Installation Guide

Advanced Authentication Server

Version 6.0

NetIQ

Legal Notices

Contents

About NetIQ Corporation **5**
About this Book **7**

1 System Requirements **9**

2 Installing Advanced Authentication **11**

3 Configuring the Basic Settings **13**

Configuring Host Name 13
Configuring HTTP Proxy Server 14
Configuring Appliance Networking 14
Configuring Time and NTP Servers 14
Rebooting Appliance 15
Shutting Down Appliance 15

4 Configuring Global Master Server **17**

Configuring YubiHSM 17

5 Upgrading Advanced Authentication **19**

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About this Book

This Installation guide is intended for system administrators and describes the procedure of installing, configuring, and upgrading the Advanced Authentication server appliance.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

1 System Requirements

IMPORTANT: Advanced Authentication is a self-contained Debian 8 64-bit based appliance. The appliance is installed from a single ISO and can be installed on bare metal hardware or on the hypervisor of your choice (VMware, Hyper-V, etc).

Before installing the product, ensure the following system requirements are met:

Minimum hardware requirements for each appliance:

- 40 GB disk space
- 2 Cores CPU
- 4 GB RAM

Recommended hardware requirements for each appliance:

- 60 GB disk space
- 8 Cores CPU
- 8 GB RAM

NOTE: The amount of allocated memory must be divisible by 1024.

Supported browsers for Advanced Authentication Administrative Portal, Self Service Portal and Helpdesk Portal:

- Microsoft Internet Explorer 11
- Microsoft Edge 20.0 and later
- Google Chrome 40.0 and later
- Mozilla Firefox 36.0 and later
- Apple Safari 8 and later

For system requirements of client components and plug-ins, see the related documentation.

2 Installing Advanced Authentication

To install Advanced Authentication Server Appliance, perform the following steps:

1. Ensure that your environment complies with the System requirements.
2. Mount the Advanced Authentication installation ISO file and boot the machine.
3. Read and accept the license agreement.
4. Wait for few minutes while the appliance installs.
5. Select the applicable networking configuration method:
   - **DHCP** - to configure networking automatically.
   - **StaticIP** - to configure networking manually.

     Specify all the required parameters manually and press **ENTER** to apply changes.
6. You must specify the Administrator password for console access. Enter and confirm the password.

   The password must contain a minimum of eight characters that include capital letters and numerals.

   Ensure that you enter the password with a United States or International keyboard.

   WARNING: On Hyper-V, you may get the issue of re-starting the installation after completing the installation. You must unmount the ISO image and restart the server.

The **AUCORE appliance services** window launches with the **Configuration Console**.

IMPORTANT: The time on Advanced Authentication servers must be synchronized. Ensure that the NTP port 123 (UDP) is open on your corporate firewalls to allow Advanced Authentication servers to sync time on the predefined NTP servers or specify your internal NTP servers.

NOTE: For information on upgrading Advanced Authentication Server, see “Upgrading Advanced Authentication”.

3 Configuring the Basic Settings

After installing Advanced Authentication, you can set the Configuration Console to manage Advanced Authentication Server appliance. You can perform the following settings in the Configuration Console:

- “Configuring Host Name” on page 13
- “Configuring HTTP Proxy Server” on page 14
- “Configuring Appliance Networking” on page 14
- “Configuring Time and NTP Servers” on page 14
- “Rebooting Appliance” on page 15
- “Shutting Down Appliance” on page 15

The Configuration Console contains Admin UI and User UI addresses. To proceed to Advanced Authentication Server appliance management, select **Advanced Menu**.

Configuring Host Name

To configure Advanced Authentication server appliance host name, perform the following steps:

1. Go to the **Advanced Menu** of the **Configuration Console**.
2. Select **Host**.
3. (Optional) Specify an applicable host name and press **ENTER** to apply changes.
4. Restart the server.

NOTE: Do not change the host name once the Advanced Authentication server has been configured.

Configuring HTTP Proxy Server

To configure the Advanced Authentication server appliance HTTP proxy server, perform the following steps:

1. In the **Advanced Menu** of the **Configuration Console**, select **Proxy.**
2. Select **Configure HTTP proxy settings** and specify the parameters to configure the server.

You can also select **Disable HTTP proxy** to disable the HTTP proxy server.

NOTE: After you apply the changes, you must restart the server.

If you authenticate with the Email OTP authentication in the Advanced Authentication server behind a proxy server, you must use an internal Email server.

Configuring Appliance Networking

To configure Advanced Authentication server appliance networking, perform the following steps:

1. Go to the **Advanced Menu** of the **Configuration Console**.
2. Select **Networking**.
3. Select an applicable networking configuration method:
   - **DHCP** - to configure networking automatically.
   - **StaticIP** - to configure networking manually.

     Specify all required parameters manually and press **ENTER** to apply changes.

Configuring Time and NTP Servers

To configure Advanced Authentication server appliance time and NTP servers, perform the following steps:

1. Go to the **Advanced Menu** of the **Configuration Console**.
2. Select **Time**.
3. Select one of the following options:
   - **Refresh** to refresh current time.
   - **NTP servers** to configure NTP servers.

     Specify applicable addresses for NTP servers and press **ENTER** to apply changes.

NOTE: The time on Advanced Authentication servers must be synchronized. Ensure that the NTP port 123 (UDP) is open on your corporate firewalls to allow Advanced Authentication servers to sync time on the predefined NTP servers or specify your internal NTP servers.

Rebooting Appliance

To reboot Advanced Authentication server appliance, perform the following steps:

1. Go to the **Advanced Menu** of the **Configuration Console**.
2. Select **Reboot**.

Shutting Down Appliance

To shut down Advanced Authentication server appliance, perform the following steps:

1. Go to the **Advanced Menu** of the **Configuration Console**.
2. Select **Shutdown**.

4 Configuring Global Master Server

After installing Advanced Authentication server, you must configure the mode on which the appliance runs. The first server is the **Global Master/ Server Registrar**. This is the server with master database. DB Master, DB servers, and Web servers are connected to the master database.

To configure the first server, perform the following steps:

1. Ensure that you install the Advanced Authentication server.
2. Open the Advanced Authentication Configuration Wizard for the server: https://<server_host_name> (the URL is displayed after you install Advanced Authentication server).
3. Select **New Cluste**r and click **Next** on the first **Server Mode** screen of the Configuration Wizard.
4. Specify the server DNS hostname in **My DNS hostname** and click **Next** on the **DNS hostname** screen.

   NOTE: You must specify a **DNS hostname** instead of an IP address because appliance does not support the changing of IP address.

5. Specify a password for the LOCAL\admin account and confirm it and click **Next** on the **Password** screen.

   NOTE: If you need to use a Hardware Security Module from Yubico, perform steps Step 1 to Step 5 and then follow the steps in the section Configuring YubiHSM. Skip the steps 6 to 8 in this section.

6. Click **Create** to generate an encryption key file on the **Create encryption key** screen.
7. Switch **Enable FIPS 140-2** to **ON** if you need to comply to the FIPS 140-2 encryption.
8. Click **Next** and wait for 60 seconds while the server restarts.

Configuring YubiHSM

YubiHSM is a hardware security module developed by Yubico. It allows to store an encryption key for Advanced Authentication server instead of storing them on appliance locally.

To configure usage of the hardware security module, you need to follow the instructions during configuration of Configuring Global Master Server:

1. Hold the YubiHSM touch area and connect the device to the server physically. Continue to hold the touch area for 3 seconds when the YubiHSM is connected to activate the configuration mode. The LED starts to flash when you have entered the configuration mode.
2. Click **Create** to create an encryption key with the YubiHSM on the **Create encryption key** screen. In some seconds an encryption key will be created on the YubiHSM and a message is displayed in green: `Key file has been created`. In the Current key name you can see a `YUBIHSM` postfix.
3. Switch **Enable FIPS 140-2** to **ON** if you need to comply to the FIPS 140-2 encryption.
4. Click **Next** and wait for 60 seconds while the server restarts.

IMPORTANT: If you use a YubiHSM on the DB Master server, on the DB Slave server you must use another YubiHSM. In such a scenario, installation of DB Slave server without a YubiHSM is not supported. There is no step to create an enterprise key during configuration of DB Slave server, the connected YubiHSM is configured when the master's database is copied to the DB Slave server.

5 Upgrading Advanced Authentication

It is recommended to upgrade when the user's activities are low. The period of upgrade must be reduced as the replication of databases that do not synchronize can break the DB servers.

Officially support for Advanced Authentication 5.4 and prior version has concluded according to https://www.microfocus.com/lifecycle/ mainstream support. NetIQ now supports the upgrade for Advanced Authentication 5.5 and newer versions.

To upgrade Advanced Authentication 5.5 and newer versions, perform the following steps:

1. Create snapshots for all the Advanced Authentication servers.

   Check System requirements and increase the RAM to 4GB if you have allocated less amount of RAM to the server.
2. Open the Advanced Authentication Administrative Portal in the Global Master server and go to the **Updates** section.
3. Click **Update** to apply the Operating System updates.

   An error `Database is restarting (AuError)` might be displayed. Wait to check for updates.
4. Click **Check for updates** and then **Update**.

   After you upgrade, an error `UnpicklingError invalid load key, 'W'. (Internal Server Error)` can occur in the Advanced Authentication Administrative Portal due to expired cookies. The workaround is to clear the browser's cookies and try again.
5. In the menu on the top, click an administrator's username and select **Reboot**.
6. Log in to the Advanced Authentication Administrative Portal on the upgraded server.
7. Switch to the **Cluster** section and click **Conflicts** to check and resolve any conflicts.
8. Repeat steps Step 2 to Step 7 for DB servers and for Step 2 to Step 6 Web servers.

IMPORTANT: If you use Advanced Authentication server as a RADIUS server and have configured different RADIUS clients in different Advanced Authentication sites, then after upgrading to 5.6 Patch Update 1, the RADIUS configuration will be synchronized between the sites. You must add all the RADIUS clients in a single site. The configuration will be replicated to the servers in other sites.

WARNING: If you deny access to some of the Advanced Authentication server URLs with firewall, you must update rules because of a fix **All Advanced Authentication Portals Require Access to /admin/api** in the Advanced Authentication Patch Update 1. Advanced Authentication no longer requires `/admin/api` to access the Advanced Authentication portal. Instead, the server uses `/user/api`.

If you upgrade from 5.5 Patch Update 1 and previous versions and if you have used the Multitenancy feature previously, then you must add a new license with the Multitenancy support and restart all the Advanced Authentication servers. Ensure that you get the new license before you perform the upgrade.

Ignore the Advanced Authentication Administrative portal error messages displayed for non-upgraded servers when DB master is already upgraded.

NOTE: If you performed an upgrade for a DB server and you are unable to log in to the Advanced Authentication Administrative portal, perform the following steps:

1. Ensure that you are able to log in to the Administrative portal on the Global Master server.
2. Turn off the Global Master server.
3. Wait until all other servers are available.
4. Start the upgrade on all other servers with the above instructions simultaneously.

NOTE: After you upgrade to 5.6 Patch Update 4, the Database (DB) slave servers are susceptible to a replication conflict. To resolve this conflict, click **Fix** in the **Conflicts** section on both the DB master and slave servers. Such conflicts will not occur again.