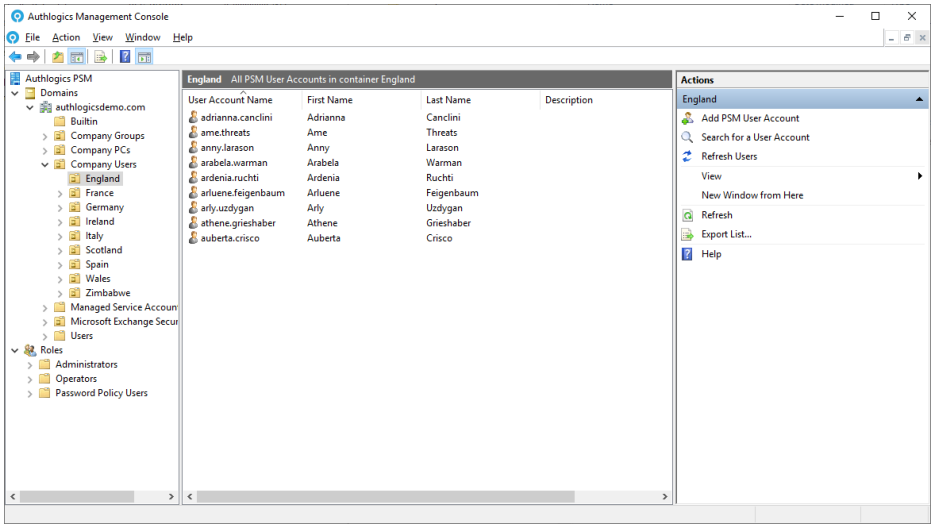
8. Click *Next*.



9. Click *Next*.

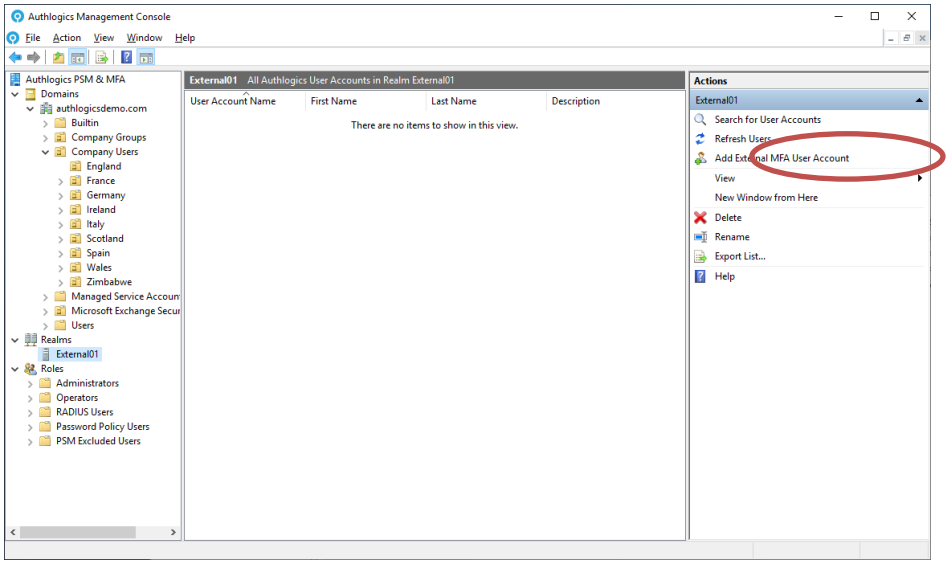


10. The New User Account(s) has/have been created.
    Click *Finish*.

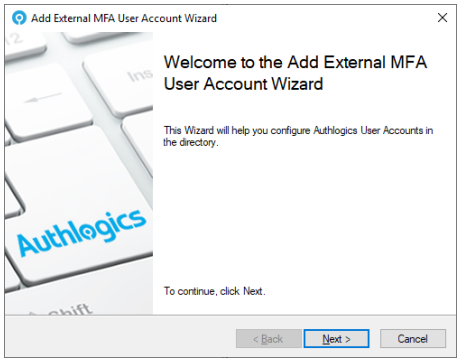


Adding a New External MFA User Account

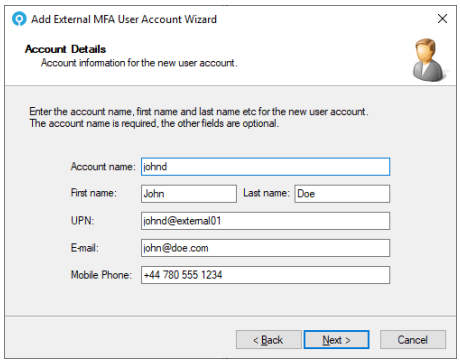
1. Expand Reams and select the appropriate Realm to add the account.



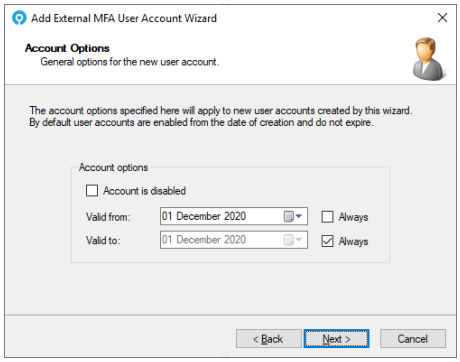
2. Click Add External MFA User Account.



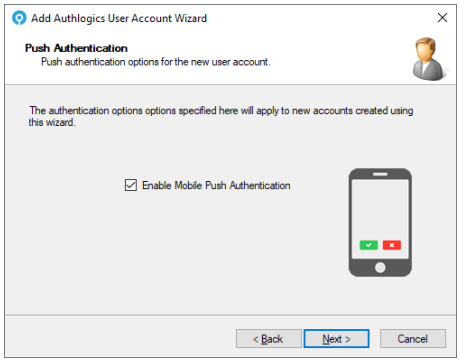
3. The Add External MFA User Account Wizard starts. Click *Next.*



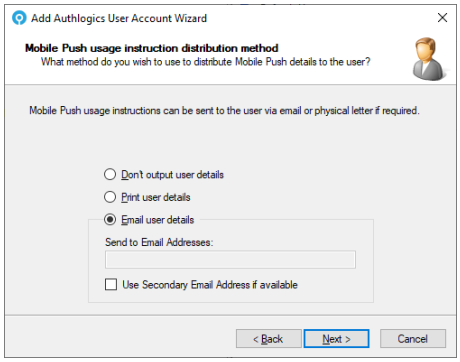
4. Enter the details for the new user account. Only the *Account name* is required, all other fields are optional. The *UPN* will be automatically generated based on the *Realm* and *Account* name however it may be manually edited as needed.
   Click *Next*



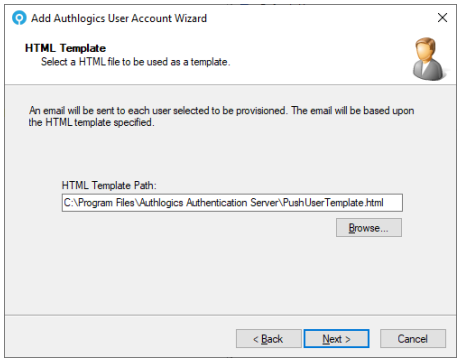
5. Account options determine the user's initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use.
   Make any required changes and click *Next.*



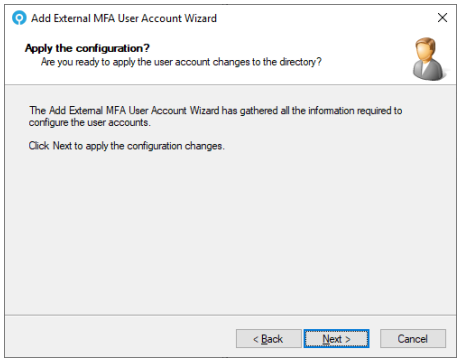
6. Choose if the users should be enabled for Mobile Push authentication or not and Click *Next.*



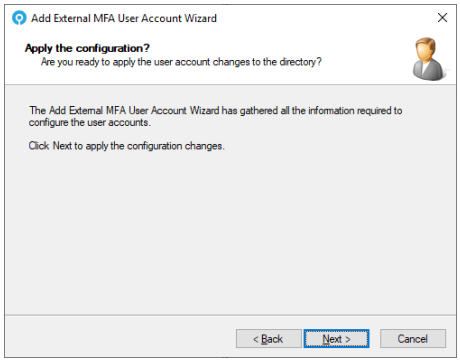
7. Choose how and if the users will receive a welcome email with instructions on how to setup their device for Mobile Push and click *Next*.



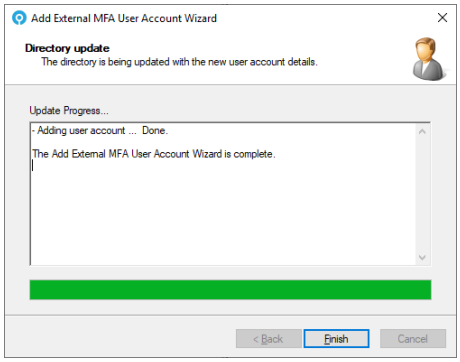
8. Select the HMTL template file to use for the letter and click *Next*.



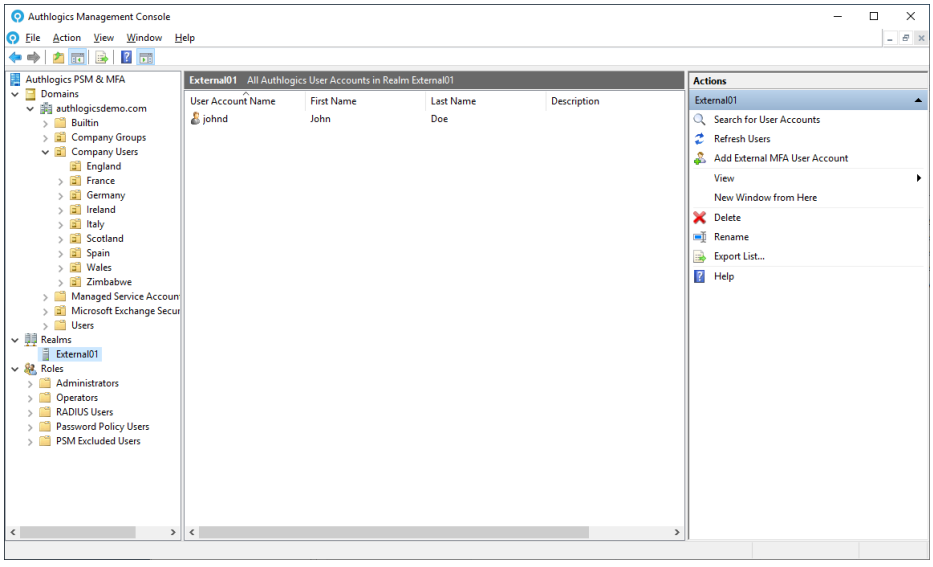
9. Click *Next*.



10. Click *Next*.



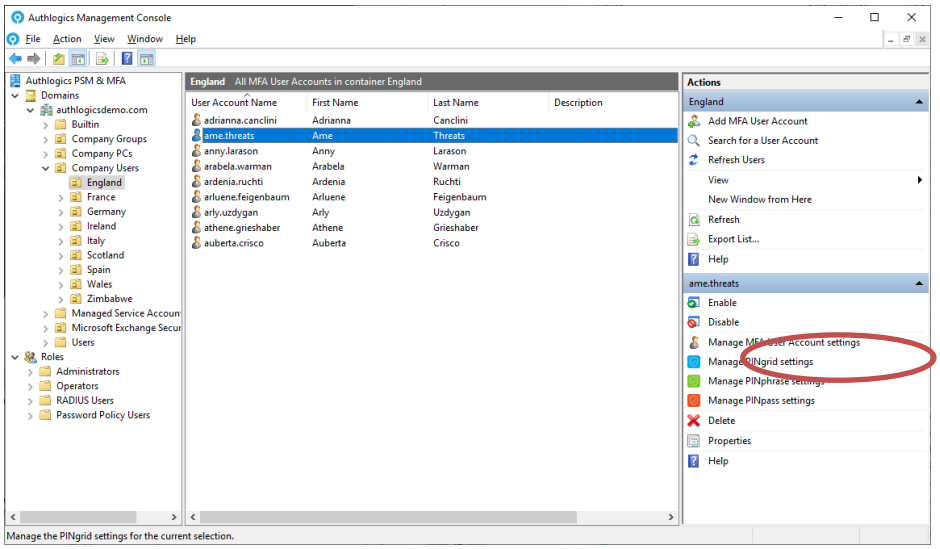
11. The New User Account has been created.
    Click *Finish*.



Setting up a user for PINgrid

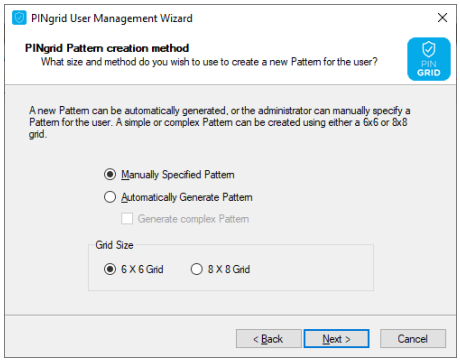
Once an Authlogics user account has been created you can configure it for use with PINgrid.

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



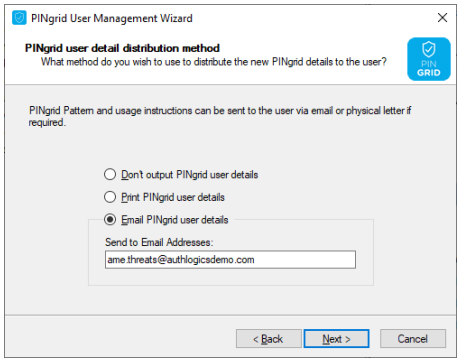
2. Click *Manage PINgrid settings* from the menu on the right or from the right-click menu to start the PINgrid User Management Wizard.

3. Click *Next*.



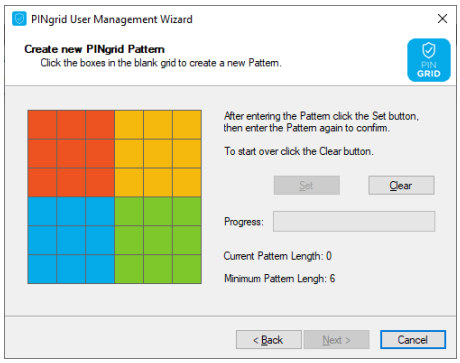
4. Users can have random PINgrid Patterns generated automatically or the administrator can choose to manually configure the user's information. By default, "simple" patterns will be generated for the user, tick the *Generate complex Pattern* box for a more secure pattern. If multiple accounts were selected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

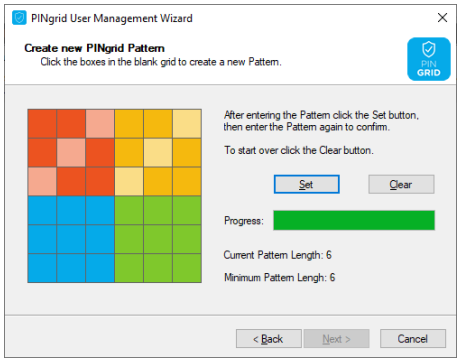


5. Select the method used to distribute the Pattern, as well as PINgrid usage instructions to the user. Auto-generated information can be either printed or emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details; this option is not available for auto-generated details. You can send the email to multiple addresses by entering multiple email addresses separated by a semi-colon ";".
   Click *Next*.

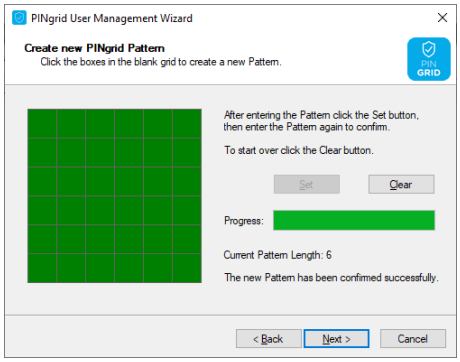
> **Note**
> For instructions on manually specifying a pattern and PIN proceed to step 6, otherwise, skip to step 9.



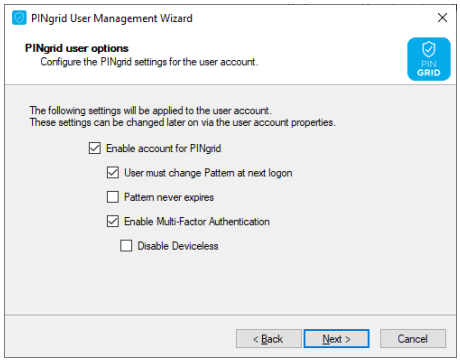
6. Enter the required pattern and click *Set*.



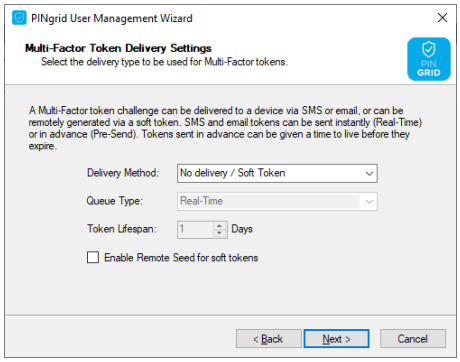
7. Confirm the Pattern entered previously.



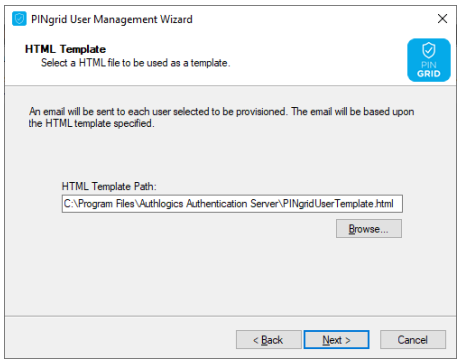
8. If the patterns match, the displayed grid will turn green. A red grid denotes a pattern mismatch. Click *Clear* to re-enter the pattern or Click *Next* to continue.



9. Configure PINgrid 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.

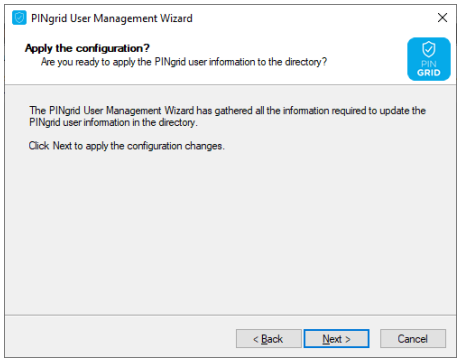


10. Select the delivery method for Multi-Factor tokens. When selecting a method, ensure that the user has either an Email address or Mobile telephone number that tokens will be delivered to.
    Queue Type determines whether tokens will be pre-sent or generated in Real-Time. When Queue Type is set to 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*.

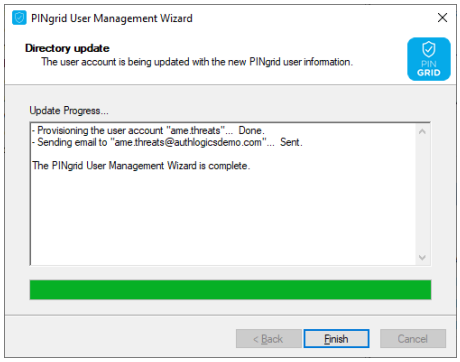


11. Specify an HTML Template Path to the automated notification letter/email each user will receive. This HTML file can be modified and customised for your organisation. Each letter/email will be customised for the user to contain their unique information by substituting HTML comment values in the template.

To locate a custom template click *Browse…* otherwise, click *Next*.



12. Click *Next*.

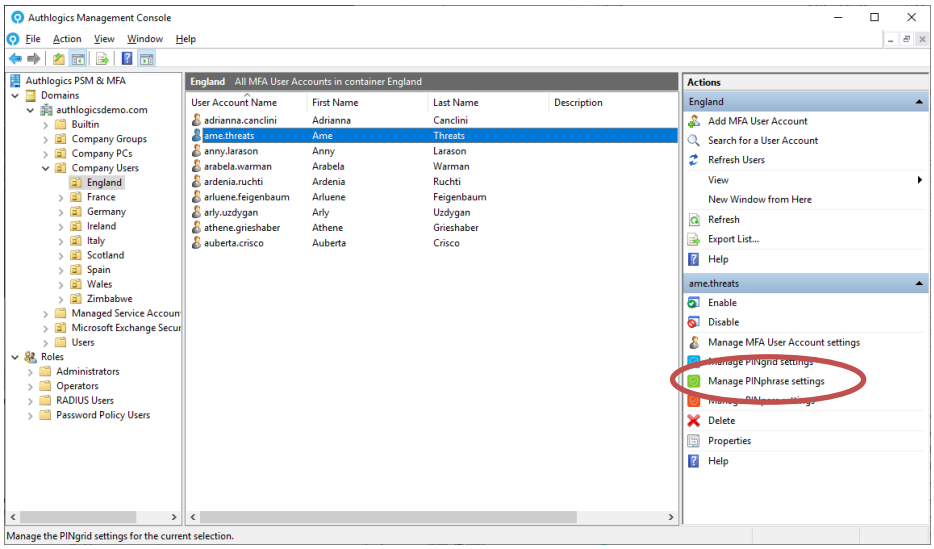


13. Click *Finish*.

Setting up a user for PINphrase

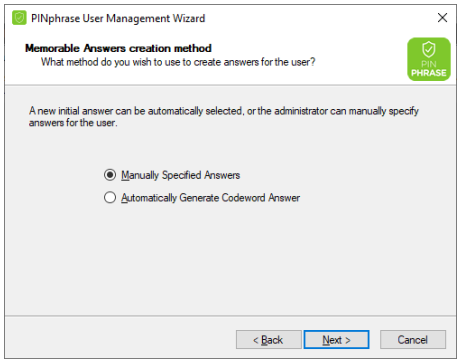
Once an Authlogics user account has been created you can configure it for use with PINphrase.

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

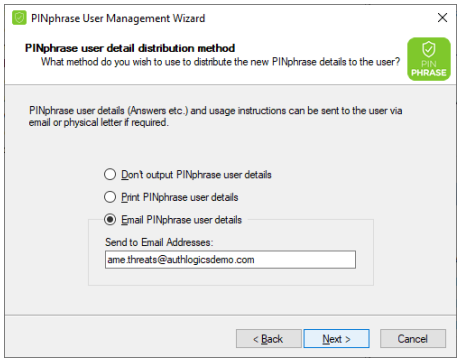


2. Click *Manage PINphrase settings* from the menu on the right or from the right-click menu to start the PINphrase User Management Wizard.

3. Click *Next*.

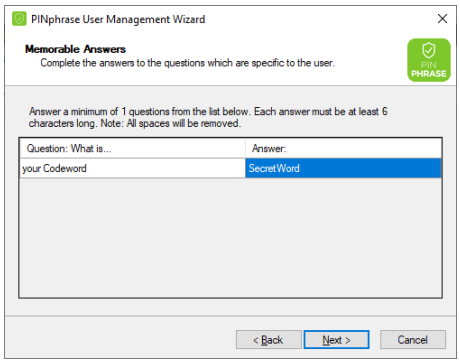


4. Users can have a randomly generated Codeword answer or the administrator can choose to manually configure the user's information. If multiple accounts were selected before starting the wizard then only the automatic option is available.
   Choose the provisioning method.
   Click *Next*.

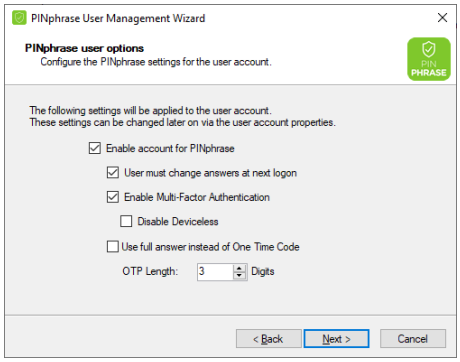


5. Select the method used to distribute the PINphrase settings as well as PINphrase usage instructions to the user. Auto-generated information can be either printed or emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details, this option is not available for auto-generated details.
   Click *Next*.

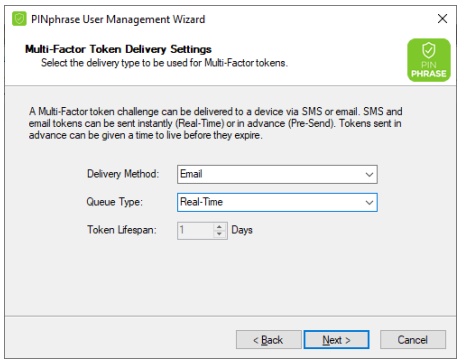
> **Note**
> For instructions on manually specifying a pattern and PIN proceed to step 6, otherwise, skip to step 7.



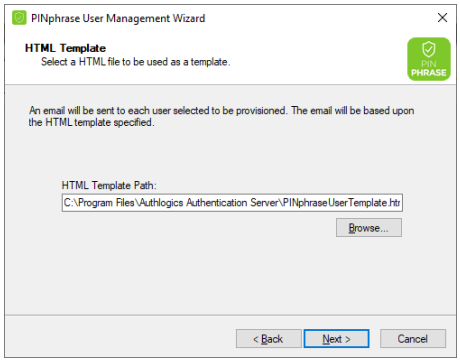
6. Enter answers for the questions ensuring that each answer is at least the minimum number of prescribed characters and that enough questions have been answered. When all PINphrase conditions have been met, the *Next* button will be available.
   Click *Next*.



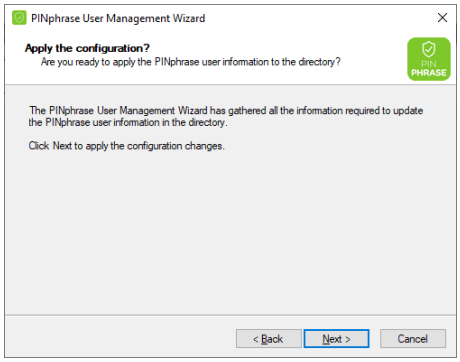
7. Configure PINphrase user options.
   An account can be set so that the next time the user logins with this account, that user will be forced to change the answers at the next logon.
   In MFA deployments, you can enable and enforce the user account to use a Multi-Factor device by selecting the *Disable 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*.



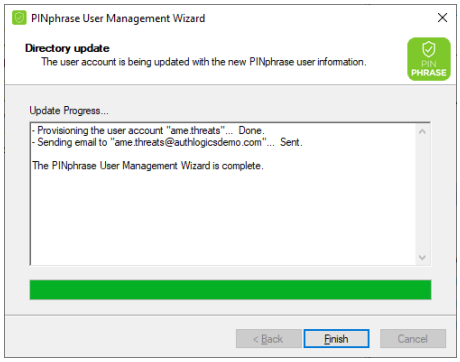
8. Select the delivery method for Multi-Factor tokens. When selecting a method, ensure that the user has either an Email address or Mobile telephone number that tokens will be delivered to.
   Queue Type determines whether tokens will be pre-sent or generated in Real-Time. When Queue Type is set to Pre-Send, an administrator must then specify the Token Lifespan for these token types.
   Click *Next*



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.



10. Click *Next* to apply the configuration changes.

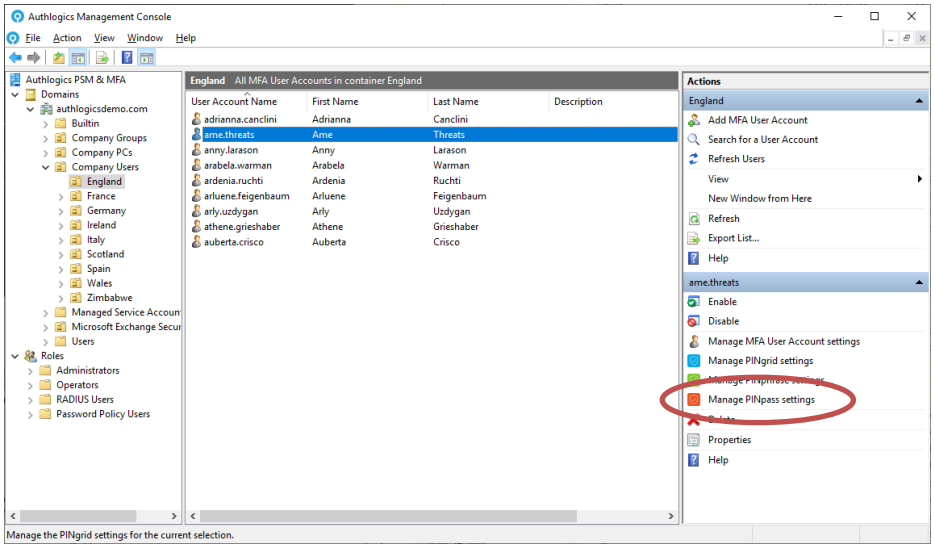


11. Click *Finish*.

Setting up a user for PINpass

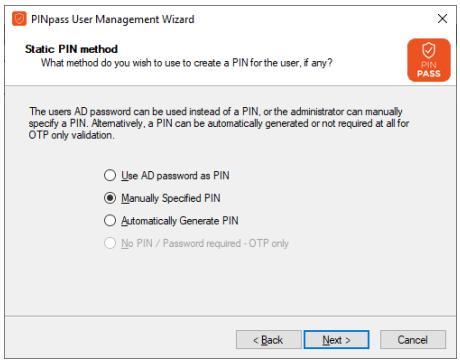
Once an Authlogics user account has been created you can configure it for use with PINpass.

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

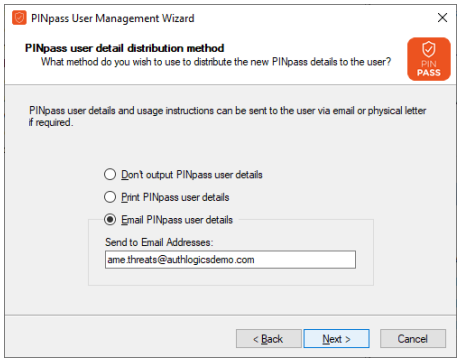


2. Click *Manage PINpass settings* from the menu on the right or from the right-click menu to start the PINpass User Management Wizard.

3. Click *Next*.

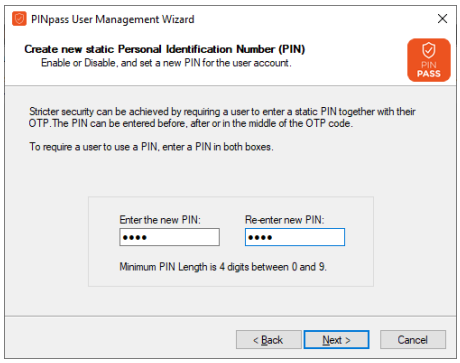


4. The user's AD password can be used instead of a PIN, or the administrator can manually specify a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation. If multiple accounts were selected before starting the wizard then the *Manually Specified* option is not available.
   Click Next.

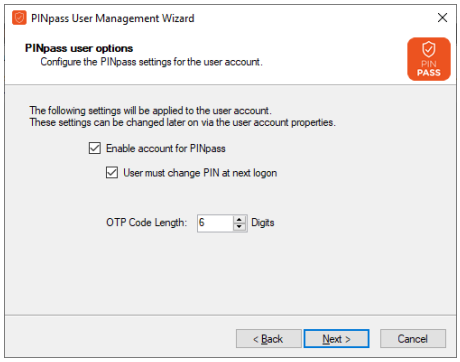


5. Select the method used to distribute the PINpass settings as well as PINpass usage instructions to the user. Auto-generated information can be either printed or emailed to the user. Additionally, if manually specified settings are provided then you can also specify not to output any details, this option is not available for auto-generated details.
   Click *Next*.

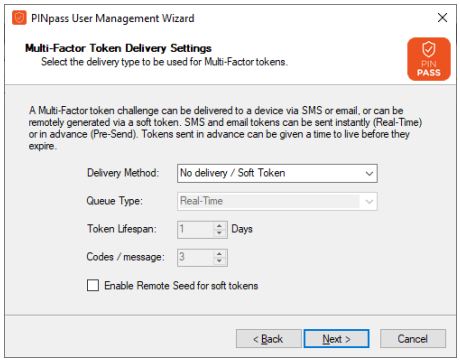
> **Note**
> For instructions on manually specifying a PIN proceed to step 6, otherwise, skip to step 7.



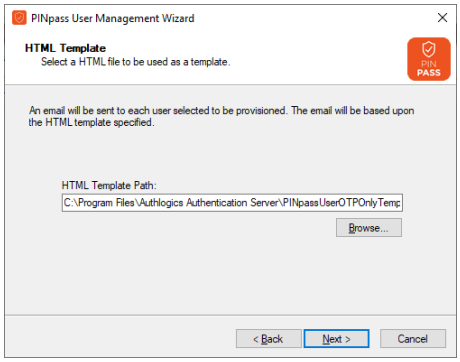
6. Enter the user's PIN and confirm the PIN. Click *Next*.



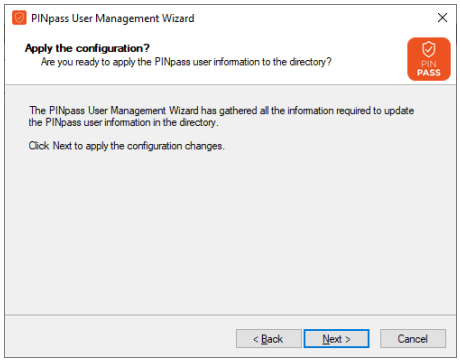
7. Configure PINpass user options.
   An account can be set so that the next time the user logins with this account, that user will be forced to change the PIN at the next logon.
   Set the *OTP Code Length* for the number of characters.
   Click *Next*.



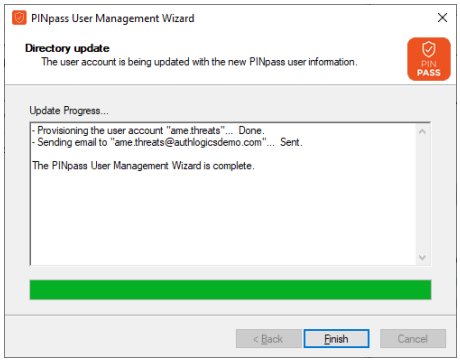
8. Select the delivery method for Multi-Factor tokens. When selecting a method, ensure that the user has either an Email address or Mobile telephone number that tokens will be delivered to.
   Queue Type determines whether tokens will be pre-sent or generated in Real-Time. When Queue Type is set to Pre-Send, 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.



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.



10. Click *Next* to apply the configuration changes.

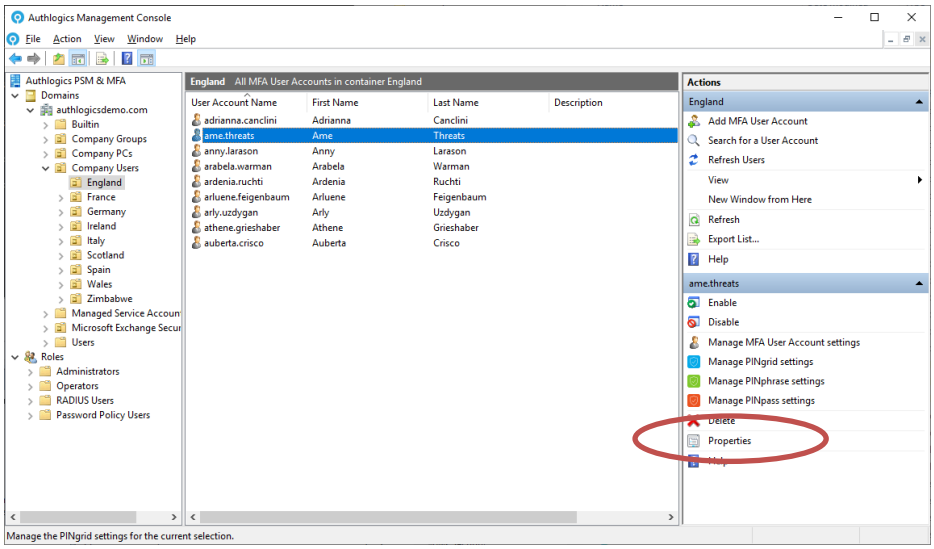


11. Click *Finish*.

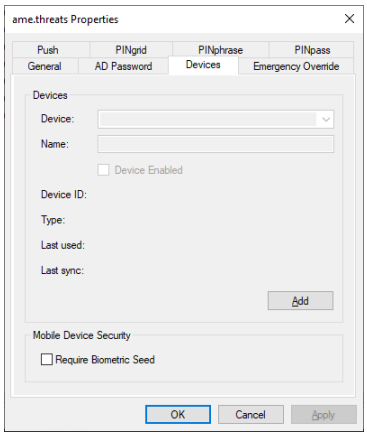
Assigning a Multi-Factor Device to a user account

In most scenarios a user will enrol their MFA device via the self-service portal, however, in some situations, it may be required for an administrator to manually add a device.

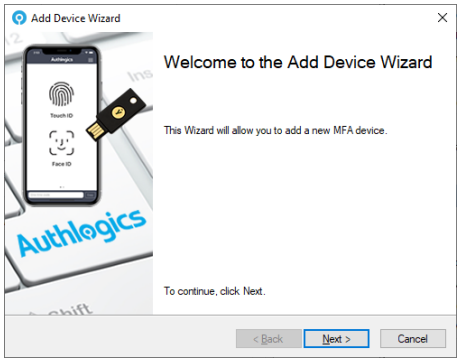
1. Expand the Domain and select the appropriate OU and user account to manage.



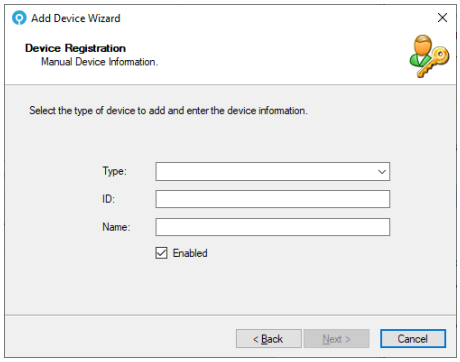
2. Click *Properties* and select the *Devices* tab.



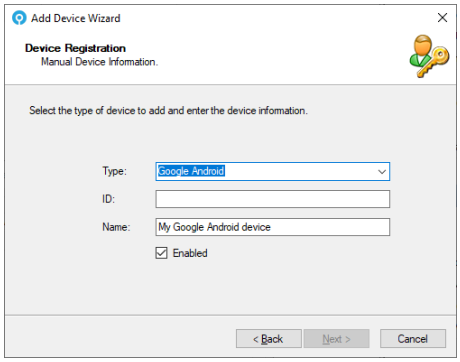
3. Click Add to start the *Add Device Wizard*.



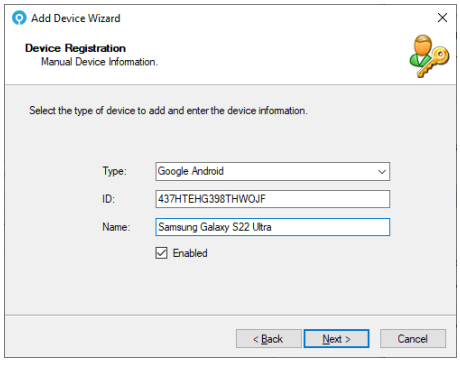
4. Click *Next*.



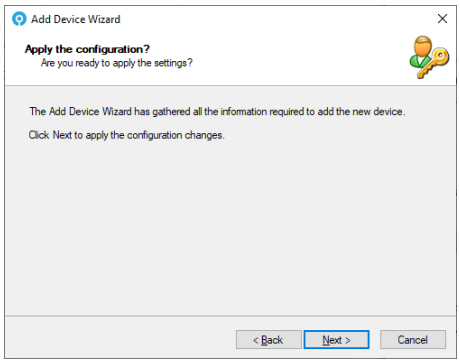
5. Select the type of device to add from the dropdown list



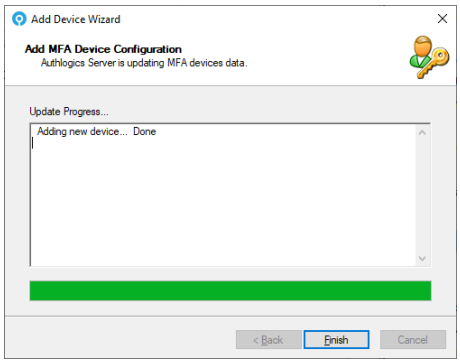
6. Enter the Device ID information from the Authlogics Authenticator App and customise the name as required.



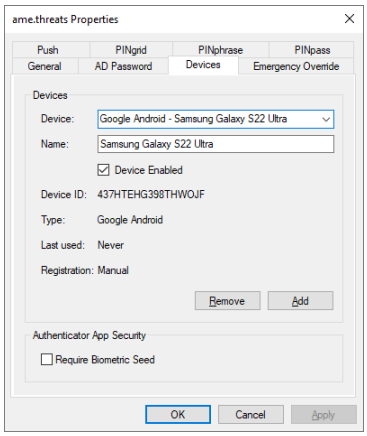
7. Click *Next*.



8. Click *Next*.



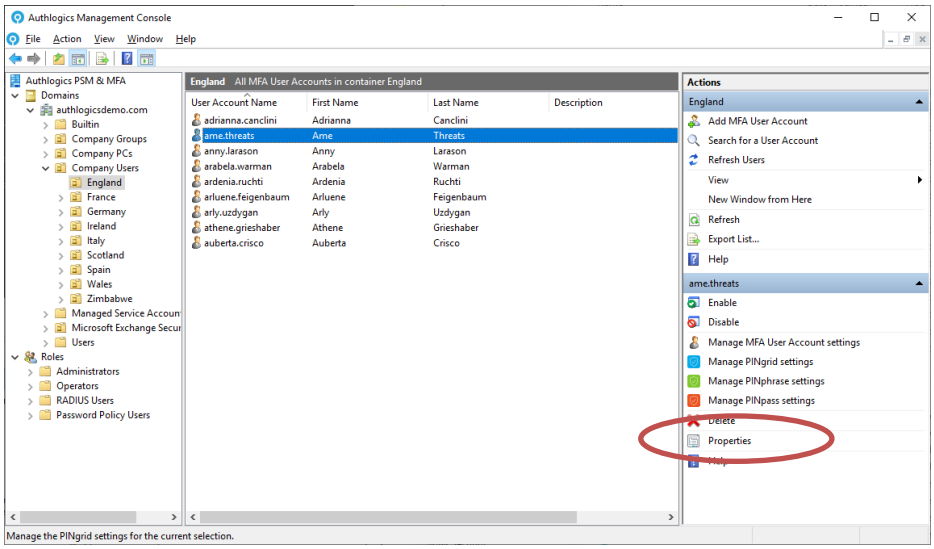
9. Click *Finish*.



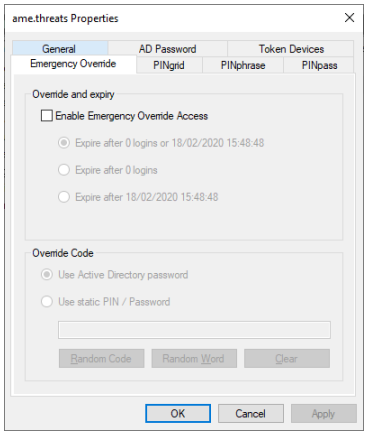
Up to 10 devices can be added for each user, repeat the process for each MFA device. Each device can be enabled or disabled as needed, e.g. it if is temporarily misplaced.

Assigning Emergency Override Access to a user (MMC)

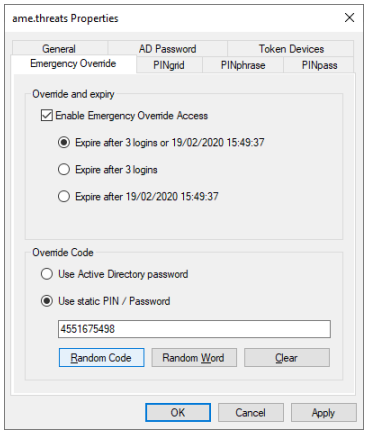
1. Ensure that Allow *Emergency Override Access* is ticked on the global settings *General* tab. See the Global Settings Walkthrough section for further information.



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.



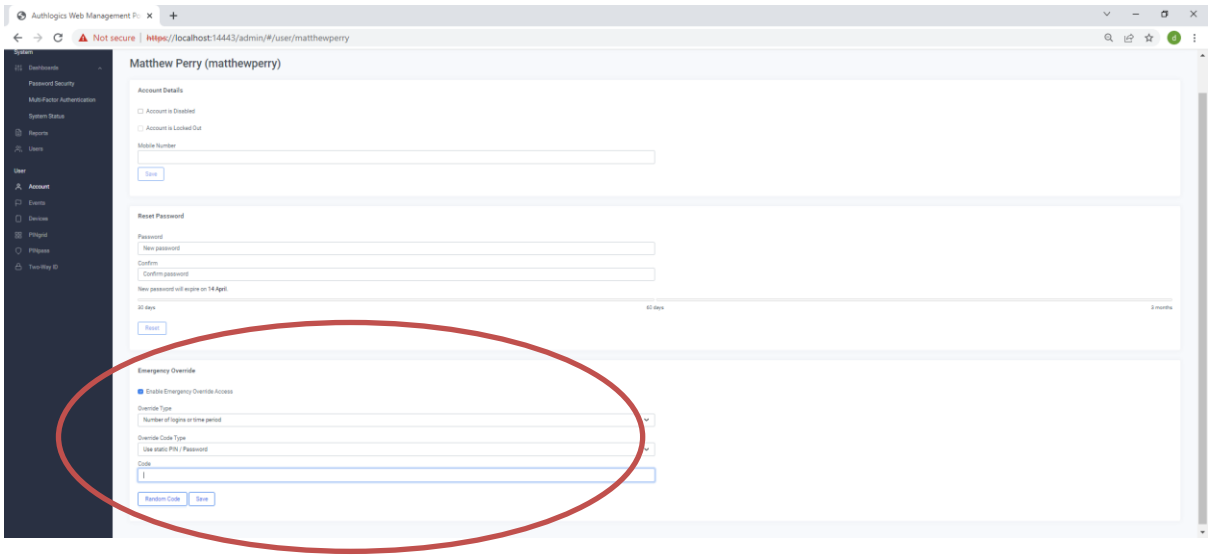
3. Tick the Enable Emergency Override Access box.
   Select under which circumstances the emergency override functionally will be automatically disabled. Options include at a specific date and time, after a specific number of uses or both; the default is both.
   Configure the user to utilise their existing 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.



4. Click *Apply* or *OK* to save the configured settings for the user account.

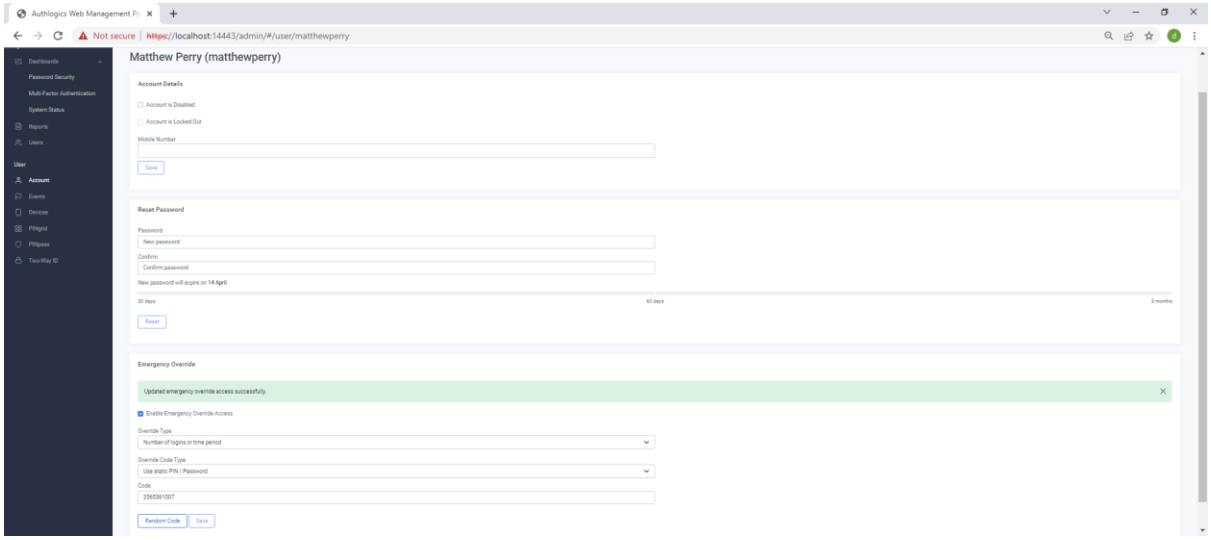
Assigning Emergency Override Access to a user (Web Management Portal)

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.



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.

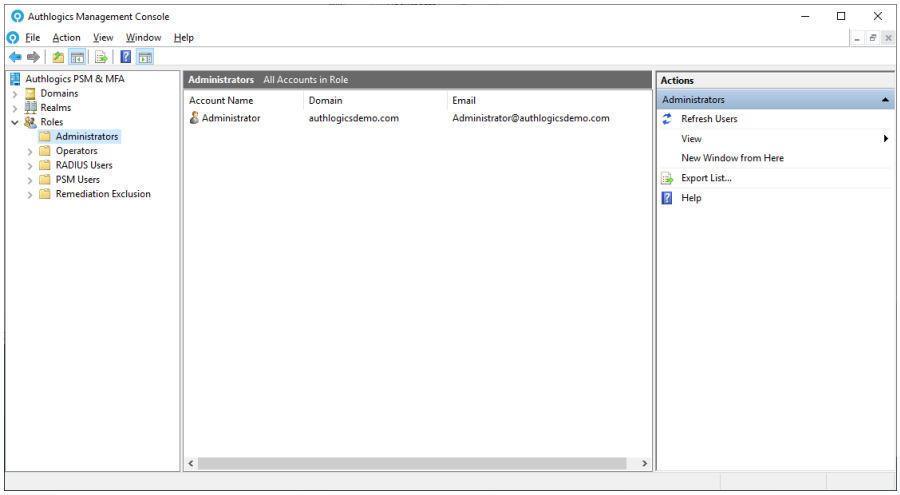


6. Click Save when done.

Roles

Authlogics Authentication Server provides administrators with the ability to assign rights to users for Authlogics administrative functions and product features. Users can be designated as Administrators and Operators.

Administrators can fully administer Authlogics via the Authlogics 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 Authlogics Management Console.



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 Authlogics 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 Authlogics 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

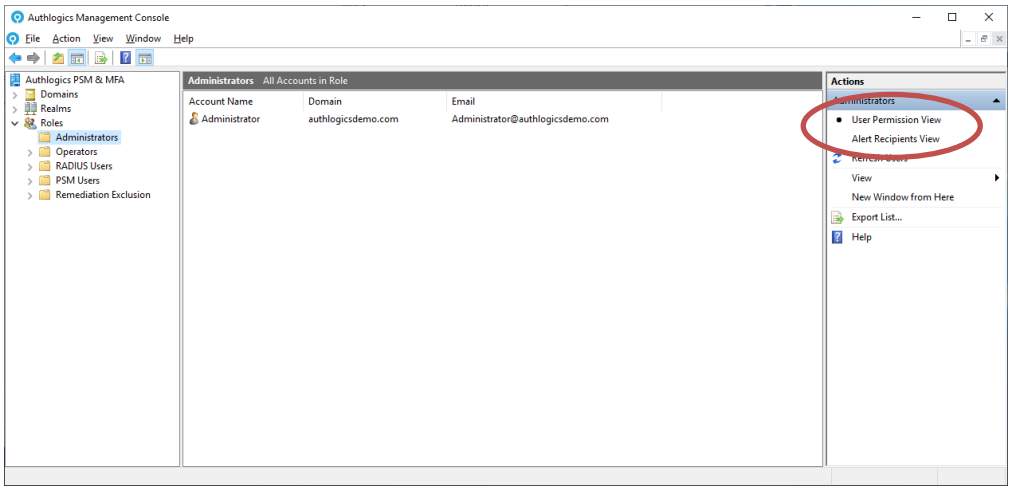
The Authlogics Administrator Role is dual purposes and thus has two views:

1. **User Permissions View**: User accounts that have Authlogics Administrative permissions.
2. **Alert Recipients View**: Email addresses that should receive Admin Alerts.

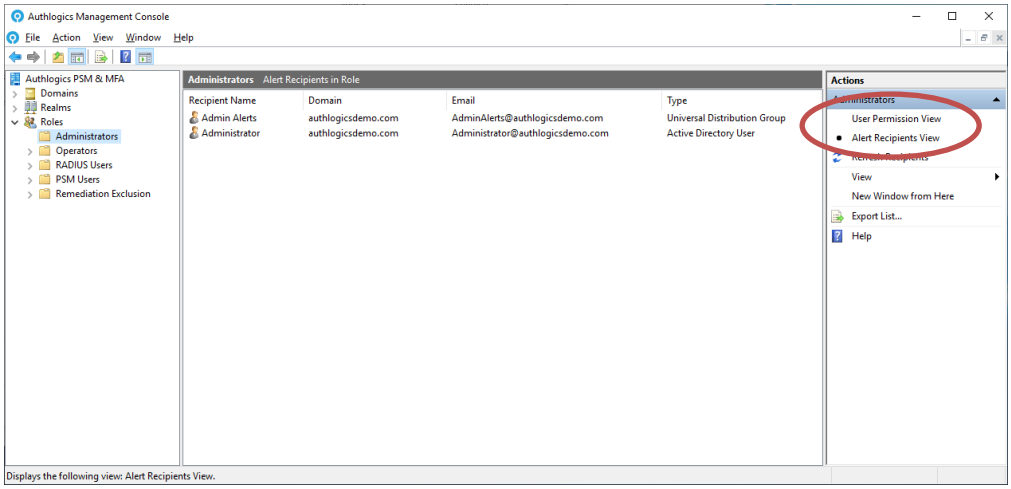
The views can be toggled on the Actions pane in the MMC which allows you to determine the resultant set of users in each use case. To achieve this the members of the Authlogics Administrators group are processed differently as needed.

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 Authlogics 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.



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.



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.

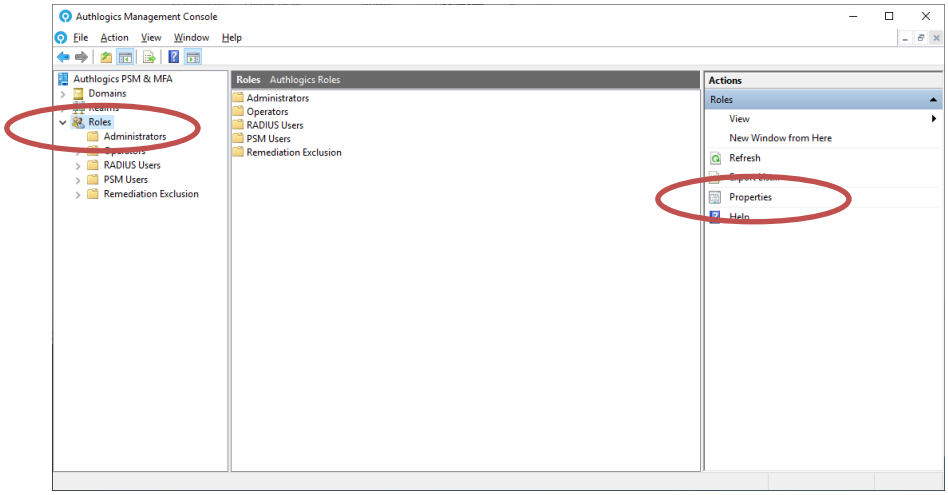
When using Microsoft Exchange, create a Mail Enabled Distribution group, add the non-admin user accounts to it, then add the group to the Authlogics Administrators group. Authlogics will then send Admin Alerts to the group and not directly to the member.

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.

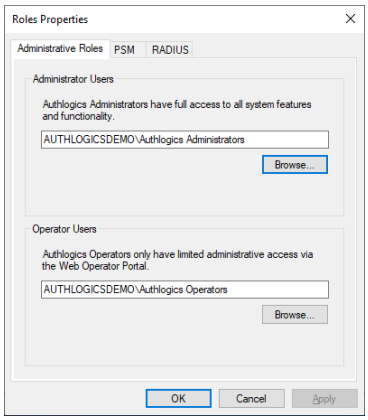
Role members cannot be added and removed via the Authlogics Management Console, this must be done by editing the appropriate Windows group either via the *Active Directory Users and Computers* MMC, or the *Local Users and Groups* MMC.

1. Open the Authlogics Authentication Server Management Console then expand Roles.

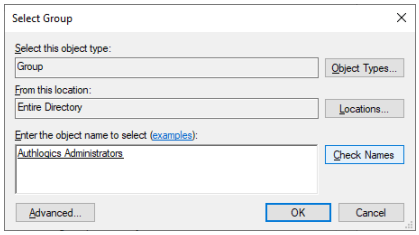


2. To assign Active Directory groups to Authlogics roles, select Roles and click *Properties*.

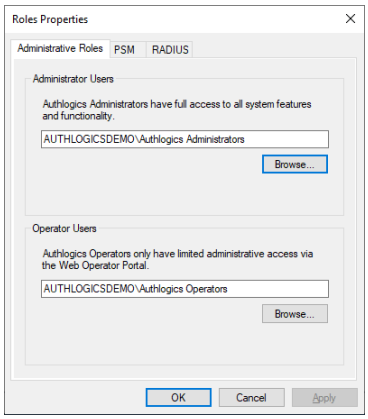
> **Note**
> The Active Directory groups must already exist in the domain.
> Authlogics Admin groups are created during setup.



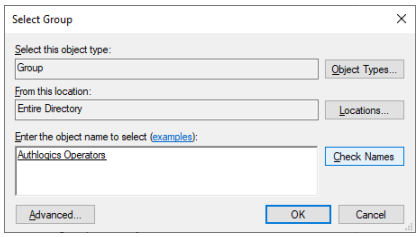
3. To select Administrators, Click *Browse…* in the Administrators Group section.



4. Locate the Active Directory group and click *OK*.



5. To select Operators, Click *Browse…* in the Operator Group section.



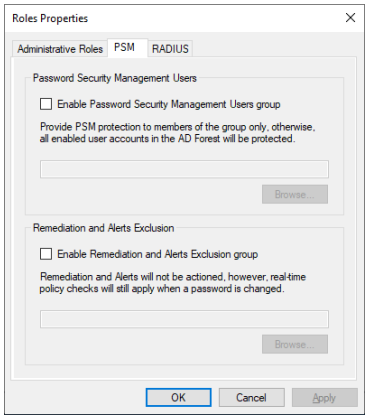
6. Locate the Active Directory group and click *OK*.

Managing the Password Security Management Users Role

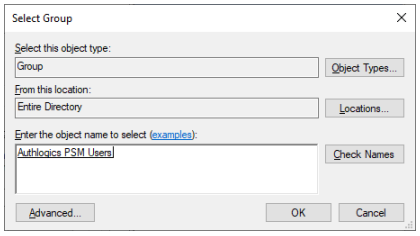
1. To assign Active Directory groups to Authlogics roles, select Roles and click *Properties*.

> **Note**
> The Active Directory groups must already exist in the domain.
> Default PSM groups are NOT created during setup.

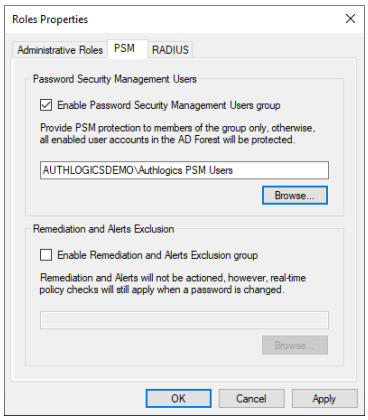
2. Select the *PSM Filters* tab.



3. Check the Enable Password Security Management Users group box and click Browse…



4. Locate the Active Directory Password Policy group and click *OK*.



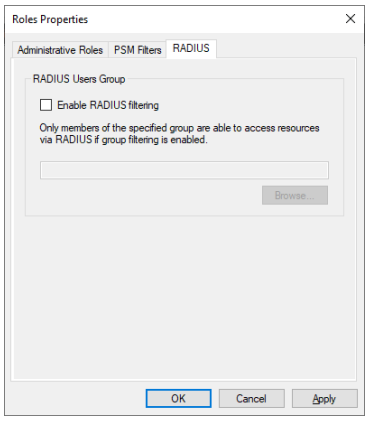
5. Click *OK*.

6. Select / Refresh the *PSM Users* role to view the members.

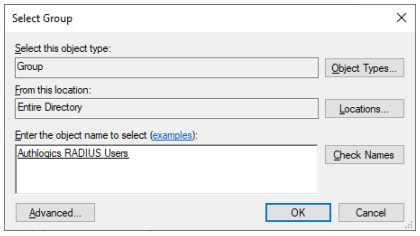
Managing the RADIUS Users Role

1. To assign Active Directory groups to Authlogics roles, select Roles and click *Properties*.

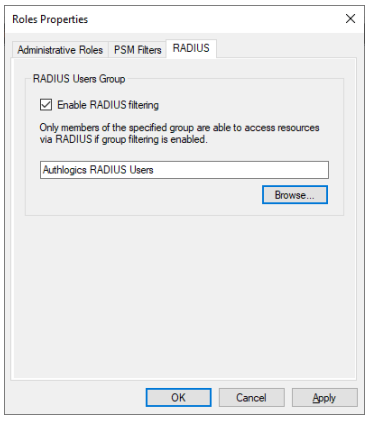
> **Note**
> The Active Directory groups must already exist in the domain.
> A default RADIUS group is NOT created during setup.



2. Select the *RADIUS* tab.
3. Check the *Enable RADIUS filtering* box and click Browse…



4. Locate the Active Directory RADIUS group and click *OK*.

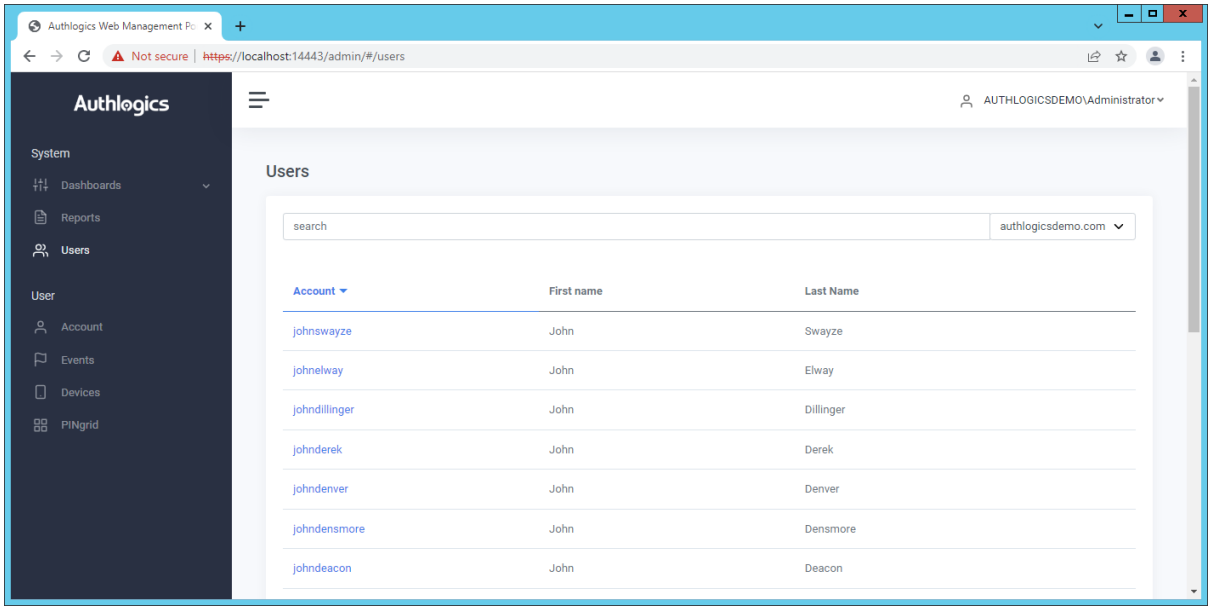


5. Click *OK*.
6. Select / Refresh the *RADIUS Users* role to view the members.

The Web Management Portal

The Authlogics 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.



Day to day user management functions available via the Web Management Portal include:

- Enabled / Disable an account
- Unlock an account
- Update a Mobile / Cellular phone number
- Reset a password
- Configure Emergency Override Access
- Enrol MFA devices
- Access the Remote Seed value
- Configure MFA settings
- Reset a PINgrid pattern
- Reset a PINphrase answers
- Reset a PINpass 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
- Generate a new seed

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 Authlogics server for easy access. Alternatively, you can use the following URL from any remote location:

https://servername:14443/admin

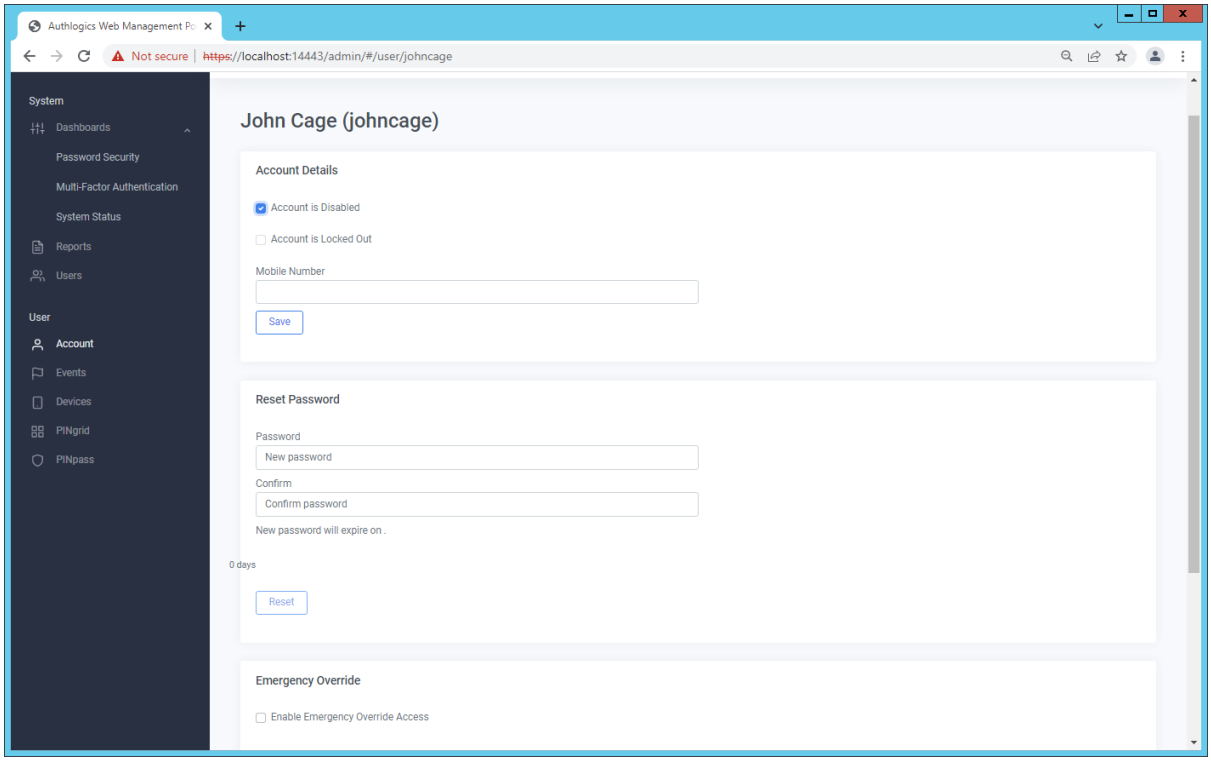
The portal can be accessed via HTTPS on port TCP:14443. The installation process configures a self-signed SSL certificate for use with the Authlogics Authentication Server, however, this certificate can be replaced with one from an internal or 3rd party trusted root when needed.

Using the Web Management Portal

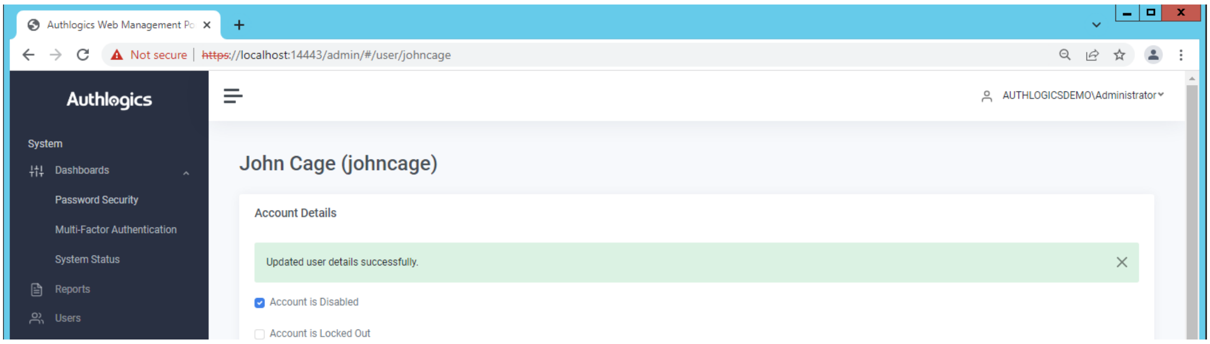
The Web Management Portal is very simple to use and very intuitive. You start by selecting the domain in the forest to administer, if there is only a single domain then it will be selected automatically.

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.



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.



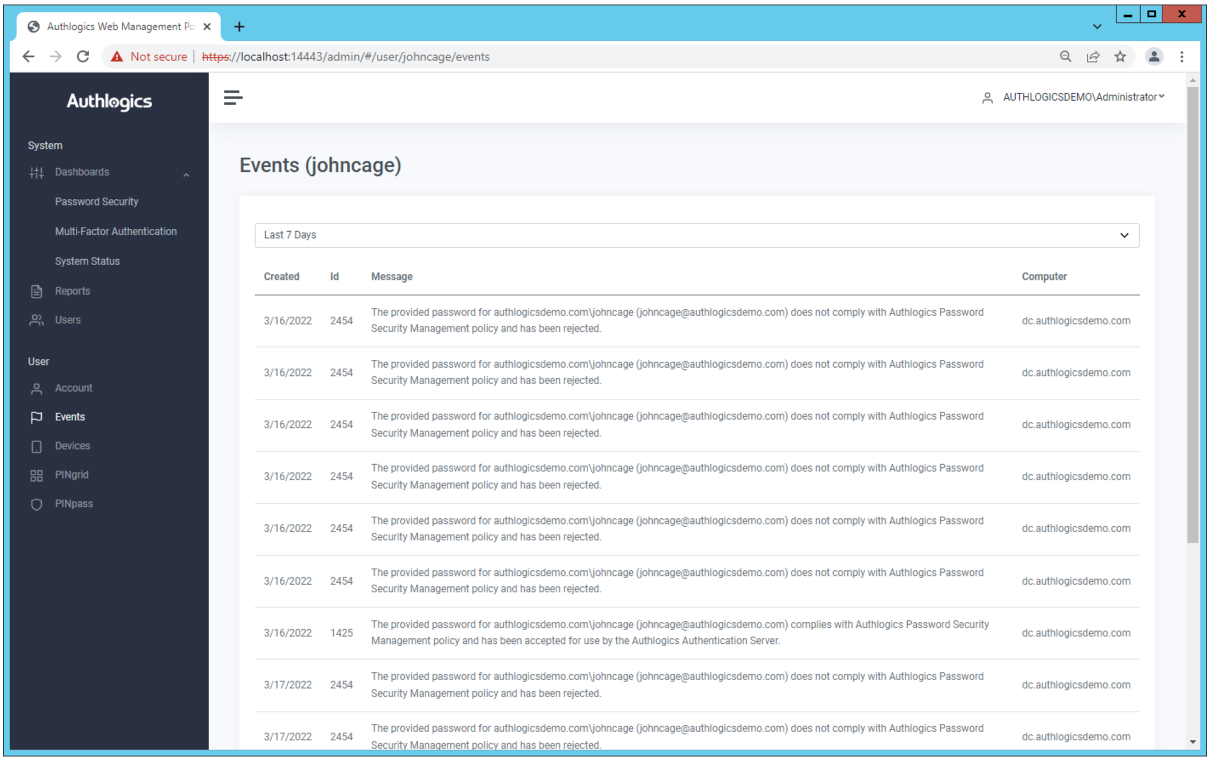
A record is kept in the Authlogics Server Application Event Log of changes made to user accounts.

Viewing all user events

Every user-related event is registered in the Windows Events log on the Authlogics Authentication Server or Domain Controller which processed the request. In environments containing multiple Authlogics 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.

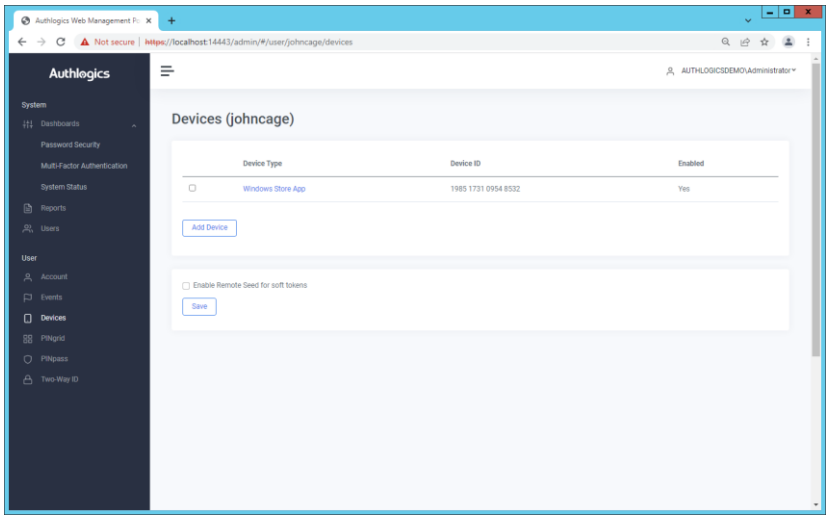
1. Select the user account to access events for
2. Select the *Events* menu item.



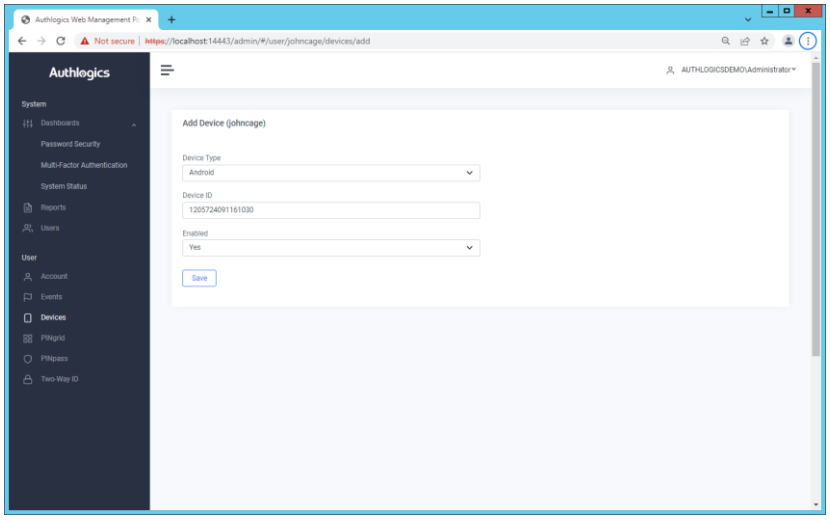
Adding a Token Device for a user account

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.

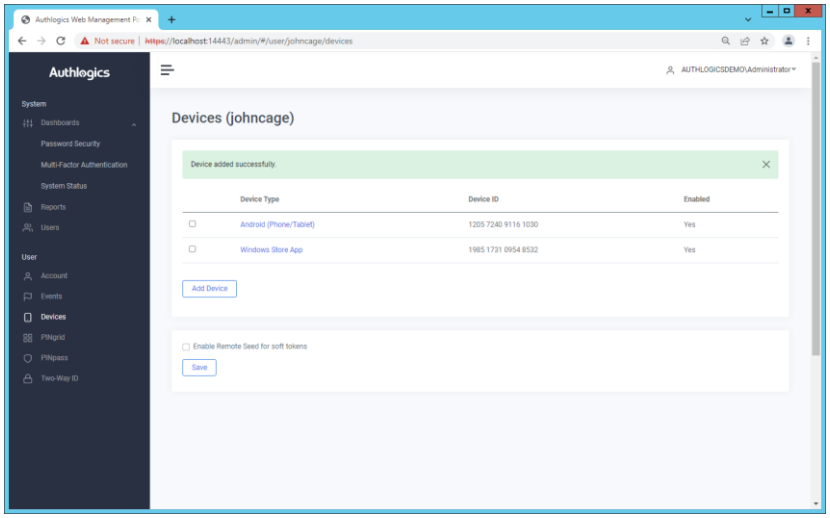
1. Select the user account to modify, then select the *Devices* tab.



2. Click Add Device.



3. Select the Device Type from the dropdown list and enter the device ID as displayed in the soft token application (available from the App store).
   Click *Save* when done.

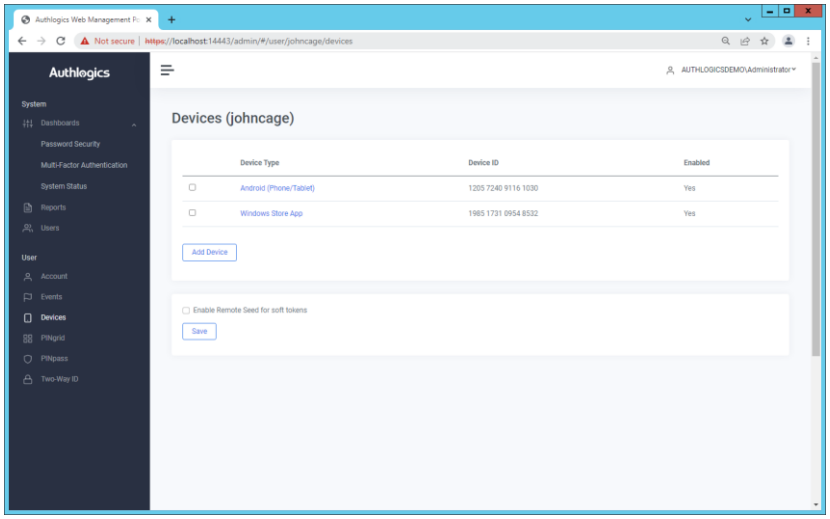


The new device is now added.

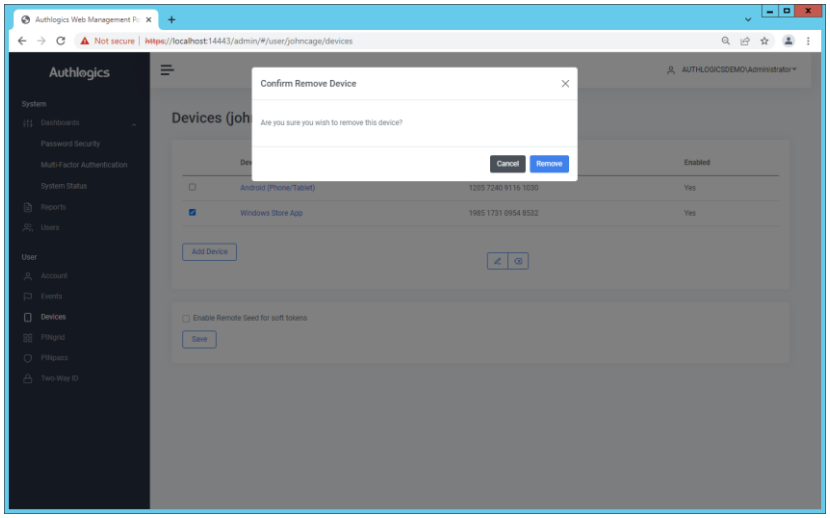
Removing a Token Device from a user account

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.

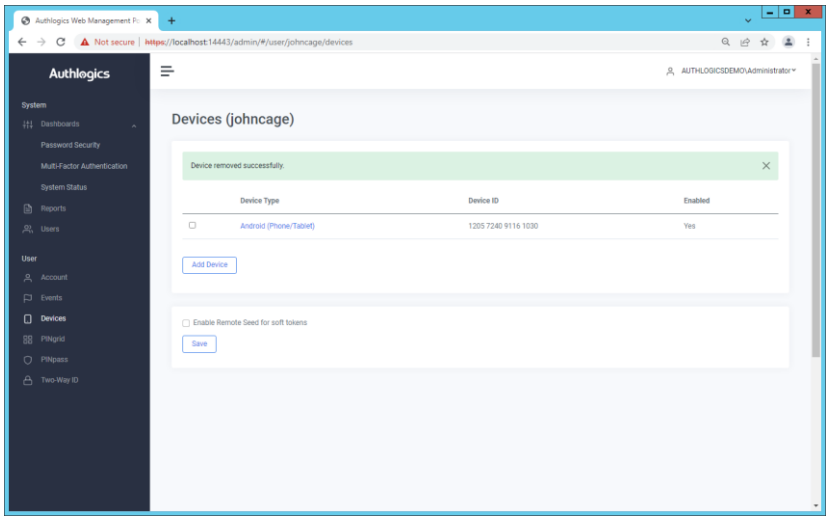
1. Select the user account to modify, then select the *Devices* tab.



2. Tick the device you wish to remove and click the *delete* button



3. Click *Remove* to confirm the removal or *Cancel* to cancel the removal.



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.

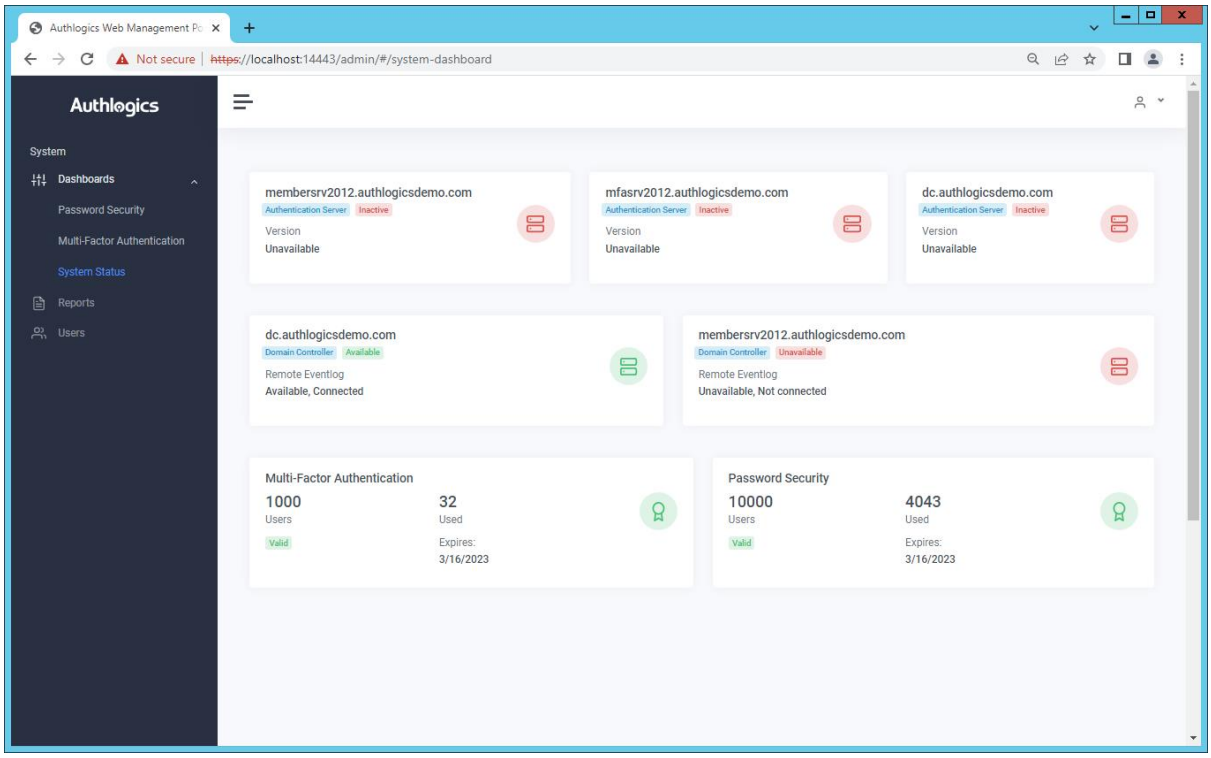
The Dashboard is broken into 3 categories; System Status, Password Security and Multi-Factor Authentication. The later 2 options will be available based on the applied MFA and PSM licences.

System Status

The System Status area of the Dashboards show all the Authlogics Authentication servers, Domain Controllers and applied Licences through the deployment.

Server listing shows the role of the server in the environment i.e. Authlogics Authentication Server and/or Domain Controller, the server's availability state and will also list Authlogics'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.



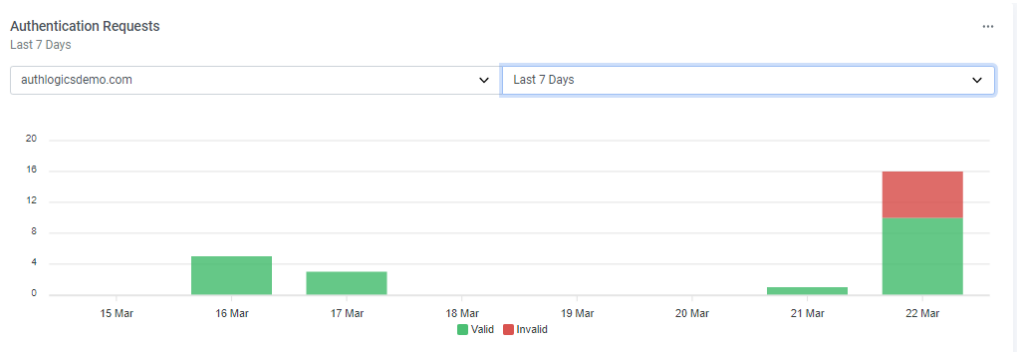
Multi-Factor Authentication

The Multi-Factor Authentication Dashboard shows a near-live view of:

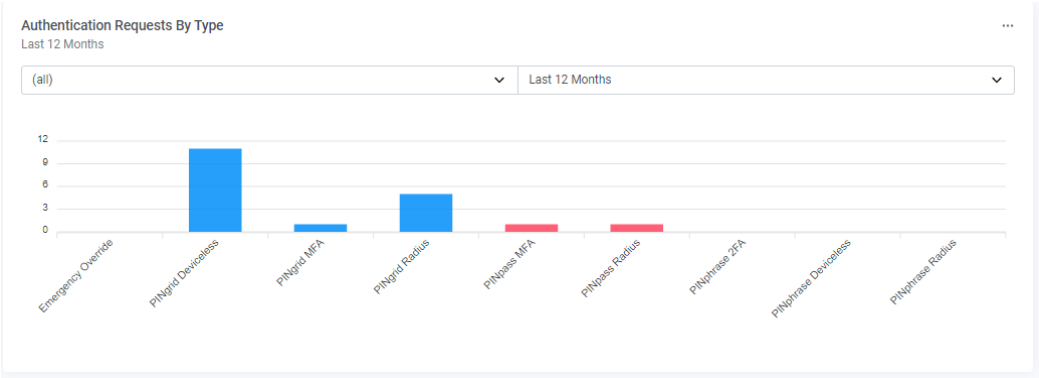
- Authentication Requests
- Authentication Request By Type
- Users By Authentication Type
- Users By Device

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.

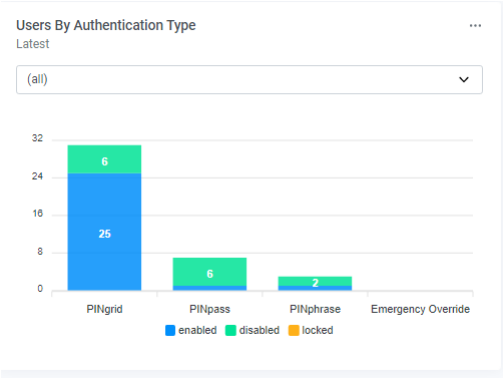
Authentication Requests module shows all valid and invalid MFA authentication requests over the selected period.



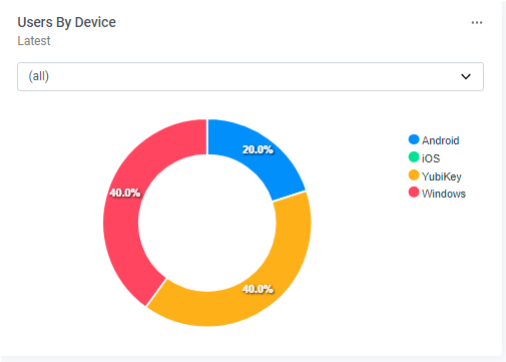
Authentication Requests By Type module shows the breakdown of successful authentication requests broken down by Authlogics MFA authentication type.



Users By Authentication Type module lists the total of users who have been provisioned to an Authlogics MFA authentication type.



Users By Device module lists the percentage of the device type which has been provisioned to users.



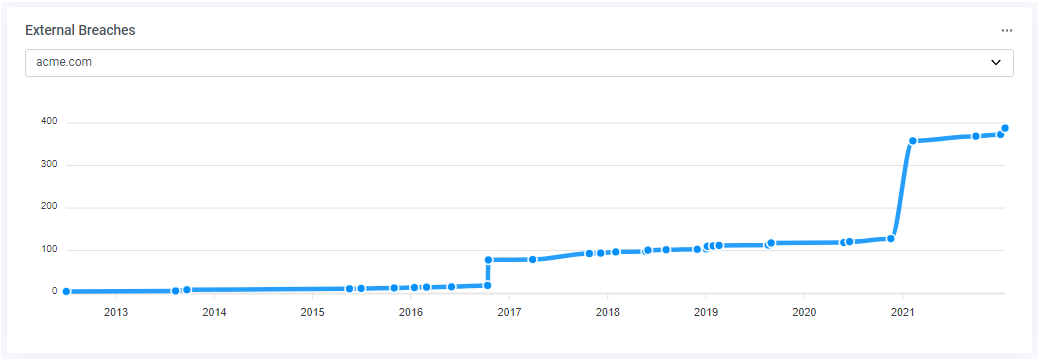
Password Security

The Password Security Dashboard shows a near-live view of:

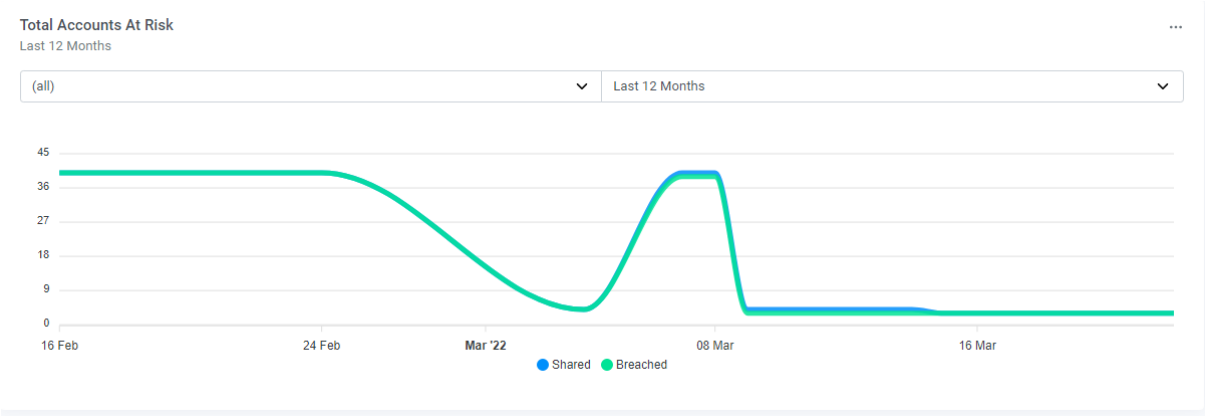
- External Breaches
- Total Accounts at Risk
- Failed Password Changes
- Users Accounts at Risk

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.

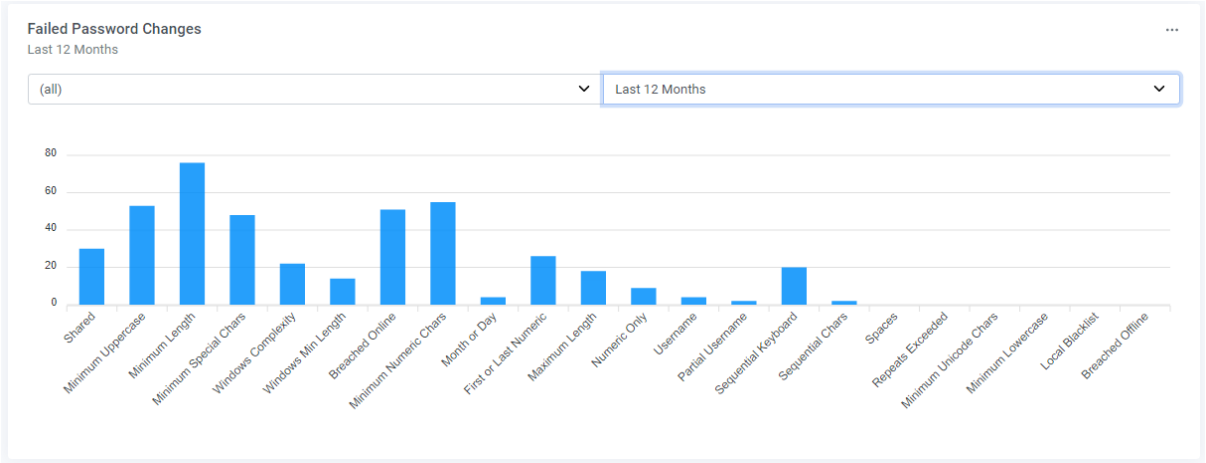
External Breaches module shows the breaches for the organisation as per the Authlogics Password Breach database.



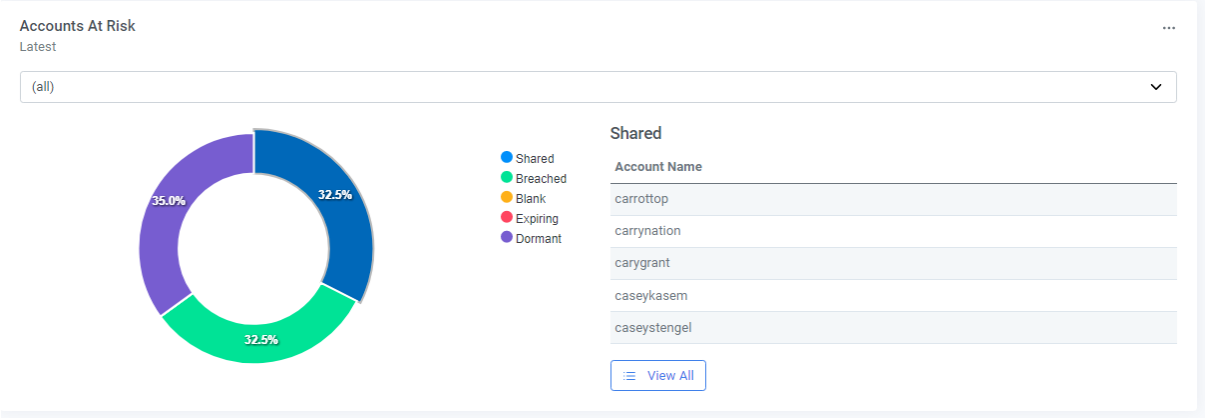
Total Accounts At Risk Breaches module shows the number of accounts using breached or shared passwords as detected over the specified period.



Failed Password Changes module shows the failed password changes and the reason for the password rejection over the selected time period.



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.



By selecting View All, all the accounts that fall under the highlighted category will be displayed.

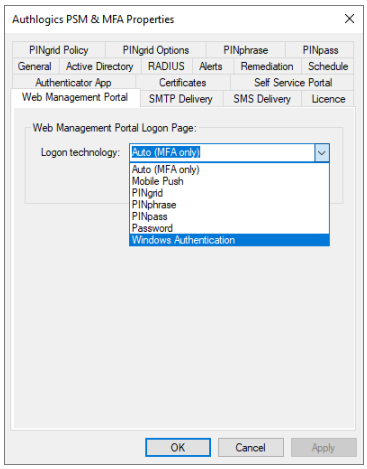
Web Portal customization

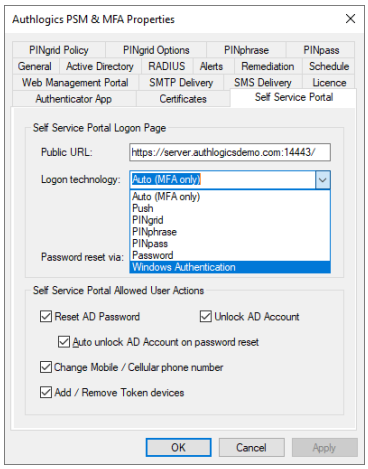
Authentication setting (Windows vs. Forms)

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 PINgrid, PINphrase, PINpass 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, within the Web Portals tab of global settings on the Authlogics MMC, select either the *Self Service Portal* or the *Web Management Portal* tab, then select the required *Logon technology* from the dropdown list.





Using Deviceless OTP with Forms authentication

The PINgrid grid and PINphrase 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 *Deviceless* checkbox on global settings *Web Portals* tab next to the chosen Logon Technology 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`	`Authlogics Self Service Portal`	Any custom text
`DisplayText`	`Authlogics 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/	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	Authlogics 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\wwwroot\Assets\css\custom.css
C:\Program Files\Authlogics Authentication Server\wwwroot\Assets\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\wwwroot\Admin\static\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. Authlogics 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

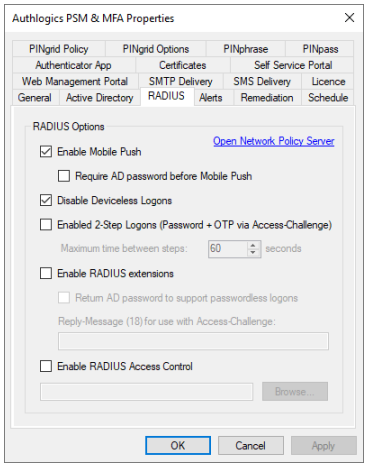
While the installer will attempt to retain your custom files, always keep a backup of your custom files to ensure they are not lost after an upgrade.

RADIUS Communication

Authlogics 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 Authlogics RADIUS server only supports PAP authentication from RADIUS client devices.

RADIUS configuration is performed via the Authlogics MMC as well as the Microsoft Network Policy Server MMC.



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 Authlogics 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

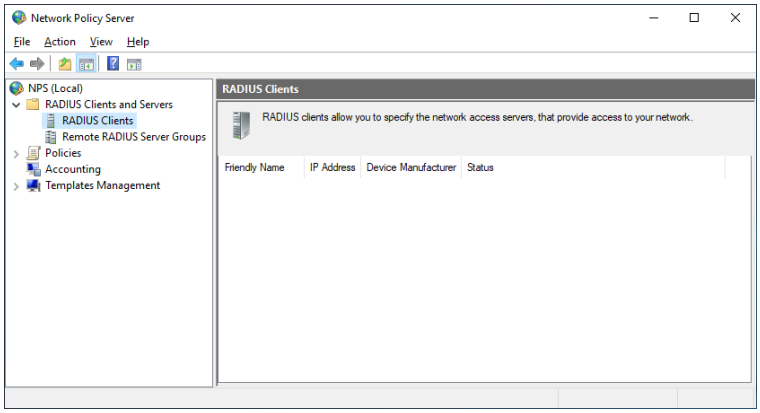
Both IPv4 and IPv6 are supported for communication with RADIUS clients.

Adding a RADIUS client

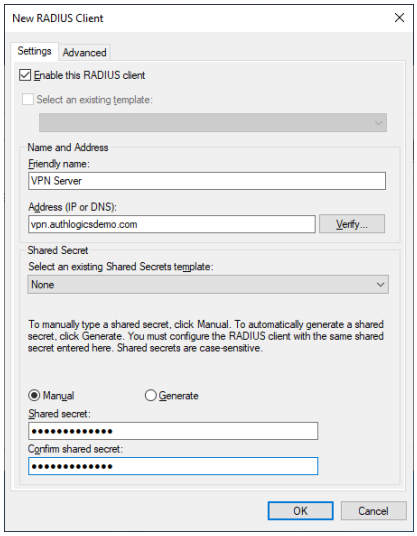
A RADIUS client device would typically be a VPN concentrator or remote access server, however, it could also be a wireless access point or a door access system. RADIUS is a common system used by a multitude of applications and platforms.

> **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.



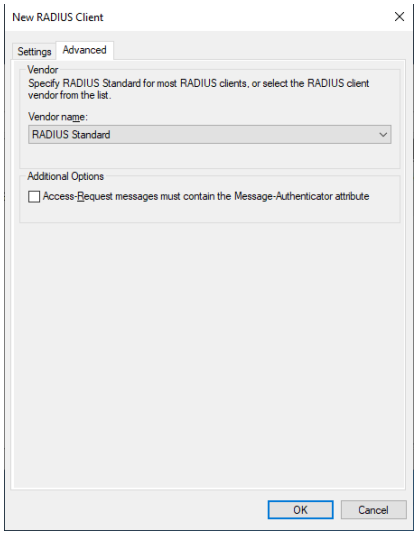
2. Select RADIUS Clients and Servers, then RADIUS Clients.
3. Right-click *RADIUS Clients* and select *New*.



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.



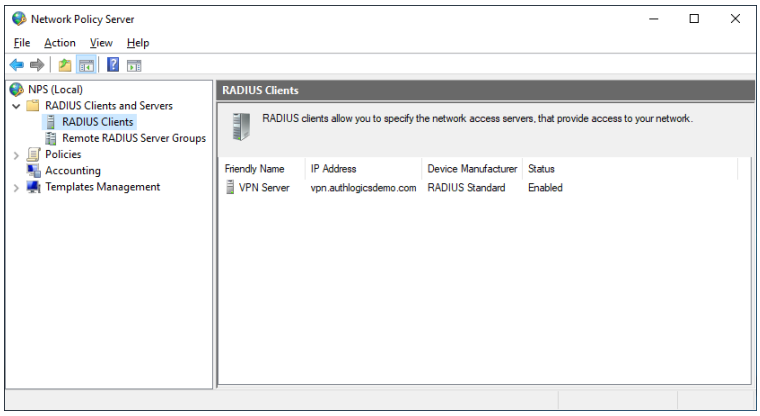
5. Select the *Advanced* tab.

   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.



You may add as many RADIUS clients as required.

RADIUS Policies

The Authlogics Authentication Server installation automatically configures a Connection Request Policy within NPS which allows Authlogics to support configured RADIUS clients automatically. A Network Policy is not required as the Authlogics 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 the PSM Password Policy

Deploying the Authlogics PSM Password Policy involves the following step:

1. Create an Authlogics PSM Password Policy in Active Directory Group Policy
2. Deploy the Domain Controller Agent
3. Group Policy changes:
    a. Assign the Authlogics Password Policy to the Domain Controllers OU
    b. Assign the Authlogics Password Policy to the Authlogics Authentication Servers group
    c. Modify the built-in *Default Domain Policy*

> **Note**
> Installing the Authlogics Domain Controller Agent does NOT modify the existing Windows password policy for the Domain.

Configuring the Authlogics Password Policy Settings

The Authlogics 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 Authlogics Password Policy applied to them. If enabled, only members of this group will have the Authlogics 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 Authlogics 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 Authlogics 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 Authlogics Password Breach Database in the Cloud consisting of billions of known previously breached passwords. If you enable this policy then no checks against the Authlogics 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 Authlogics 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 Authlogics Password Breach Database installed on the Authlogics Authentication Server. If you enable this policy then no checks against the offline Authlogics 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 Authlogics 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 Authlogics Password Breach Database. Warning: By enabling this policy the full password HASH will be sent over the Internet to Authlogics as k-Anonymity cannot be used. If you disable or do not configure this policy then heuristic scanning will not be performed with the Authlogics 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	127
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. 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 default value of 8 will be used 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 consecutively repeated 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 default value of 3 will be used 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 default value of 3 will be used 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 Authlogics 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 Authlogics 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.

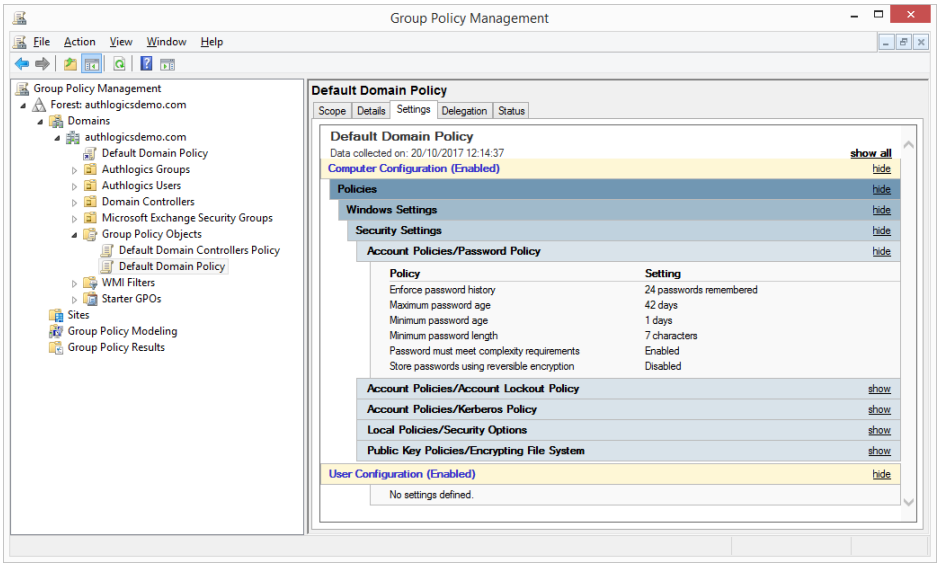
Setting	Maximum Password Age
Values	Maximum Age in days: (1 - 999)
Default	42
Description	
This policy setting configures the maximum password age for accounts that are NOT a member of the PSM Users Role. If you enable this policy you must specify the Maximum Age in days until the user account's password 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.	

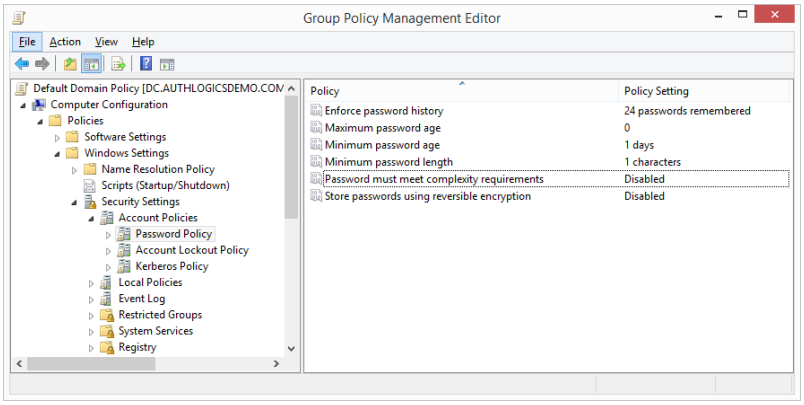
Modifying the Default Domain Policy

The following password settings apply to the Default Domain Policy by default:



The following password settings for the Default Domain Policy must be changed so that the built-in Windows policy does not conflict with the Authlogics Password Policy and NIST guidance:

- **Maximum password age: 0**
  - This should be set to 0 when Authlogics 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 Authlogics PSM "Minimum Password Length" complexity rule setting.
- **Passwords must meet complexity requirements: Disabled**
  - This should be set to Disabled to allow the Authlogics PSM policy to function or to comply with NIST SP 800-63B which states that passwords should not be forced to contain complexity rules.



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

Authlogics 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 Authlogics 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 Authlogics 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 Authlogics are controlled via the Windows registry. The following entries are created during the installation of Authlogics server components and typically most of them should only be changed if instructed by an Authlogics support engineer.

> **Note**
> After changing a registry key on the Authlogics Server the IIS components must be restarted by running `IISRESET` from an elevated admin command prompt.

Specifying Active Directory Domain Controllers

The Authlogics Authentication Server will automatically locate domain controllers as needed. In environments where network segmentation exists not all DC's may be contactable by the Authlogics 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\Authlogics Authentication Server\DomainGCs
```

Default Value: `{blank}`

Used by components: Authlogics Authentication Server; Management Console

The Authlogics 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\Authlogics Authentication Server\DomainDCs
```

Default Value: `{blank}`

Used by components: Authlogics Authentication Server; Management Console

The Authlogics 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 Authlogics 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 Authlogics 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 Authlogics agents or make use of a wide card certificate.
2. The certificate must be trusted by all systems that connect directly to the Authlogics server.
3. Using Internet Information Services (IIS) Manager, edit the HTTPS IIS bindings for the *Authlogics* 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 Authlogics 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 Authlogics Support.

Integration with external systems

Authlogics provides integration guides for various external systems which may include step-by-step instructions or custom integration components.

The Authlogics Authentication Server Developers Guide should be used when planning to programmatically access the Authlogics 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 Authlogics 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 Authlogics 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.