
Installation and Upgrade Guide

Advanced Authentication Server

Version 6.1

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/>.

Copyright © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About this Book	5
About NetIQ Corporation	7
1 System Requirements	9
2 Installing Advanced Authentication	11
Obtaining Advanced Authentication	11
Downloading the Purchased Version	11
Downloading the Trial Version	11
Installing Advanced Authentication	12
Deploying Advanced Authentication on Amazon Web Services	12
Prerequisites	13
Deployment Procedure	13
Deploying Advanced Authentication on Azure Kubernetes Services	13
Prerequisites	14
Deployment Procedure	14
3 Getting the Latest Online Updates	15
Registering to the Online Update Service	15
Performing an Online Update	16
Updating Advanced Authentication to a Field Patch	17
4 Upgrading Advanced Authentication	19
Upgrading Advanced Authentication Appliance 6.0 to 6.1	19
Migrating Advanced Authentication from Version 5.x	20
5 Troubleshooting	21
Viewing the Logs for Debugging	21
Managing Systemd Services	21
Enabling SSH for Appliance	21
The Advanced Authentication Portals are Inaccessible After Upgrade	22

About this Book

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

Intended Audience

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

Advanced Authentication Overview

For an overview about Advanced Authentication, see “[Advanced Authentication Overview](#)”.

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.

1 System Requirements

IMPORTANT: The Advanced Authentication 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 system requirements for Advanced Authentication appliance:

Requirement	Detail
Virtual Systems	<ul style="list-style-type: none">♦ Hyper-V Server 2016♦ 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 Processor must support SSE 4.2 instructions. For more information about how to check whether the CPU supports SSE 4.2 instructions, see Verifying SSE 4.2 Instructions on CPU .
Browsers	Any one of the following browsers: <ul style="list-style-type: none">♦ 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 (https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html) .

Requirement	Detail
LDAP Repositories	<p>Any one of the following repositories:</p> <ul style="list-style-type: none"> ♦ Microsoft Active Directory Services ♦ Microsoft Active Directory Lightweight Directory Services ♦ NetIQ eDirectory ♦ OpenLDAP ♦ OpenDJ ♦ Microsoft SQL Server 2016

Verifying SSE 4.2 Instructions on CPU

Ensure that CPU supports SSE 4.2 instructions.

To check whether your CPU supports the SSE 4.2 instructions, run the following command:

```
grep -q sse4_2 /proc/cpuinfo && echo "SSE 4.2 supported" || echo "SSE 4.2 not supported"
```

If your CPU supports SSE 4.2, the command returns a message `SSE 4.2 supported`.

2 Installing Advanced Authentication

This chapter includes the following topics:

- ♦ “Obtaining Advanced Authentication” on page 19
- ♦ “Installing Advanced Authentication” on page 20
- ♦ “Deploying Advanced Authentication on Amazon Web Services” on page 12
- ♦ “Deploying Advanced Authentication on Azure Kubernetes Services” on page 13

Obtaining Advanced Authentication

Advanced Authentication is available in two versions: trial and purchased.

- ♦ “Downloading the Full Version” on page 19
- ♦ “Downloading the Trial Version” on page 19

Downloading the Purchased 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 to download.

Downloading the Trial Version

You can download and install the trial version of Advanced Authentication to see how the product works.

To download the trial version:

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

Installing Advanced Authentication

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

- 1 Ensure that your environment complies with the [System Requirements](#).
- 2 Unpack the file `advancedauthappliance-x86_64-x.x-xxx.zip`, and use the `advancedauthappliance-x86_64-x.x-xxx.iso` file.
- 3 Mount the Advanced Authentication installation ISO file and boot the machine.
- 4 Select the **Install advancedauthappliance** option from the list.
- 5 Select **Yes** to delete all data in the SDA drive.
- 6 Select the appropriate language, read the license, and click **Accept**.
- 7 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 a 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 DNS servers.
- 8 Click **Finish** and wait for the appliance initialization to complete.
- 9 After a prompt to login is displayed on the console, you must wait for 15 minutes. Even after the wait, if you are unable to access the Advanced Authentication portals then reboot the appliance.

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 about time setting, see [Configuring Time Settings \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/time.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/time.html).

NOTE: For information about migrating Advanced Authentication appliance from version 5.x to 6.1, see [“Migrating Advanced Authentication from Version 5.x”](#).

WARNING: When you log in to the console as **root** and run **yast novell-vainit**, it is recommended to not select the **Reboot** or **Shutdown** option. Otherwise, you will not be able to access the web user interface when you reboot the appliance or start the appliance after shut down.

Deploying Advanced Authentication on Amazon Web Services

This section contains details about how to deploy Advanced Authentication on Amazon Web Services (AWS) using Kubernetes. You can deploy Advanced Authentication containers into Kubernetes clusters by using the Helm charts.

- ♦ [“Prerequisites” on page 13](#)
- ♦ [“Deployment Procedure” on page 13](#)

NOTE: The procedures in this section are based on the assumption that you know basics of how containers work.

Prerequisites

In addition to the system requirements of Advanced Authentication appliance, ensure that you have completed following tasks:

- ♦ Created an administrative account on Amazon Elastic Container Service for Kubernetes (Amazon EKS).
- ♦ Configured an Amazon EKS cluster.

For more information about how to configure an Amazon EKS cluster, see [Getting Started with Amazon EKS \(https://docs.aws.amazon.com/eks/latest/userguide/getting-started.html\)](https://docs.aws.amazon.com/eks/latest/userguide/getting-started.html).

- ♦ Installed `kubectl` and configured it to work with the Amazon EKS.

For more information about installing and configuring `kubectl`, see [install kubectl \(https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html\)](https://docs.aws.amazon.com/eks/latest/userguide/install-kubectl.html) and [configure kubectl \(https://docs.aws.amazon.com/eks/latest/userguide/configure-kubectl.html\)](https://docs.aws.amazon.com/eks/latest/userguide/configure-kubectl.html).

Deployment Procedure

- 1 Download the `aaf-<version>-helm-chart.zip` file from [NetIQ Downloads \(https://dl.netiq.com\)](https://dl.netiq.com).

- 2 Unpack the zip file. You can view the `aaf-<version>.tgz` tar file.

- 3 Run the following command to unpack the tar file:

```
tar zxvf aaf-<version>.tgz
```

- 4 Run the following command to deploy three Advanced Authentication instances into the cluster:

```
helm install --namespace aaf-test --name=aaf-test-1 -set lb.enabled=true ./aaf/  
helm install --namespace aaf-test --name=aaf-test-2 -set lb.enabled=true ./aaf/  
helm install --namespace aaf-test --name=aaf-test-3 -set lb.enabled=true ./aaf/
```

- 5 Run the following command to get the IP addresses that are assigned to each Advanced Authentication instance in the cluster:

```
kubectl -n aaf-test get svc | grep LoadBalancer
```

NOTE: The Configuration Portal (port 9443) is not available for the Kubernetes environment. The [Managing the Appliance \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/ch-appliance-config.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/ch-appliance-config.html) is only relevant for the appliance.

Deploying Advanced Authentication on Azure Kubernetes Services

This section contains details about how to deploy Advanced Authentication on Azure Kubernetes Service. You can deploy Advanced Authentication containers into Kubernetes clusters by using the Helm charts.

NOTE: The procedures in this section are based on the assumption that you know basics of how containers work.

Prerequisites

In addition to the system requirements of Advanced Authentication appliance, ensure that you have completed following tasks:

- ♦ Created an administrative account on Azure Kubernetes Services (AKS)
- ♦ Configured a Microsoft AKS cluster.

For more information about how to configure a Microsoft AKS cluster, see [Get started tutorial \(https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough\)](https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough).

- ♦ Installed `kubectl` and configured it to work with Microsoft AKS.

Deployment Procedure

- 1 Download the `aaf-<version>-helm-chart.zip` file from [NetIQ Downloads \(https://dl.netiq.com\)](https://dl.netiq.com).

- 2 Unpack the zip file. You can view the `aaf-<version>.tgz` tar file.

- 3 Run the following command to unpack the tar file:

```
tar zxvf aaf-<version>.tgz
```

- 4 Run the following command to deploy three Advanced Authentication instances into the cluster:

```
helm install --namespace aaf-test --name=aaf-test-1 -set lb.enabled=true ./aaf/
```

```
helm install --namespace aaf-test --name=aaf-test-2 -set lb.enabled=true ./aaf/
```

```
helm install --namespace aaf-test --name=aaf-test-3 -set lb.enabled=true ./aaf/
```

- 5 Run the following command to get the IP addresses that are assigned to each Advanced Authentication instance in the cluster:

```
kubectl -n aaf-test get svc | grep LoadBalancer
```

NOTE: The Configuration Portal (port 9443) is not available for the Kubernetes environment. The [Managing the Appliance \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/ch-appliance-config.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/ch-appliance-config.html) is only relevant for the appliance.

3 Getting the Latest Online Updates

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

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 Firewall](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html) (<https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html>).

This chapter contains the following sections:

- ♦ “[Registering to the Online Update Service](#)” on page 15
- ♦ “[Performing an Online Update](#)” on page 16
- ♦ “[Updating Advanced Authentication to a Field Patch](#)” on page 17

Registering to the Online Update Service

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** as:
 - ♦ Micro Focus Customer Center
- 5 Specify the following information about the [Customer Center](https://www.netiq.com/customercenter) (<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).
Perform the following steps to obtain the activation key:
 1. Log in to [Micro Focus Customer Center](https://www.netiq.com/customercenter) (<https://www.netiq.com/customercenter>).
 2. Click **Software > Entitled Software > NetIQ Advanced Authentication > Keys**.
 3. Make a note of the applicable key.
 - ♦ Select any of the following options to allow data send:
 - ♦ Hardware Profile
 - ♦ Optional information
- 6 Click **Register**.

Wait while the appliance registers with the service.

7 Click **OK**.

After you register 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.

You can perform the following actions after registration:

- ♦ **Update Now:** Perform the following steps to install the downloaded updates:
 1. Create snapshots for all Advanced Authentication servers.
 2. Click **Update Now** to install the downloaded updates.
 3. Restart the server to complete the update. It may take up to 10 minutes to get the required services started.
 4. Log in to the Advanced Authentication Administration portal on the upgraded server.
 5. Click **Cluster > Conflicts** to resolve the conflicts.
 6. Repeat steps Step 2 to Step 5 for database servers and Step 2 to Step 4 for web servers.
- ♦ **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

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=xxxxxxxxxxxxx -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-6.1-OS/sle-12-x86_64/ SLES
```

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

```
zypper ar https://nu.novell.com/repo/\$RCE/AAuth-Appliance-6.1-Product/sle-12-x86_64/ AAF
```

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

```
zypper refresh
```

- 5 Run the following command to update all packages:

```
zypper up
```

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

Updating Advanced Authentication to a Field Patch

You can add patches provided by the product team in the **Field Patch** tab. A field patch is not a complete patch and you must use it only until a complete patch is released.

Perform the following steps to apply a field patch:

- 1 Disable all other updates for the appliance. Else, the field patch might be overwritten.
- 2 Create snapshots for all Advanced Authentication servers.
- 3 [Log in](#) to the Configuration console as the `vaadmin` user.
- 4 Click **Field Patch**, then follow the prompts to install the patch update.
- 5 (Conditional) Install a downloaded patch update:
 - 5a Download the Advanced Authentication patch update file from the [Patch Finder \(https://dl.netiq.com/patch/finder/\)](https://dl.netiq.com/patch/finder/) website.
 - 5b In the **Install a Downloaded Patch** section, click **Browse**.
- 6 (Conditional) Uninstall a patch update:

You might not be able to uninstall some patch updates.

 - 6a In the **Patch Name** column of the **Field Patch** list, select the patch update that you want to uninstall.
 - 6b Click **Uninstall Latest Patch**.
- 7 (Conditional) Click **Download Log File** for the appropriate patch update.

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

- 8 Restart the server to complete the update. It may take up to 10 minutes to get the required services started.
- 9 Log in to the Advanced Authentication Administration portal on the upgraded server.
- 10 Click **Cluster > Conflicts** to resolve the conflicts.
- 11 Repeat steps [Step 3](#) to [Step 10](#) for database servers and [Step 3](#) to [Step 9](#) for web servers.

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 \(https://lukerawlins.com/opensuse-patch-vs-update/\)](https://lukerawlins.com/opensuse-patch-vs-update/).

4 Upgrading Advanced Authentication

This section describes how to upgrade Advanced Authentication to the latest version through the Configuration console.

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**.

IMPORTANT: It is recommended to upgrade when users' activities are less. The period of upgrade must be reduced as the replication of databases that do not synchronize can break the database servers.

This section includes the following topics:

- [“Upgrading Advanced Authentication Appliance 6.0 to 6.1” on page 19](#)
- [“Migrating Advanced Authentication from Version 5.x” on page 20](#)

Upgrading Advanced Authentication Appliance 6.0 to 6.1

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

For migrating from Advanced Authentication 5.x to 6.1, see [“Migrating Advanced Authentication from Version 5.x”](#) section.

The **Product Upgrade** option is displayed only when you can use it to upgrade the service hosted on your appliance.

To upgrade Advanced Authentication Appliance 6.0 to 6.1, perform the following steps:

- 1 Create snapshots for all Advanced Authentication servers.
- 2 Click the **Online Update** tab and apply all updates.
- 3 Click the **Product Upgrades** tab and upgrade the appliance.
- 4 Restart the server to complete the update.
It may take up to 10 minutes to get the required services started.
- 5 Log in to the Advanced Authentication Administration portal on the upgraded server.
- 6 Click **Cluster > Conflicts** to resolve the conflicts.
- 7 Repeat steps [Step 3](#) to [Step 6](#) for database servers and [Step 3](#) to [Step 5](#) for web servers.

Migrating Advanced Authentication from Version 5.x

You cannot upgrade from Advanced Authentication 5.0 to 6.1. However, you can export the configurations of the database from Advanced Authentication 5.6 to 6.1. After you install Advanced Authentication 6.1, you can import all configuration details from 5.6.

For example, to upgrade from Advanced Authentication 5.5 to 6.1, you must first upgrade from Advanced Authentication 5.5 to 5.6. Then, install Advanced Authentication 6.1 and import the configuration details 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 5.0 to Advanced Authentication 6.1, perform the following steps:

- 1 Deploy the Advanced Authentication Global Master 6.1 server. For more information about deploying the Global Master, see [Configuring Global Master Server \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/configuringglobalmaster.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/configuringglobalmaster.html).
- 2 Export the database of Advanced Authentication 5.6 and import it to the database of Advanced Authentication 6.1.

For information about how to export and import the configurations, see “[Exporting and Importing the Database](#)” in the *Advanced Authentication - Administration* guide.

NOTE: The first 6.1 server where the database is imported becomes the new Global Master server of the cluster by default.

- 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 6.1, you must redirect all these third-party integrations to the new 6.1 server.
- 5 Create the `_aav6` DNS service location records for the new servers of the 6.1 cluster.
For more information about how to set the DNS records in Windows Client, see “[Setting a DNS for Advanced Authentication Server Discovery](#)” in the *Advanced Authentication - Windows Client* guide.
- 6 Upgrade the client packages on the endpoints.

NOTE

- ♦ It is recommended to not migrate all clients together. Instead, first migrate a few clients and complete the testing for these. Then upgrade the other set of clients and perform the testing. After that, complete the migration of the remaining clients.
 - ♦ Do not delete the `_aaa` service location records from DNS for the servers available in the Advanced Authentication 5.6 cluster until all endpoints are migrated to Advanced Authentication 6.1.
-

5 Troubleshooting

This chapter contains the following sections:

- ♦ [“Viewing the Logs for Debugging” on page 21](#)
- ♦ [“Managing Systemd Services” on page 21](#)
- ♦ [“The Advanced Authentication Portals are Inaccessible After Upgrade” on page 22](#)

Viewing the Logs for Debugging

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

You can reboot Advanced Authentication from the command prompt.

To start the Systemd services, run the following command:

```
systemctl start aauth
```

To stop the Systemd services, run the following command:

```
systemctl stop aauth
```

To view the status of Advanced Authentication services running on the appliance, run the following command:

```
systemctl status aauth
```

Enabling SSH for Appliance

To enable Advanced Authentication server to interact with the clients, you must enable the SSH option.

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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/services.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/services.html) of the Configuration console.

The Advanced Authentication Portals are Inaccessible 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: Perform the following steps:

- 1 Execute the command `/opt/aaauth/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 \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/firewall.html).

- 3 Ensure the proxy settings are configured in YaST.

For more information about the proxy settings, see [Configuring the Proxy Settings \(https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/network.html#t46ltypcv7a\)](https://www.netiq.com/documentation/advanced-authentication-61/server-administrator-guide/data/network.html#t46ltypcv7a)

- 4 Navigate to the path `/etc/systemd/system/docker.service.d`.

- 5 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"
```

- 6 Save the configuration file.
- 7 Restart the server.