

Multi-Factor Authentication

Quick Start Guide

Product Version: 4.2.1050.0

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

Email us: sales@authlogics.com



Authlogics, 329, Doncastle Road, Bracknell, Berkshire, RG12 8PE, UK www.authlogics.com | sales@authlogics.com | +44 1344 568 900 | +1 408 706 2866



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) Add AD accounts of Authlogics administrators to the Authlogics Administrators AD security group.
- (4) After the installation the server will require a reboot.
- (5) Internet access to <u>https://*.authlogics.com</u> 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.

Authlogics	-		\times	
Installing / The progr	Aut	hløg	ics	
Ø	Please wait while the Installation Wizard installs Authle Authentication Server. This may take several minutes.			
	Status: Configuring Windows Server Roles			
Authlogics				
	< <u>B</u> ack <u>N</u> e	ext >	Can	cel

(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 Authlogics User Account" from the actions on the right to start the wizard.
- (3) Select all the AD user which must be configured for Authlogics.



- (4) Complete the Wizard.
- (5) Select all the users to provision an MFA technology, e.g. PINgrid, PINpass, PINphrase, then click "PINxxxx Management" to start the wizard.
- (6) Configure the technology settings for the selected users:

×

🥑 PINgrid User Management Wizard		×
Directory update The user account is being updated with the new PINgrid us		
Update Progress		
- Provisioning the user account "auberta.crisco" Done.	^	1
The PINgrid User Management Wizard is complete.		
	~	
< <u>B</u> ack	Einish Cance	

(7) Complete the Wizard.

ame.threats Properties

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

Push General	PINgrid AD Password	PINphras Devices	e PINpass Emergency Override	
Devices	AD Tassword		Energency overnue	• Add Device Wizard
Device: Name:			~	Device Registration Manual Device Information.
Device II	Device Enab	oled		Select the type of device to add and enter the device information.
Type: Last used Last sync				Type: Google Android 🗸
Last sync			Add	ID: Name: My Google Android device
	ice Security re Biometric Seed			C Enabled
		OK	Cancel Apply	< Back Next > Cancel

(9) 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".

Authlogics RADIUS Clier	ıt										
Authlogics Authentication Se	rver Details	Devic	eless OTP								
Name / IP Address: 192.168.255.155				PINgrid PINphrase							
HTTPS Port (TCP):	14443		_								
RADIUS Shared Secret:	Pa55w0rd		1	1	5	2	5	0			
RADIUS Request			5	2	4	0	2	4			
Account Name:	ame threats		1	2	3	0	2	3			
One Time Passcode:	125020 Send Request		4	5	3	1	5	0			
Authenticating user ame threa	ts - 21/06/2021 15:29:51 erver 192.168.255.155 on UDP port 1812		1	5	0	2	4	3			
RADIUS response : ACCES	S_ACCEPT		1	4	0	4	3	3			
Authenticator : System.Byte[] Identifier : 245 Header : NasPortType : ASYNC Valid : True			Get PI	Ngrid							
Call response completed in 41 Call Complete 21/06/2021 15											
<	>							C	Close		

d. The RADIUS result is shown.





Monitoring MFA Usage

Authlogics Server includes a Dashboard to graphically display the state of your MFA deployment.

Launch the Authlogics Admin portal via https://localhost:14443/admin.

Select System - Dashboards - Multi-Factor Authentication.

The dashboard reflects MFA actions for:

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







Configuring the Windows Desktop Agent

This section assumes a separate workstation test PC is being used which is domain joined. Authlogics Windows Desktop Agent can be deployed on non-domain joined PCs however, the Group Policy Objects will need to be applied to these PCs manually.

Configuring the Windows Desktop Agent

Perform these actions on the server:

- (1) Download the Windows Desktop Agent installer from <u>https://authlogics.com/downloads/</u> and extract the ZIP.
- (2) Import the GPO\AuthlogicsWDA.admx 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

	Group F	Policy Management Editor			
Eile <u>A</u> ction <u>V</u> iew <u>H</u> elp					
Þ 🔿 🙍 📷 🔒 🛛 🖬 🛛 🍸					
PSM-4.1 [SUB-DC.SPAWN.AUTHLOGICSDEMO.COM] Policy Policies Software Settings Software Settings Administrative Templates: Policy definitions (ADMX files) ret Authlogics Control Panel Control Panel Pinters Sat Henu and Takbar Sat Henu and Takbar System Windows Components All Settings Windows Components All Settings Preferences Preferences 	Windows Desktop Agent , Select an item to view its description.	Setting Offline Logon Security Security Allow Username and Password logons for non-Authlogics u Deviceless OTP Authentication Provider Disable Multi-Factor Authentication Disable Multi-Factor Authentication Disable Password Reset via SMS Enable Password Papiny Notice Active Directory Account Expiny Notice E Use legacy version 3x Authlogics Authentication Servers	State Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured	Comment No No No No No No No No No No	
>	Extended Standard				
1 setting(s)					

(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 enable 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:



