

Multi-Factor Authentication

Quick Start Guide

Product Version: 4.01750.0

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

Email us: sales@authlogics.com



Introduction

This guide provides an overview of the steps required to setup Authlogics Multi-Factor Authentication in a new environment. For detailed information about a specific feature or deployment scenario please see the *Authlogics Authentication Server Installation and Configuration Guide*.

Considerations

- (1) Authlogics Multi-Factor Authentication requires a Windows Server and an Active Directory domain to be available prior to installation.
- (2) A Domain Administrator / Enterprise Administrator account is required to perform the installation.
- (3) After the installation the server will require a reboot.
- (4) Internet access to https://*.authlogics.com is required.

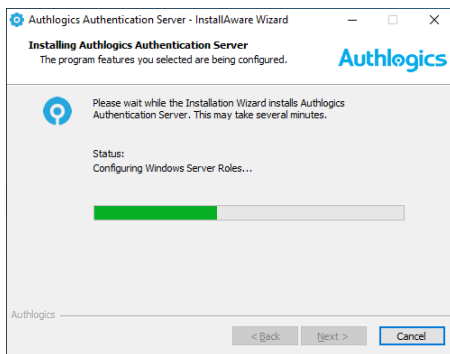
Required information

- (1) AD administrator credentials.
- (2) SMTP Server details: name, port, authentication requirements.
- (3) The DNS name for the server.
- (4) Understanding of which authentication technology to use.

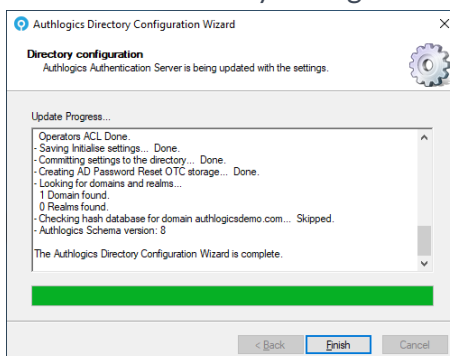


Installing the Authentication Server

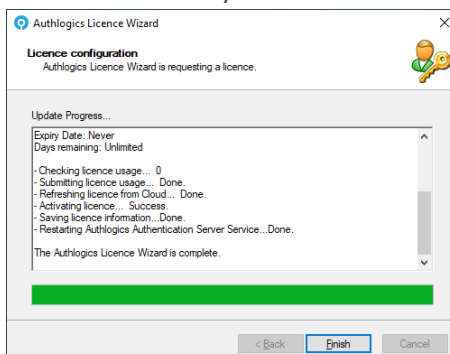
- (1) Download the Authentication Server installer from <https://authlogics.com/downloads/> and extract the ZIP.
- (2) Run the setup file in the *Install* folder.
- (3) Follow the Installation Wizard instructions to install the product binaries.



- (4) Follow the Directory Configuration Wizard to setup the AD for use with Authlogics.



- (5) Follow the Licence Wizard to configure a licence for Authlogics MFA. If you do not have a licence key the wizard can request a 30 day evaluation licence for you.



- (6) **Reboot the Server** after the Authlogics Management Console loads to complete the initial setup.

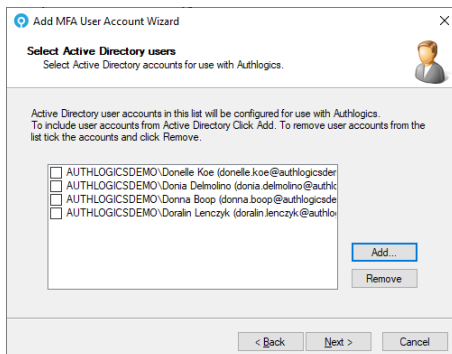


Configuring the Authentication Server

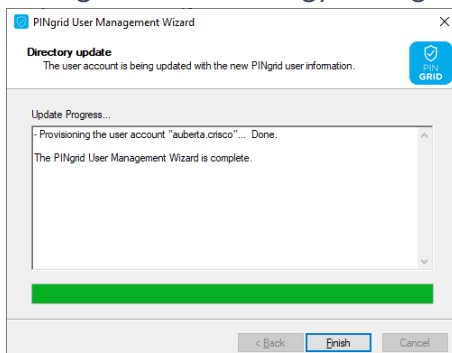
- (1) Launch the Authlogics Management Console, right click “Authlogics MFA” and select properties.
- (2) Configure the SMTP Server settings to be able to deliver alerts and new user emails.

Adding MFA Users

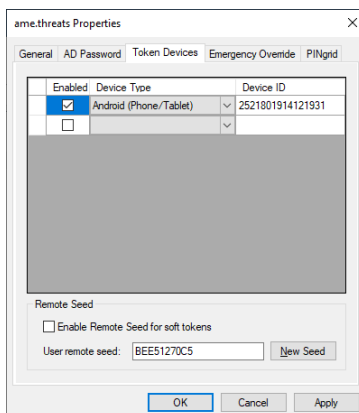
- (1) Expand domains and open the domain to add MFA users to.
- (2) Click “Add MFA User Account” from the actions on the right to start the wizard.
- (3) Select all the AD user which must be configured for MFA.



- (4) Select all the users to provision an MFA technology, e.g. PINgrid, PINpass, PINphrase, then click “Manage PINxxxx settings” to start the wizard.
- (5) Configure the technology settings for the selected users:



- (6) Double click a user account to open the account properties and add an MFA device:

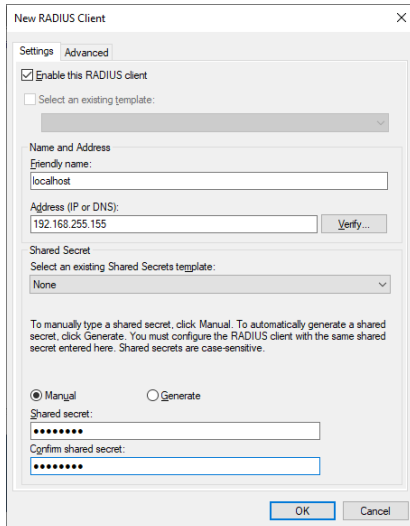


- (7) Test the user login using the Self Service Portal via <https://localhost:14443/>

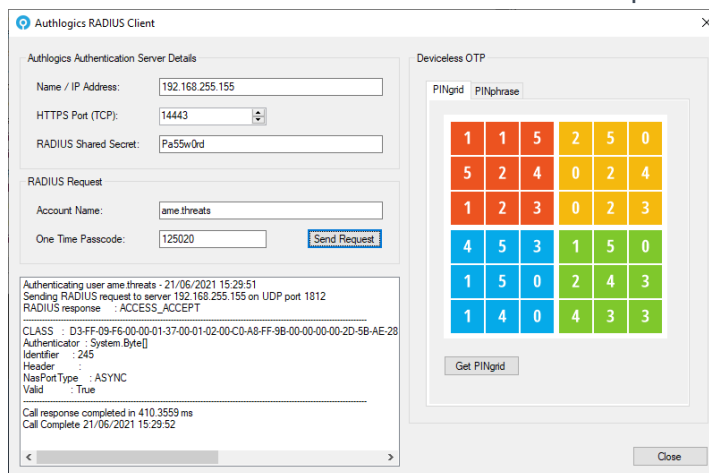


Setting up RADIUS

- (1) Launch the Authlogics Management Console, right click “Authlogics MFA” and select properties.
- (2) Configure the RADIUS settings on the RADIUS tab as required.
- (3) Click the “Open Network Policy Server” and add the local server as a RADIUS client using the local IP address and a shared secret.



- (4) Start the Authlogics RADIUS test client from: `C:\Program Files\Authlogics Authentication Server\ResKit\RadiusClient\Authlogics Radius Client.exe`
 - a. Enter the local server IP address and shared secret from step 3
 - b. Enter the test user account name. Click “GetPINgrid” to show a grid if PINgrid is being used.
 - c. Enter the One Time Passcode and click “Send Request”.



- d. The RADIUS result is shown.



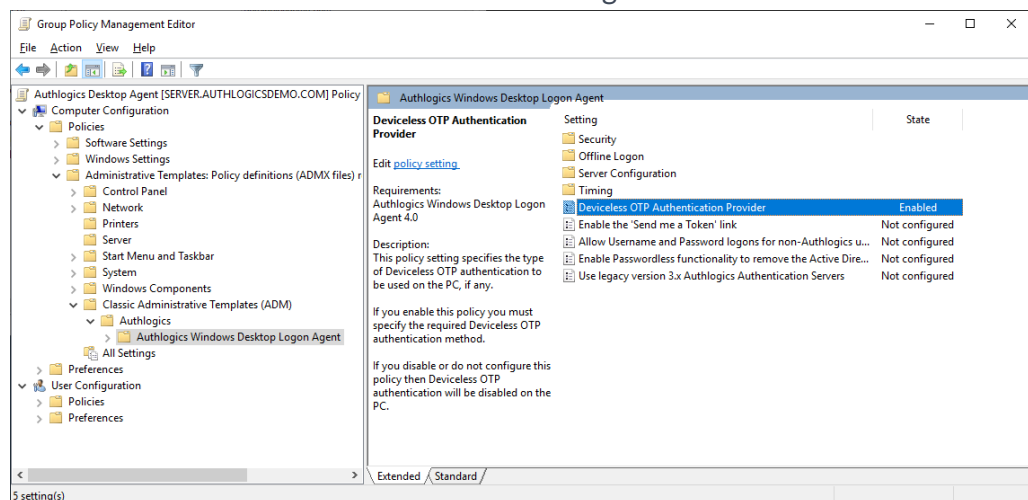
Configuring the Windows Desktop Agent

This section assumes a separate workstation test PC is being used which is domain joined.

Configuring the Windows Desktop Agent

Perform these actions on the server:

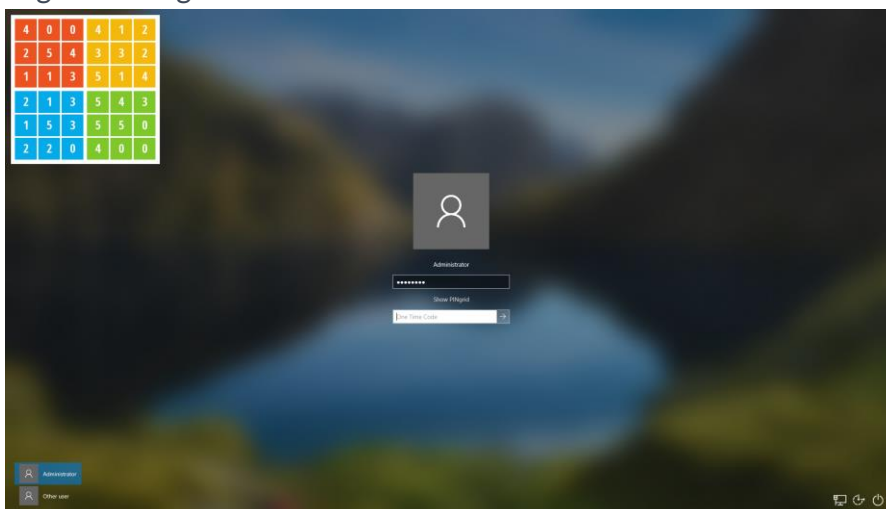
- (1) Download the Windows Desktop Agent installer from <https://authlogics.com/downloads/> and extract the ZIP.
- (2) Import the GPO\AuthlogicsWinDLA.adm file into a new Group Policy object
- (3) Configure the following settings (assuming PINgrid):
 - a. Deviceless OTP Authentication Provider: Enabled, PINgrid
 - b. Disabled Windows Username and Password logons



- (4) Apply the GPO to an OU containing the workstation computer account.

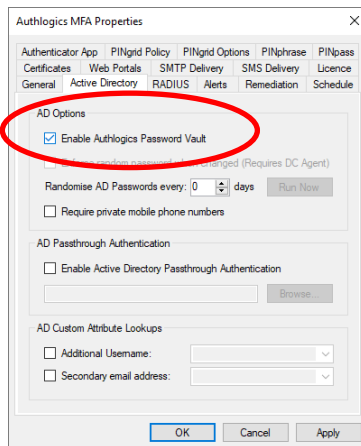
Perform these actions on the workstation:

- (1) Ensure the GPO settings are applied to the PC by running `GPUPDATE /FORCE`
- (2) Install the Agent from the install folder.
- (3) Log off and log on with MFA



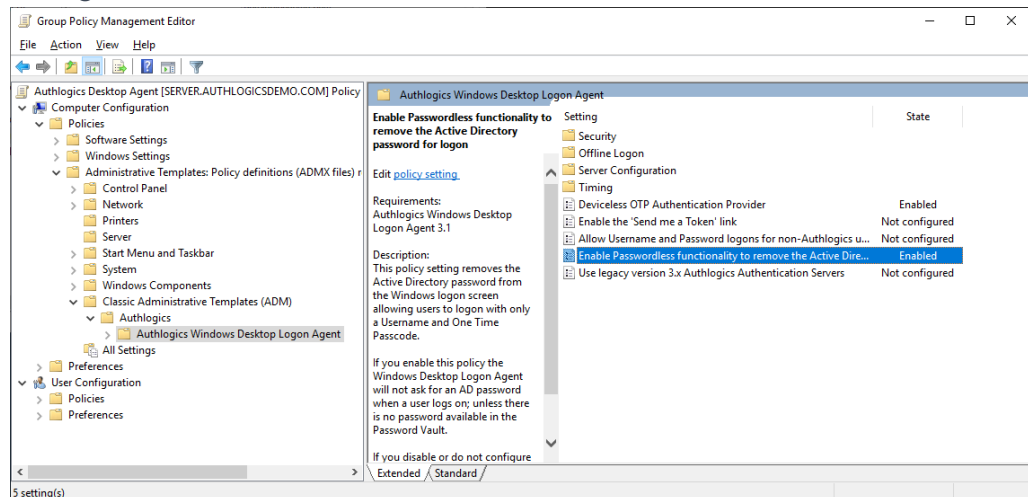
Configuring passwordless Windows logons

(1) On the server enabled the Authlogics Password Vault:



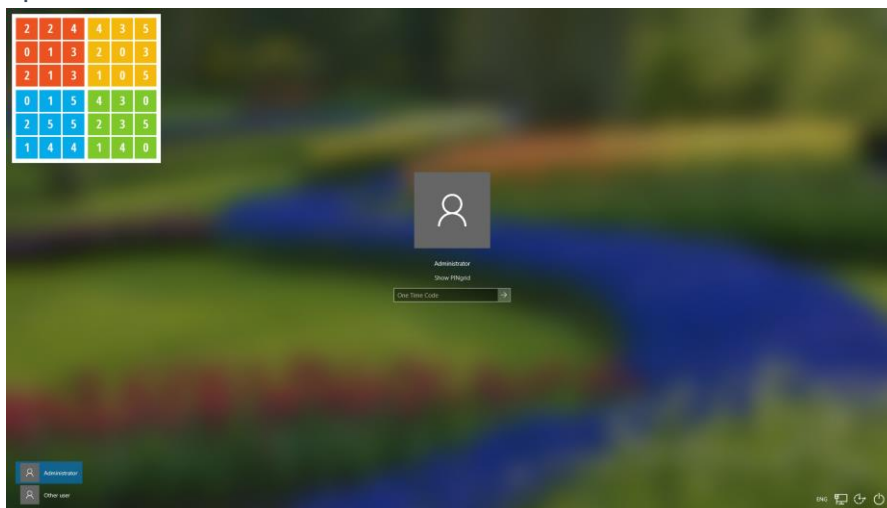
(2) Update the group policy settings:

- a. Enabled Passwordless functionality to remove the Active Directory password for logon: Enabled

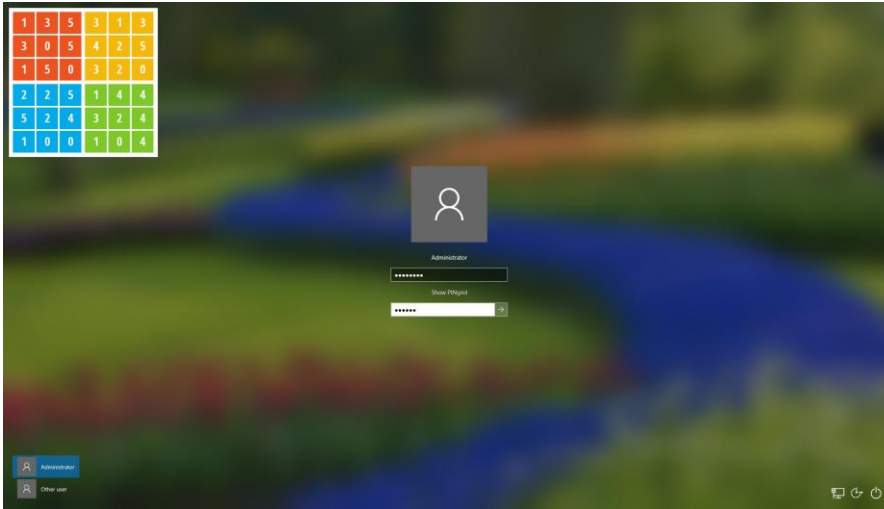


(3) Ensure the GPO settings are applied to the PC by running `GPUPDATE /FORCE`

(4) Reboot the workstation and logon as the test user – note that there is no password option available:



- (5) On first attempt the login will fail if there is no password in the vault. The password option will automatically appear the 2nd time around.



- (6) After the login the password will be saved to the vault and can be seen on the user account on the server:

