Installation and Upgrade Guide

Advanced Authentication Server

Version 6.0

NetIQ

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Contents

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 audience responsible for understanding administration concepts and implementing a secure, distributed administration model.

1 Advanced Authentication Overview

Advanced Authentication™ is a multi-factor authentication solution that enables you to protect your sensitive data by using a more advanced way of authentication on top of the typical username and password authentication. With Advanced Authentication, you can authenticate on diverse platforms by using different types of authenticators such as Fingerprint, Card, and OTP. Advanced Authentication provides a single authentication framework that ensures secure access to all your devices with minimal administration.

Authentication comprises of the following three factors:

- Something that you know such as password, PIN, and security questions.
- Something that you have such as smartcard, token, and mobile phone.
- Something that you are such as biometrics (fingerprint or iris).

You can achieve multi-factor or strong authentication by using any two factors out of this list. For example, multi-factor authentication can include combination of a password and a token or a smartcard and a fingerprint.

This section contains the following topics:

How Is Advanced Authentication Better Than Other Solutions

Advanced Authentication leverages the needs of users to authenticate on different platforms with different needs. The following points explain how Advanced Authentication is different from other solutions:

- Works on multiple platforms such as Windows, Mac OS X, Linux and so on.
- Supports multi-site configurations that helps organizations to distribute the authentication globally.

Key Features

- **Multi-factor Authentication**: The solution provides a flexibility of combining more than twenty authentication methods to create authentication chains. You can assign these chains to different events to use the specific authentication chains for different kinds of endpoints.
- **Supports Multiple Repositories:** Advanced Authentication supports Active Directory, Active Directory Lightweight Domain Services, NetIQ eDirectory, and other RFC 2037 and RFC 2037 bis compliant LDAP repositories.

- **Supports Distributed Environments**: Advanced Authentication works on geographically distributed environments containing high loads.
- **Multitenancy**: A single Advanced Authentication solution can support multiple tenants to serve multiple customers with different environments.
- **Supports Multiple Platforms:** Advanced Authentication works on various platforms such as Windows, Linux, and Mac OS.
- **Helpdesk**: Advanced Authentication provides a separate role of Helpdesk or Security officer. A user with Helpdesk or Security Officer role can manage authenticators for the end users through the Helpdesk portal.
- **Supports the RADIUS Server**: Advanced Authentication Server contains a built-in RADIUS server to provide strong authentication for third-party RADIUS clients. Also, it can act as a RADIUS client for the third-party RADIUS servers.
- **Supports ADFS 3 and 4, OAuth 2.0, and SAML 2.0:** Advanced Authentication integrates with Active Directory Federation Services, OAuth 2.0, and SAML 2.0. This enables you to perform strong authentication for the users who need to access the third-party consumer applications.
- **Reporting**: Advance Authentication provides the Reporting portal that enables you to access different security reports. You can also create customized reports based on your requirement.
- **Syslog support**: Advanced Authentication provides the central logging server that can be used for log forwarding. You can configure the solution to forward logs to an external Syslog server.
- **FIPS 140-2 Compliant Encryption**: Advanced Authentication adheres to Federal Information Processing Standard (FIPS) 140-2.
- **Supports Localization**: Advanced Authentication supports several languages such as Arabic, Chinese, Dutch, and Danish.

Advanced Authentication Server Components

Advanced Authentication server comprises of the following components:

- **Administration Portal**

  For more information, see “Administration Portal” on page 10
- **Self-Service Portal**

  For more information, see “Self-Service Portal” on page 11
- **Helpdesk Portal**

  For more information, see “Helpdesk Portal” on page 11
- **Reporting Portal**

  For more information, see “Reporting Portal” on page 11

Administration Portal

Administration Portal is a centralized portal that helps you to configure and manage various authentication settings such as methods, events, and so on. You can also configure various policies that are required for authentication. You can perform the following tasks:

- **Add repositories**: A repository is a database that stores users information. For example: An organization, Digital Airlines contains an Active Directory that stores all of the user’s information such as username, telephone, address, and so on. Administrator can add this Active Directory to Advanced Authentication solution to help different departments in the organization such as the

IT, finance, HR, and Engineering departments to authenticate based on their requirements. For more information about how to add repositories, see “Adding a Repository” in the *Advanced Authentication - Administration* guide.

- **Configure methods**: A method or an authenticator helps to confirm the identification of a user (or in some cases, a machine) that is trying to log on or access resources. You can configure the required settings for the appropriate methods depending on the requirement by each department. For more information about how to configure methods, see “Configuring Methods” in the *Advanced Authentication - Administration* guide.
- **Create chains:** A chain is a combination of methods. Users must authenticate with all the methods in a chain. For example, a chain with Fingerprint and Card method can be applicable for the IT department and a chain with Smartphone, LDAP Password, and HOTP is applicable for the Engineering department. For more information about how to create chains, see “Creating a Chain” in the *Advanced Authentication - Administration* guide.
- **Configure events**: An event is triggered by an external device or application that needs to perform authentication such as a Windows machine, a RADIUS client, a third party client and so on. After creating the chain, Administrator maps the chain to an appropriate event. For more information about how to configure events, see “Configuring Events” in the *Advanced Authentication - Administration* guide.
- **Map endpoints**: An endpoint is a device on which you can authenticate. Endpoints can be computers, Laptops, tablets, and so on. For more information about how to configure endpoints, see “Managing Endpoints” in the *Advanced Authentication - Administration* guide.
- **Configure policies**: An administrator can manage policies that are specific to users, devices, or locations to control a user’s authentication. In Advanced Authentication, you can manage the policies in a centralized policy editor. For more information about how to configure policies, see “Configuring Policies” in the *Advanced Authentication - Administration* guide.

Self-Service Portal

The Self-Service Portal allows users to manage the available authentication methods. This portal consists of **Enrolled authenticators** and **Add authenticator**. T**he Enrolled authenticators** section displays all the methods that users have enrolled. The **Add authenticator** section displays additional methods available for enrollment. You must configure and enable the “Authenticators Management Event” event to enable users to access the Self-Service portal. For more information on Self-Service portal, see *Advanced Authentication- User* guide.

Helpdesk Portal

The Helpdesk Portal allows the helpdesk administrators to enroll and manage the authentication methods for users. Helpdesk administrators can also link authenticators of a user to help authenticate to another user’s account. For more information on Helpdesk portal, see the *Advanced Authentication- Helpdesk Administrator* guide.

Reporting Portal

The Reporting Portal allows you to create or customize security reports that provide information about user authentication. It also helps you understand the processor and memory loads. For more information on Reporting portal, see “Reporting” *Advanced Authentication - Administration* guide.

Architecture

Advanced Authentication architecture is based on the following three levels of architecture:

- Basic Architecture

  For more information, see “Basic Architecture” on page 12
- Enterprise Level Architecture

  For more information, see “Enterprise Level Architecture” on page 13
- Enterprise Architecture With A Load Balancer

  For more information, see “Enterprise Architecture With A Load Balancer” on page 15

Basic Architecture

The basic architecture of Advanced Authentication is a simple configuration that requires only one Advanced Authentication server.

An Advanced Authentication server is connected to a directory such as Active Directory Domain Services, NetIQ eDirectory, Active Directory Lightweight Directory Service or other compliant LDAP directories. An Event Endpoint can be Windows, Linux or Mac OS X machine, NetIQ Access Manager, NetIQ CloudAccess, or RADIUS Client to authenticate through the RADIUS Server that is built-in the Advanced Authentication Server.

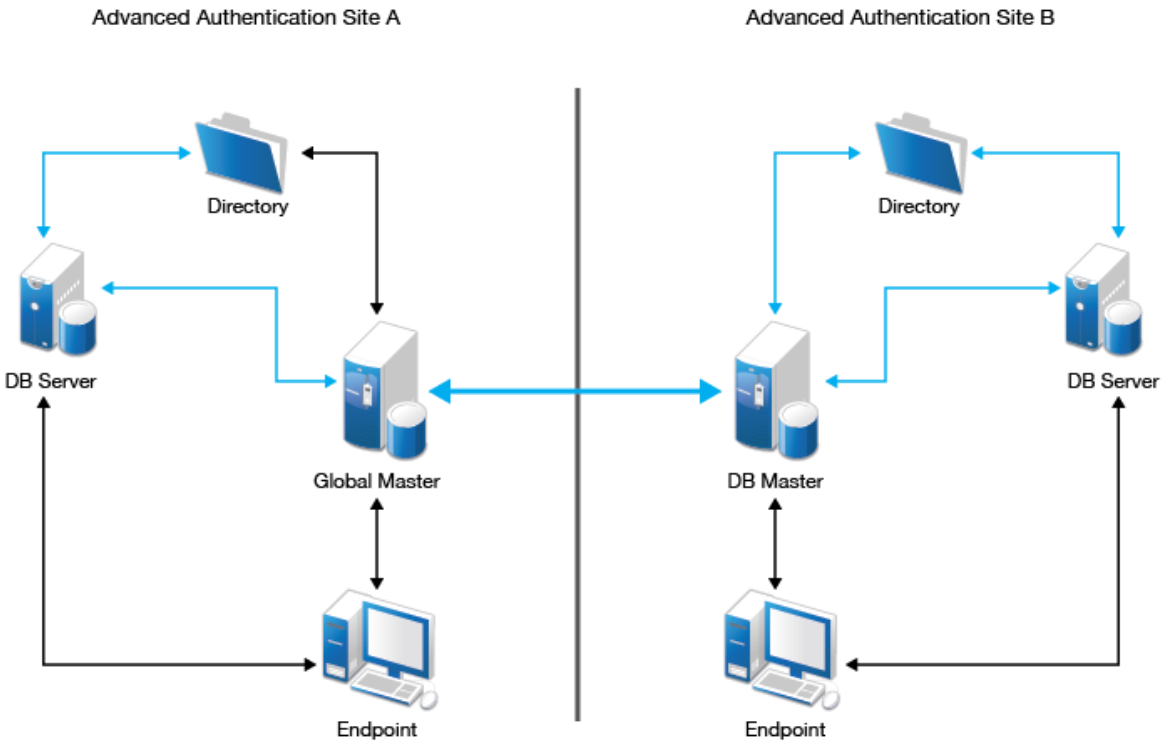
For a complete list of supported events, see “Configuring Events” in the *Advanced Authentication - Administration* guide.

Enterprise Level Architecture

In the enterprise level architecture of Advanced Authentication, you can create several sites for different geographical locations.

For example, the Figure 1-1 on page 13 displays two Advanced Authentication sites, **Site A** and **Site B**.

Figure 1-1 *Enterprise Level Architecture*



- **Site A**: The first site that is created for headquarters in New York. The first Advanced Authentication server of site A contains the **Global Master** and **Registrar** roles. This server contains a master database and it can be used to register new sites and servers.
- **Site B**: Another site created for the office in London. The structure of site B is similar to site A. The Global Master in another site has the DB Master role. DB servers interact with the DB Master.

  DB Server provides a database that is used for backup and fail-over. You can create a maximum of two DB servers per site. When the Global Master is unavailable, the DB server responds to the database requests. When the Global Master becomes available again, the DB server synchronizes with the Global Master and the Global Master becomes the primary point of contact for database requests again.

  Endpoints interact with Global Master or DB Master servers. When these servers are not available, they interact with DB servers.

NOTE: DB servers connect to each other directly. If the Global Master is down, the DB servers will replicate.

A Global Master must have a connection to each of the LDAP servers. Hence in a data center with Global Master, you must have LDAP servers for all the used domains.

Master servers do not initiate a connection to the DB servers. Master servers initiate connection to Master servers only. DB servers initiate connection to the DB Master of the same site and Registrar only.

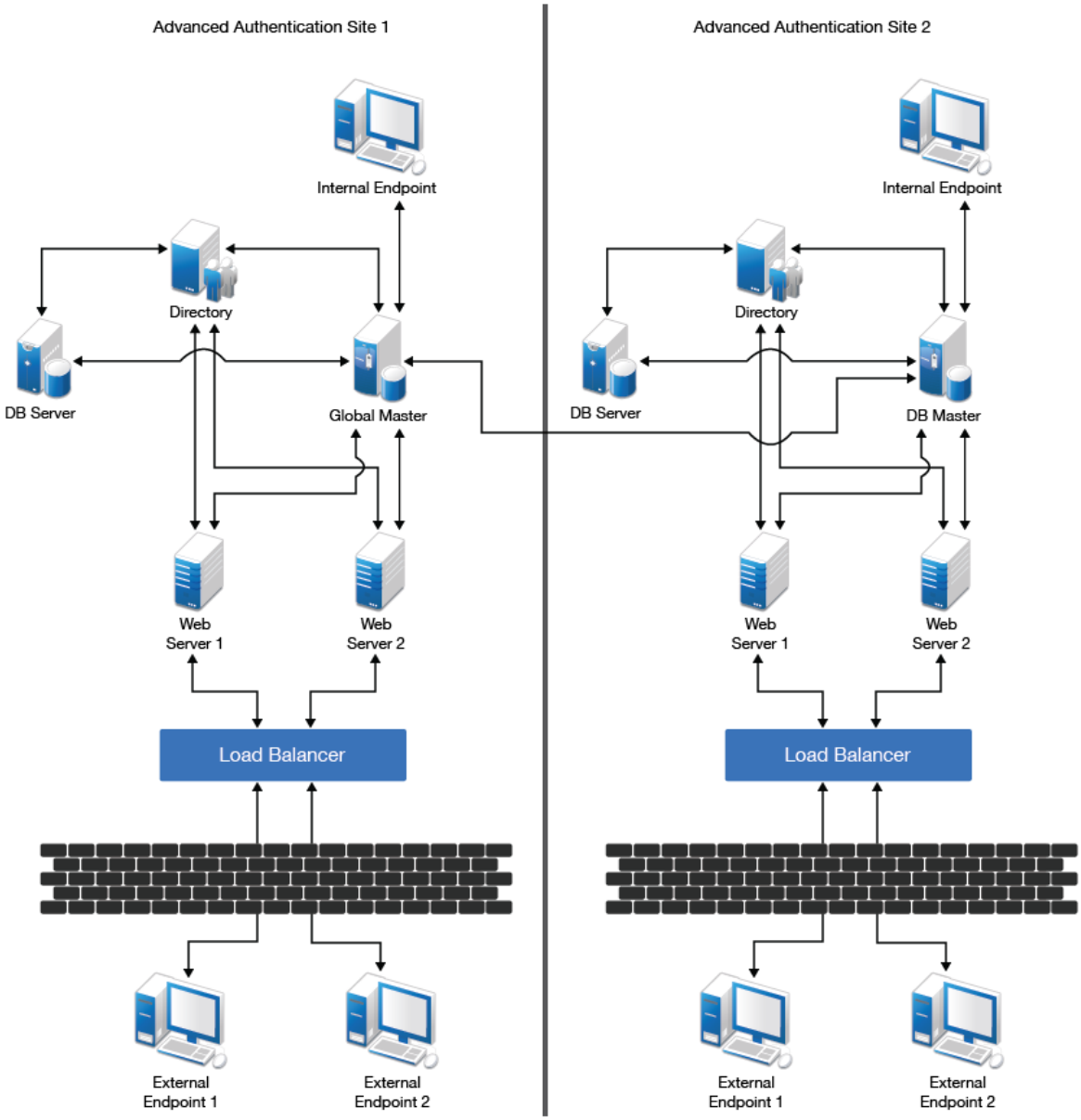
IMPORTANT: Ensure to take regular snapshots or to clone the primary site to protect from any hardware issues or any other accidental failures. It is recommended to do it each time after you change the configuration of repositories, methods, chains, events and policies, or add or remove servers in the cluster.

You can convert DB server of primary site to Global Master. This requires corresponding DNS changes. Nothing can be done if Global Master and all slaves are lost.

Enterprise Architecture With A Load Balancer

The enterprise architecture with a load balancer contains web servers and load balancers along with the components in Enterprise Level Architecture. Figure 1-2 on page 15 illustrates the Enterprise architecture with a load balancer.

Figure 1-2 *Enterprise Architecture with Load Balancer*



- **Web Servers**: Web server does not contain a database. It responds to the authentication requests and connects to Global Master. You need more web servers to serve more workload.

  NOTE: It is not recommended to deploy more than 5-6 web servers per site.

- **Load Balancer**: A load balancer provides an ability to serve authentication requests from **External Endpoints**. A load balancer is a third-party component. It must be configured to interact with Web servers.

NOTE: To view an example of configuring a load balancer for an Advanced Authentication cluster, see “Installing a Load Balancer for Advanced Authentication Cluster” in the *Advanced Authentication - Administration* guide.

Terminologies

Authentication Method

An authentication method verifies the identity of an individual who wants to access data, resources, or applications. Validating that identity establishes a trust relationship for further interactions.

Authentication Chain

An authentication chain is a combination of authentication methods. A user must pass all methods in the chain to be successfully authenticated. For example, if you create a chain with LDAP Password and SMS, a user must first specify the LDAP Password. If the password is correct, the system sends an SMS with a One-Time-Password (OTP) to the user’s mobile. The user must specify the correct OTP to be authenticated.

You can create chains with multiple methods that are applicable for highly secure environments. You can create authentication chains for specific group of users in the repositories.

Authentication Event

An authentication event is triggered by an external device or application that needs to perform authentication. It can be triggered by a RADIUS Client (Citrix Netscaler, Cisco VPN, Juniper VPN and so on) or an API request. Each event can be configured with one or more authentication chains that enables a user to authenticate.

Endpoint

An endpoint is a device on which you can authenticate. Endpoints can be computers, Laptops, tablets, Smartphones, and so on.

Tenant

A tenant is a company with a group of users sharing common access with specific privileges. In Advanced Authentication, tenants have the privileges to customize some of the configuration settings.

2 System Requirements

IMPORTANT: The appliance is based on the SUSE Linux Enterprise Server 12 Service Pack 3 operating system.

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

The following table lists the minimum and recommended requirements to deploy the Advanced Authentication appliance.

Component	Requirements
Virtual Systems	◆ Hyper-V version 4.0 ◆ VMware ESX 5.5 or later
Memory	Minimum requirement: 4 GB of RAM Recommended requirement: 8 GB of RAM
Hard disk space	Minimum requirement: 40 GB Recommended requirement: 60 GB
CPU	Minimum requirement: 2 Cores CPU Recommended requirement: 8 Cores CPU SSE 4.2 instructions must be supported by the processor
Browsers	◆ Microsoft Internet Explorer 11 ◆ Microsoft Edge 20.0 and later ◆ Google Chrome 65 and later ◆ Mozilla Firefox 58 and later ◆ Safari 11 and later
IP Ports	Ensure that the default ports for the Advanced Authentication appliance are open in your firewall. For more information, see “Configuring the Firewall”.
LDAP Repositories	◆ Microsoft Active Directory Directory Services ◆ Microsoft Active Directory Lightweight Directory Services ◆ NetIQ eDirectory ◆ OpenLDAP ◆ OpenDJ ◆ Microsoft SQL Server 2016

3 Installing Advanced Authentication

This chapter guides you through the process of installing the components and framework required for Advanced Authentication.

Obtaining Advanced Authentication

Advanced Authentication is available in two types: a trial version and a full version. You can access the different version in different locations.

Downloading the Full Version

You must have purchased Advanced Authentication to access the full version of the product. To buy a full version of Advanced Authentication, see How to Buy. The activation code is in the Customer Center where you download the software. For more information, see Customer Center Frequently Asked Questions.

To access a full version of Advanced Authentication:

1. Log in to the Customer Center.
2. Click **Software**.
3. In the **Entitled Software** tab, click the appropriate version of Advanced Authentication for your environment to download.

To deploy the Advanced Authentication server on VMware, unpack the file `advancedauthappliance-vmware-x86_64-x.x-xxx.ovf.tar.gz`.

To deploy the Advanced Authentication server on Hyper-V, unpack the file `advancedauthappliance-hyperv-x86_64-x.x-xxx.zip`.

Downloading the Trial Version

A trial version of Advanced Authentication can also be provided to allow you to see how the product works.

To download the trial version:

1. Access the Download page at https://dl.netiq.com.
2. Click the **Find Trial Download** link.
3. Scroll down to find Advanced Authentication, then click **Download**.
4. Specify your information to receive an email with the download link.

IMPORTANT: You must specify a valid email address or you will not receive the email that contains the link to download the trial version.

5 After you receive the email, click the link and download the appropriate version for your environment.

6 (Conditional) Extract the compressed file for the appliance.

To deploy the Advanced Authentication server on VMware, unpack the file `advancedauthappliance-vmware-x86_64-x.x-xxx.ovf.tar.gz`.

To deploy the Advanced Authentication server on Hyper-V, unpack the file `advancedauthappliance-hyperv-x86_64-x.x-xxx.zip`.

Installing Advanced Authentication

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

1 Ensure that your environment complies with the System Requirements.

2 Deploy the appliance to your virtual environment. For more information, see:

VMware: Deploy an OVF Template.

Hyper-V: Deploy a server with VHD.

3 Power on the appliance.

4 Select the appropriate language, read the license, and click **Accept**.

5 Use the following information to configure the appliance:

- **root Password**: Specify a password for the root user on the appliance.
- **NTP Server**: Specify a primary and secondary NTP server used to keep time on the appliance.
- **Region and Time Zone**: Select your region and time zone.
- **Hostname and Networking options**: Specify a hostname for the appliance, then select whether to use a **Static IP address** or **DHCP**. If you use a static IP address, you must specify the IP address, subnet mask, the gateway, and the DNS servers.

6 Click **Finish** and wait for the appliance initialization to complete.

IMPORTANT: The time on Advanced Authentication servers must be synchronized with NTP servers. 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. For more information on time setting, see "Configuring Time Settings".

NOTE: For information on migrating Advanced Authentication server from v5 to 6.0, see "Migrating Advanced Authentication to 6.0".

WARNING: When you log in to the console as **root** and run **yast novell-vainit**, it is strongly not recommended to select the **Reboot** or **Shutdown** option in the **YaSTZ-novell-vainit** installer. You will not be able to access the web user interface after shutting down or rebooting appliance and loading it again.

4 Managing the Appliance

After installing the appliance, you can edit the configurations such as administrative passwords for the `root` user, network settings, and certificate settings in the Configuration portal. You must perform these tasks only from the Console because native Linux tools do not recognize the configuration requirements and dependencies of the Advanced Authentication services.

IMPORTANT: NetIQ delivers and updates the Advanced Authentication appliance as a single unit including the operating system, the Advanced Authentication application, and associated runtime components. NetIQ does not recommend adding any additional software components to the appliance. Any support issues that arise with the customer supplied components might require removal before the support issues are resolved.

To access the Configuration console, perform the following steps:

1. In a web browser, specify the DNS name or the IP address of the appliance with the port number 9443. For example:

   ```
   https://10.10.10.1:9443
   ```

   or

   ```
   https://mycompany.example.com:9443
   ```

2. Specify **root** or **vaadmin** as the user name and specify the password for the appliance, then click **Sign in**.
3. Continue using the Appliance Configuration tools.

The Configuration console displays the following options:

Configuring Network Setting

You can configure settings for the DNS servers, search domains, gateway, and NICs for the appliance in the **Network** tab. You might need to modify these settings after the initial setup if you move the appliance VM to a new host server, or move the host server to a new domain in your network environment. You can also optionally restrict the networks that are allowed to access the appliance.

To configure network settings for the appliance:

1. Log in to the Configuration Console as the `root` user.
2. Click **Network**.
3. In the **DNS Configuration** section, you can modify the DNS name servers, search domains, and gateway settings for your appliance network.

   If **Search Domains** is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is `ptm.mycompany.com`, the domain is auto-populated with `mycompany.com`.
4. In the **NIC Configuration** section, you can modify the IP address, hostname, and network mask of any NIC associated with the appliance.
   - **4a** Click the ID of the NIC.
   - **4b** Edit the IP address, hostname, or network mask for the selected NIC.
   - **4c** Click **OK**.
   - **4d** Repeat the Step 4a to Step 4c for each NIC that you want to configure.
5. (Optional) In the **Appliance Administration UI (port 9443) Access Restrictions** section, do one of the following:
   - Specify the IP address of each network for which you want to allow access to the appliance. Only the listed networks are allowed.
   - Leave this section blank to allow any network to access the appliance.

   NOTE: After you configure the appliance, changes to your appliance network environment can impact the appliance communications.

   ---
6. Click **OK**.
7. Restart the server.

Configuring the Proxy Settings

If access to internet in your company is possible only through the proxy server, you must configure the proxy settings to enable the Advanced Authentication appliance to communicate with the proxy server.

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

1. Open the YaST Proxy Configuration module. To open the yast configuration module, specify `yast2 proxy` in the command line as a root user, or select **Network Services > Proxy** from YaST Control Center.
2. Select **Enable Proxy**.
3. Specify the URL for the protocols in the **Proxy Settings** section.

This URL is used for the proxy. The URL must include the colon (:) and port number. For example, http://<ip address>:<port number>.

4 Specify the user name and password in the **Proxy Authentication** section if the proxy server requires authentication.

5 Click **Test Proxy Settings** to validate the connection between the appliance and proxy server.

6 Click **OK**.

7 Reboot the appliance.

Configuring Time Settings

You can configure the Network Time Protocol (NTP) server, the geographic region, and the time zone where you have deployed the appliance with the Time settings.

To configure time parameters for the appliance:

1 Log in to the Configuration Console as the `root` user.

2 Click **Time**.

3 Change the following time configuration options as appropriate:

NTP Server: Specify the NTP server that you want to use for time synchronization.

Region: Select the geographic region where your appliance is located.

Time Zone: Select the time zone where your appliance is located.

4 Click **OK**.

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.

Managing Digital Certificates

You can add and activate certificates for the appliance in the **Digital Certificates** tab. You can create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair.

IMPORTANT: In this section, you can only manage certificates for the Advanced Authentication appliance (port 9443). To change the certificates for the Advanced Authentication application (port 443), goto the **Server Options** tab in the Administration portal.

The appliance is shipped with a self-signed digital certificate. Instead of using this self-signed certificate, it is recommended that you use a trusted server certificate that is signed by a trusted certificate authority (CA) such as Digicert or Equifax.

To change the digital certificate for appliance, perform the following tasks:

- “Using the Digital Certificate Tool” on page 24
- “Using an Existing Certificate and Key Pair” on page 25
- “Activating the Certificate” on page 25

Using the Digital Certificate Tool

Creating a New Self-Signed Certificate

1 Log in to the Configuration Console as the `root` user.

2 Click **Digital Certificates**.

3 In the **Key Store** list, select **Web Application Certificates**.

4 Click **File** > **New Certificate (Key Pair)** and specify the following information:

4a **General**

Alias: Specify a name that you want to use to identify and manage this certificate.

Validity (days): Specify for how long you want the certificate to remain valid.

4b **Algorithm Details**

Key Algorithm: Select either **RSA** or **DSA**.

Key Size: Select the preferred key size.

Signature Algorithm: Select the preferred signature algorithm.

4c **Owner Information**

Common Name (CN): This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.

Organization (O): (Optional) Large organization name. For example, My Company.

Organizational Unit (OU): (Optional) Small organization name, such as a department or division. For example, Purchasing.

Two-letter Country Code (C): (Optional) Two-letter country code. For example, US.

State or Province (ST): (Optional) State or province name. For example, Utah.

City or Locality (L): (Optional) City name. For example, Provo.

5 Click **OK** to create the certificate.

After the certificate is created, it is self-signed.

6 Make the certificate official, as described in "Getting Your Certificate Officially Signed" on page 24.

Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.

2 Complete the process of emailing your digital certificate to a certificate authority (CA), such as Digicert.

The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then emails the new certificate and certificate chain back to you.

3 After you have received the official certificate and certificate chain from the CA:

   3a Revisit the Digital Certificates page.

   3b Click **File** > **Import** > **Trusted Certificate**.

   3c Click **Browse** and select the trusted certificate chain that you received from the CA, then click **OK**.

   3d Select the self-signed certificate, then click **File** > **Certification Request** > **Import CA Reply**.

   3e Click **Browse** and select the official certificate to be used to update the certificate information.

   On the **Digital Certificates** page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

4 Activate the certificate, as described in "Activating the Certificate" on page 25.

Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use a `.P12` key pair format.

1 Log in to the Configuration Console as the `root` user.

2 Click **Digital Certificates**.

3 In the **Key Store** menu, select **JVM Certificates**.

4 Click **File** > **Import** > **Trusted Certificate**.

5 Click **Browse** and select your existing certificate, then click **OK**.

6 Click **File** > **Import** > **Trusted Certificate**.

7 Click **Browse** and select your existing certificate chain for the certificate that you selected in Step 4, then click **OK**.

8 Click **File** > **Import** > **Key Pair**.

9 Click **Browse** and select your `.P12` key pair file, specify your password if required, then click **OK**.

10 Continue with "Activating the Certificate" on page 25.

Activating the Certificate

1 On the **Digital Certificates** page, in the **Key Store** list, select **Web Application Certificates**.

2 Select the certificate that you want to make active and click **Set as Active**, then click **Yes**.

3 Select the certificate and click **View Info** to verify that the certificate and certificate chains are created appropriately.

4 Click **Close**, when you have activated the certificate successfully.

Accessing System Services

You can view the status of services running on the appliance in the **System Services** tab. System services include the following:

- SSH

To access the System Services page:

1. Log in to the Configuration Console as the `root` user.
2. Click **System Services**.

You can perform the following actions:

- Starting, Stopping, or Restarting System Services
- Making System Services Automatic or Manual

Starting, Stopping, or Restarting System Services

You can start, stop, or restart the SSH or the Advanced Authentication service.

To start, stop, or restart a service on the appliance:

1. Click **System Services**.
2. Select the service that you want to start, stop, or restart.
3. Click **Action**, then select **Start**, **Stop**, or **Restart**.

Making System Services Automatic or Manual

1. Click **System Services**.
2. Select the service that you want to make automatic or manual.
3. Click **Options**, then select either **Set as Automatic** or **Set as Manual**.

You can click **Refresh List** to refresh the list of the services.

Configuring the Firewall

You can view your current firewall configuration directly from the appliance in the **Firewall** tab. By default, all ports are blocked except those that are required by the appliance. For example, the Login page for the Configuration Console uses port 9443, so this port is open by default.

NOTE: To have a seamless experience with the appliance, ensure that you do not block the ports with your firewall settings.

To view firewall settings for the appliance:

1. Log in to the Configuration Console as the `root` user.
2. Click **Firewall**.

   The Firewall page lists port numbers with the current status of each port number. The page is not editable.

Configuring the Ports and Firewall

IMPORTANT: The Advanced Authentication server uses ports 443 and 80. These ports cannot be changed.

Port forwarding is not recommended in a production environment because the entire appliance is available through the internet. It is recommended to use reverse proxy to map only the specific URLs.

By default, the Advanced Authentication server uses the following RFC standard ports.

Service	Port	Protocol	Usage
REST	443	HTTPS	All Communications
Administration portal, Self-Service portal, Helpdesk portal, Reporting portal, and Search card portal	443	HTTPS	All Communications (<AAServer>/admin, <AAServer>/account, <AAServer>/helpdesk, <AAServer>/report)
Server Update	443	HTTPS	Update channel: appliance - update server (repo.authasas.com)
Database replication	5432	TCP	Database replication between DB servers. The port must be opened to the Master server of the same site (or to the Global Master server for the installation of DB Master Server in the new sites) only for the installation of new server. Then the port can be closed.
Database replication	8080	TCP	Database replication between DB servers
DNS	53	TCP, UDP	DNS
NTP	123	UDP	NTP, used for time synchronization
LDAP	389	TCP, UDP	LDAP (if used with repository)
LDAPS	636	TCP,UDP	LDAP over TLS/SSL (if used with repository)
Dashboard and Reporting portal	9200, 9300	HTTPS	Collecting statistics from the Advanced Authentication servers in the cluster
SQL	1433	TCP, 1434 UDP	Microsoft SQL Server (if used with repository)

Advanced Authentication server uses the following ports for the different methods:

Service	Port	Protocol	Usage
RADIUS	1812	TCP, UDP	Authentication
RADIUS	1813	TCP, UDP	Accounting
E-Mail Service	Variable	SMTP	E-Mail Traffic
Voice Call Service	Variable	HTTPS	All Communications (<AAServer>/twilio/status, <AAServer>/twilio/gather)
Smartphone	Variable	HTTPS	All Communications (<AAServer>/smartphone)
Smartphone Push Service	443	HTTPS	Communication between AAF and proxy.authasas.com (push service)
SMS	Variable	HTTPS	Communication to a used SMS service

Service	Port	Protocol	Usage
Swisscom Mobile ID	Variable	HTTPS	Communication to the specified Swisscom Mobile ID service URL
Voice OTP Service	Variable	HTTPS	All Communications (<AAServer>/twilio/otp)
Face Recognition	443	HTTPS	Microsoft Cognitive Services (URL specified in **Administration portal > Methods > Face Recognition > Endpoint URL**)

IMPORTANT: For reverse proxy, you can use any port. For example, `https://dnsname:888/smartphone`. A reverse proxy redirect is done from port 888 to port 443 internally to appliance. Port 888 is used from outside, but port 443 is used inside the appliance.

The following table lists the ports of the common appliance:

Port	Description
22	SSH port for the appliance
25	SMTP and SMTPS outbound ports
80	Standard Web server ports
1099	Java RMI port
7380	Ganglia RRD-REST ports
9080	Apache/HTTPD port
9090, 9443	Jetty port for the appliance (Administrator Interface)

The following table lists the URLs to access the external address for Advanced Authentication.

URL	Port	Description
`docker.io`	443	Required to download the docker updates
`ftp.novell.com`	21	Required to upload the logs for sending information to the Support team. For more information, see “Sending Information to Support”
`www.novell.com`	80	Required for the testing of YaST Proxy. For more information, see “Configuring the Proxy Settings”
`nu.novell.com` and `secure-www.novell.com`	443	Required for all the SUSE products
`proxy.authasas.com`	443	Required for the push service in Smartphone authentication

Advanced Authentication uses the following URLs.

URL	Used for
Advanced Authentication Server	
/static/*, /user/api	Web portals
/admin	Administration portal
/account	Self-Service portal
/helpdesk	Helpdesk portal
/report	Reporting portal
/api	REST API calls
/adfs	ADFS plug-in
/osp	SAML 2.0, OAUTH 2.0 integrations
/search-card	Search Card portal
Authentication Agent	
/oob/{oob_proc_id:[0-9a-zA-Z-]{3,32}}	Authentication Agent
Smartphone	
/smartphone/adddevice/{path}/{enc_dev_id}	
/smartphone/confirm/{path}	
/smartphone/pushid/{path}	
/smartphone/requestsalt/{path}	
/smartphone/saltpushid/{path}	
Twilio (SMS, Voice Call, Voice OTP)	
/twilio/gather/{proc_id}	
/twilio/otp/{proc_id}	
/twilio/otp_anon/{tenant_id}/{otp}	
/twilio/status/{proc_id}	

Setting Administrative Passwords

You can modify the passwords and SSH access permissions for the appliance administrator: the `root` user in the **Administrative Passwords** tab. If your password policy requires it, you must modify passwords periodically or if you reassign responsibility for the appliance administration to another person.

NOTE: The `vaadmin` helps to manage virtual-machine-level settings and service configurations that affect an entire service and its interactions with other services.

The `vaadmin` user can use the **Administrative Passwords** page to perform the following tasks:

- Modify the `vaadmin` user password. To change a password, you must provide the old password.

- The vaadmin user automatically has permissions necessary to remotely access the appliance with SSH instead of using a VMware client. The SSH service must be enabled and running to allow SSH access.

  NOTE: The SSH service is disabled and is not running by default. For information about how to start SSH on the appliance, see Accessing System Services.

The `root` user can use the **Administrative Passwords** page to perform the following tasks:

- Modify the `root` user password. To change a password, you must provide the old password.
- Enable or disable the `root` user SSH access to the appliance.

  When you select **Allow root access to SSH**, the root user is able to SSH to the appliance.

To manage the administrative access as the `vaadmin` user:

1. Log in to the Configuration Console as the `vaadmin` user.
2. Click **Administrative Passwords**.
3. Specify a new password for the `vaadmin` administrator. You must also specify the current `vaadmin` password.
4. Click **OK**.

To manage the administrative access as the `root` user:

1. Log in to the Configuration Console as the `root` user.
2. Click **Administrative Passwords**.
3. Specify a new password for the `root` administrator. You must also specify the current `root` password.
4. (Optional) Select or deselect **Allow root access to SSH**.
5. Click **OK**.

Adding a Field Patch to the Appliance

You can add patches provided by engineering in the **Field Patch** tab. A field patch is not a complete patch and must only be used until a complete patch is released. Before applying a field patch, you must disable all other updates for the appliance or the field patch can be overwritten.

The Patches are intended for specific bug fixes and security fixes for software that comes packaged by OpenSUSE and is maintained in the Main Updates repository. For more information, see OpenSUSE patch vs update (https://lukerawlins.com/opensuse-patch-vs-update/).

To manage the field patch updates:

1. Log in to the Configuration Console as the `vaadmin` user.
2. Click **Field Patch**, then follow the prompts to install the patch update.
3. (Conditional) Install a downloaded patch update:
   - **3a** Download the Advanced Authentication patch update file from the Patch Finder website.
   - **3b** In the **Install a Downloaded Patch** section, click **Browse**.
4. (Conditional) Uninstall a patch update:

You might not be able to uninstall some patch updates.

4a In the **Patch Name** column of the Field Patch list, select the patch update that you want to uninstall.

4b Click **Uninstall Latest Patch**.

5 (Conditional) Download a log file that includes details about the patch update installation.

5a Click **Download Log File** for the appropriate patch update.

NOTE: Ensure that you disable online updates and automatic updates until you apply a full patch that contains the fix.

Sending Information to Support

You can send the configuration information of appliance to Technical Support (https://www.netiq.com/support/) by uploading files directly to FTP, or by downloading the files to your management workstation and sending them by an alternative method to the Support team.

To send configuration files to Technical Support:

1. Log in to the Configuration Console as the `root` user.
2. Click **Support**.
3. Use one of the following methods to send the appliance's configuration files to Technical Support (https://www.netiq.com/support/):
   - Select **Automatically send the configuration to Micro Focus using FTP** to initiate the FTP transfer of configuration information.
   - Select **Download and save the configuration file locally, then send it to Micro Focus manually** to download configuration information to your management workstation. You can then send the information to Technical Support (https://www.netiq.com/support/) using a method of your choice.
4. Click **OK** to complete the process.

Performing an Online Update

Use the **Online Update** option to register for the online update service from the Customer Center (https://www.netiq.com/customercenter). You can install updates automatically or manually to update the appliance. For more information on the OpenSUSE online updates, see OpenSUSE patch vs update (https://lukerawlins.com/opensuse-patch-vs-update/).

If you want to control the updates further, you can configure the appliance to get the updates from a local Subscription Management Tool (SMT). This allows you to download the updates to a single SMT server in your network and all other Advanced Authentication appliances receive their updates from this server. For more information, see *Subscription Management Tool Guide*. To obtain the proper credentials to use the SMT server, see "Mirroring Credentials" in the *Subscription Management Tool Guide*.

To activate the Update Channel, you must obtain the key from the Customer Center. If the key is not available, contact the Customer Center through an email.

WARNING: Before performing the online update, ensure to add rules in the firewall to allow https traffic to the URLs such as docker.io, nu.novell.com and secure-www.novell.com.

For more information about configuring the firewall, see Configuring the Ports and Firewall.

To register for the Online Update Service:

1. Log in to the Configuration Console as the `root` user.
2. Click **Online Update**.
3. If the Registration dialog does not open automatically, click the **Register** tab.
4. Select the **Service Type**:
   - Local SMT (Proceed to Step 5.)
   - Micro Focus Customer Center (Skip to Step 6.)
5. (Local SMT) Specify the following information for the SMT server, then continue with Step 7.
   - Hostname such as `smt.example.com`
   - (Optional) SSL certificate URL that communicates with the SMT server
   - (Optional) Namespace path of the file or directory
6. (Micro Focus Customer Center) Specify the following information about the Customer Center (https://www.netiq.com/customercenter) account for this appliance:
   - Email address of the account in Customer Center
   - Activation key (the same Full License key that you used to activate the product)
   - Allow data send (select any of the following)
     - Hardware Profile
     - Optional information
7. Click **Register**.

   Wait while the appliance registers with the service.
8. Click **OK** to dismiss the confirmation.

After you have registered the appliance, you can view a list of the needed updates, or view a list of installed updates. You can use manual or automatic options to update the appliance.

To perform other actions after registration:

- **Update Now:** Click **Update Now** to trigger downloaded updates.
- **Schedule:** Configure the type of updates to download and whether to automatically agree to the licenses.

  To schedule online update:

  1. Click the **Schedule** tab.
  2. Select a schedule for download updates (**Manual**, **Daily**, **Weekly**, **Monthly**).
- **View Info:** Click **View Info** to display a list of installed and downloaded software updates.
- **Refresh:** Click **Refresh** to reload the status of updates on the Appliance.

Performing an Online Update Through Console

You can perform an online update through console to install the SLES and Advanced Authentication appliance updates. To initialize the updates, perform the following steps:

1. (Optional) Run the following command to register as a root user:

```
suse_register -a regcode-aauth=xxxxxxxxxxxx -a email=user@example.com -L /tmp/
register.txt
```

2 Run the following command to add a SLES repository:

```
zypper ar https://nu.novell.com/repo/\$RCE/AAuth-Appliance-6.0-OS/sle-12-
x86_64/ SLES
```

3 Run the following command to add Advanced Authentication appliance repository:

```
zypper ar https://nu.novell.com/repo/\$RCE/AAuth-Appliance-6.0-Product/sle-12-
x86_64/ AAF
```

4 Run the following command `to refresh the configured repositories:`

zypper refresh

5 Run the following command to updated all packages:

zypper up

NOTE: After adding and refreshing the repositories, you can also update the packages from the **Appliance Configuration console > Online Update > Update Now** instead of performing Step 5.

Adding Additional Hosts to the Hosts File

You can add additional entries to the `hosts` file for the Advanced Authentication appliance. You must add the entry to the `/etc/opt/novell/base/hosts.appliance` file. This is a manual process. You cannot change the host entries in any other way.

1 Access the command line console of the appliance.

2 Navigate to `/etc/opt/novell/base/hosts.appliance`.

3 Open the file in a text editor, then add the additional entries to the `hosts` file.

4 Save and close the file.

5 Reboot the appliance.

Performing a Product Upgrade

You can upgrade your appliance using the **Product Upgrade** option.

For migrating from Advanced Authentication 5 to 6.0, see “Migrating Advanced Authentication to 6.0” section.

This option will work in a future release of Advanced Authentication.

Rebooting or Shutting Down the Appliance

You might need to initiate a graceful shutdown or to restart the appliance for maintenance. It is recommended to use the Configuration Console options than Power Off/On option in the hypervisor's VM management tool.

1 Log in to the Configuration Console as the `root` user.

2 In the upper right corner of the Appliance Configuration pane, click **Reboot** or click **Shutdown**.

Logging Out

For security reasons, you should sign out to exit your management session with the appliance, then close your web browser. Your session terminates automatically when you close your web browser.

To sign out of the Configuration Console:

1. In the upper-right corner of the Configuration Console page, next to the user name, click **Logout**.
2. Close the web browser.

5 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 have installed 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 change 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 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.

   NOTE: FIPS 140-2 is enabled by default to comply with the FIPS 140-2 encryption.

7. Click **Next**.
8. Click three download icons on the lower-right corner to download the respective log files as follows:
   - web server log (`uwsgi.log`)
   - super user log (`root_commander.log`)
   - replication log (`symds.log`)

     NOTE: The replication log may not be available until the database replication begins.

     It is recommended to download the log files during restart process because the download icons are not displayed after the restart process is complete.

     Log files contain all actions that occur during the server installation and initial database replication. If you experience problems while installing the server, you can consult the log files to troubleshoot.

Configuring YubiHSM

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

To configure usage of the hardware security module, perform the following steps 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 after 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 using YubiHSM on the **Create encryption key** screen. After 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. Click **Next**.

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 configuration to create an enterprise key during configuration of DB Slave server, the connected YubiHSM that is configured when the master's database is copied to the DB Slave server.

---

6 Migrating Advanced Authentication to 6.0

You cannot upgrade from Advanced Authentication 5.6 to 6.0. However, you can export the configurations of the database from Advanced Authentication 5.6 to 6.0. After you install Advanced Authentication 6.0, you can import all the configurations from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.0, you must first upgrade from Advanced Authentication 5.5 to 5.6. Then, you must install 6.0 and import the configurations from 5.6.

For information about how to export and import the configurations, see "Exporting and Importing the Database" in the *Advanced Authentication - Administration* guide.

To migrate 5.6 to Advanced Authentication 6.0, perform the following steps:

1. Deploy the Advanced Authentication Global Master 6.0 server. For more information, see Configuring the Global Master server.
2. Migrate the database.

   To do this, you must export the database in 5.6 and import the database in 6.0.

   For information about how to export and import the configurations, see "Exporting and Importing the Database" in the *Advanced Authentication - Administration* guide.

   NOTE: By default, for the existing customers, the first 6.0 server where the database is imported will be the new Global Master server (GMS) of the cluster.
3. Deploy other Advanced Authentication servers in the cluster.

   For more information about clustering, see Configuring a Cluster in the *Advanced Authentication - Administration* guide.
4. Reconfigure the third-party integrations to point them to the new server address.

   For example, Advanced Authentication integrates with ADFS through the SAML or OAuth event. After you migrate Advanced Authentication from 5.6 to 6.0, you must point all these third-party integrations to the new 6.0 server.
5. Create the **_aav6** DNS service location records for the new servers of the 6.0 cluster.

   For more information about how to set the DNS records in Windows Client, see "Setting DNS for Server Discovery" in the *Advanced Authentication - Windows Client* guide.
6. Upgrade the client packages on the endpoints.

NOTE

- It is recommended to upgrade a couple of Clients and perform the testing for a couple of days. Then upgrade the next portion of Clients and perform the testing for few more days. After this upgrade the rest of the Clients.
- Do not delete the **_aaa** service location records from DNS for the servers available in the 5.6 cluster unless all the endpoints are migrated Advanced Authentication to 6.0.

7 Troubleshooting

This chapter contains the following sections:

Viewing the Logs

To view the logs of Advanced Authentication appliance docker, specify the following path:

`/var/lib/docker/volumes/aaf_aucore-logs/_data`

The `/var/lib/docker/volumes/aaf_aucore-logs/_data` contains logs related to aucore, replication, webauth, and so on.

To view the processes running on docker, run the following command

```
$ docker ps --format "{{.Names}}"
```

Managing Systemd Services

To start and stop the Systemd services, run the following commands:

```
systemctl status aauth
```

```
systemctl stop aauth
```

```
systemctl start aauth
```

Enabling SSH for Appliance

To enable SSH for appliance, run the following commands:

```
systemctl enable sshd.service
```

```
systemctl start sshd.service
```

`lsof -i :22` (to check that the port is listening)

NOTE: You can also perform these services in “Accessing System Services” of the Configuration portal.

Unable to Open the Advanced Authentication Portals After Upgrade

Issue: After updating Advanced Authentication, if you are unable to open the Advanced Authentication portals except for the Configuration portal (:9443). This issue occurs when the docker bypasses the proxy settings.

Workaround: As a solution, perform the following steps:

1. Run the command `/opt/aauth/start` to start the Advanced Authentication services manually.

   If an error message `ERROR: Get https://registry-1.docker.io/v2/: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)` is displayed then proceed to step 3.
2. Check the firewall settings. The Advanced Authentication server must be able to access `docker.io` through the port 443 (HTTPS).

   For more information about the firewall settings, see Configuring the Firewall.
3. Navigate to the path `/etc/systemd/system/docker.service.d`.
4. Create a file `http-proxy.conf` and specify the following parameters:
   - `[Service]`
   - `Environment="HTTP_PROXY=<proxy_URL>"`
   - `Environment="NO_PROXY=<proxy_exception>"`
   - `Environment="PROXY_USER=<username>:<password>"`

   For example,

   ```
   [Service]
   Environment="HTTP_PROXY=http://proxy.local:8080/"
   Environment="NO_PROXY=.local, .company.com"
   Environment="PROXY_USER=proxuser:password"
   ```
5. Save the configuration file.
6. Restart the server.