Administration Guide

Advanced Authentication

Version 5.5

MICRO FOCUS

Legal Notice

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

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation **7**
About this Book **9**

1 Advanced Authentication Overview **11**

1.1 How Is Advanced Authentication Better Than Other Solutions . . . 11
1.2 Key Features . . . 11
1.3 Advanced Authentication Server Components . . . 12
1.3.1 Administration Portal . . . 12
1.3.2 Self-Service Portal . . . 13
1.3.3 Helpdesk Portal . . . 13
1.3.4 Reporting Portal . . . 13
1.4 Architecture . . . 14
1.4.1 Basic Architecture . . . 14
1.4.2 Enterprise Level Architecture . . . 15
1.4.3 Enterprise Architecture With A Load Balancer . . . 17
1.5 Terminologies . . . 18
1.5.1 Authentication Method . . . 18
1.5.2 Authentication Chain . . . 18
1.5.3 Authentication Event . . . 18
1.5.4 Endpoint . . . 18
1.5.5 Tenant . . . 18

Part I Installing and Upgrading Advanced Authentication **19**

2 System Requirements **21**

3 Installing Advanced Authentication **23**

4 Upgrading Advanced Authentication **25**

Part II Configuring Advanced Authentication **27**

5 Configuring the Basic Settings **29**

5.1 Configuring Host Name . . . 29
5.2 Configuring HTTP Proxy Server . . . 30
5.3 Configuring Appliance Networking . . . 30
5.4 Configuring Time and NTP Servers . . . 30
5.5 Rebooting Appliance . . . 30
5.6 Shutting Down Appliance . . . 31

6 Configuring Global Master Server **33**

6.1 Configuring YubiHSM . . . 33

7 Logging In to the Advanced Authentication Administrative Portal 35

8 Configuring Advanced Authentication Server Appliance 37

8.1 Adding a Tenant . . . 37
8.2 Adding a Repository . . . 38
8.2.1 Advanced Settings . . . 39
8.2.2 Used Attributes . . . 42
8.2.3 Local Repository . . . 45
8.3 Configuring Methods . . . 46
8.3.1 Bluetooth . . . 46
8.3.2 Card . . . 47
8.3.3 Email OTP . . . 47
8.3.4 Emergency Password . . . 48
8.3.5 Fingerprint . . . 48
8.3.6 FIDO U2F . . . 49
8.3.7 LDAP Password . . . 51
8.3.8 OATH OTP . . . 51
8.3.9 Password . . . 53
8.3.10 PKI . . . 54
8.3.11 Radius Client . . . 55
8.3.12 SMS OTP . . . 56
8.3.13 Security Questions . . . 56
8.3.14 Smartphone . . . 58
8.3.15 Swisscom Mobile ID . . . 60
8.3.16 Voice . . . 60
8.3.17 Voice OTP . . . 61
8.4 Creating a Chain . . . 62
8.5 Configuring Events . . . 63
8.5.1 ADFS . . . 66
8.5.2 AdminUI . . . 66
8.5.3 Authenticators Management . . . 66
8.5.4 Helpdesk . . . 67
8.5.5 Helpdesk User . . . 67
8.5.6 Linux Logon . . . 67
8.5.7 Mac OS logon . . . 67
8.5.8 NAM . . . 67
8.5.9 NCA . . . 67
8.5.10 Report logon . . . 68
8.5.11 Windows logon . . . 68
8.5.12 Radius Server . . . 68
8.6 Managing Endpoints . . . 77
8.7 Configuring Policies . . . 79
8.7.1 Admin UI Whitelist . . . 80
8.7.2 Authenticator management options . . . 80
8.7.3 Cache Options . . . 81
8.7.4 CEF log forwarding . . . 81
8.7.5 Delete me options . . . 83
8.7.6 Endpoint Management Options . . . 83
8.7.7 Helpdesk Options . . . 83
8.7.8 HTTPS Options . . . 84
8.7.9 Kerberos SSO Options . . . 84
8.7.10 Last Logon Tracking Options . . . 85
8.7.11 Lockout Options . . . 85
8.7.12 Login Options . . . 85
8.7.13 Logo . . . 86
8.7.14 Logon Filter for AD . . . 86
8.7.15 Mail Sender . . . 86
8.7.16 Multitenancy Options . . . 87

8.7.17 Password Filter for AD . . . 88
8.7.18 SMS Sender . . . 88
8.7.19 Services Director Options . . . 90
8.7.20 Voice Sender . . . 91
8.7.21 Geo fencing options . . . 92
8.7.22 Event categories . . . 93
8.7.23 SAML 2.0 options . . . 93
8.8 Configuring Server Options . . . 93
8.8.1 Enabling Web Authentication . . . 94
8.8.2 Uploading Keytab File . . . 94
8.9 Adding a License . . . 95

9 Configuring Default Ports for Advanced Authentication Server Appliance 97

10 Configuring a Cluster 99

10.1 Registering a New Site . . . 100
10.2 Registering a New Server . . . 101
10.3 Resolving Conflicts . . . 103
10.4 How to Install a Load Balancer for Advanced Authentication Cluster . . . 104
10.4.1 Installing nginx on Ubuntu 16.04 . . . 104
10.4.2 Configuring nginx . . . 104
10.4.3 Configuring Advanced Authentication Client . . . 107
10.5 Restoring Operability When a Global Master Server is Broken . . . 107

11 Authentication Methods Enrollment 109

12 Configuring Integrations 111

12.1 Configuring Integration with Barracuda SSL VPN . . . 111
12.2 Configuring Integration with Citrix NetScaler . . . 113
12.3 Configuring Integration with Dell SonicWall SRA EX-Virtual appliance . . . 114
12.4 Configuring Integration with FortiGate . . . 116
12.5 Configuring Integration with OpenVPN . . . 117
12.5.1 User Account Locks After Three Successful Authentications with SMS AP to OpenVPN . . . 118
12.6 Configuring Integration with Salesforce . . . 119
12.7 Configuring Integration with NetIQ Access Manager (SAML) . . . 121

Part III Maintaining Advanced Authentication 123

13 Reporting 125

14 Logging 127

15 Troubleshooting 139

15.1 Fatal error while trying to deploy ISO file and install in graphic mode . . . 139
15.2 Partition Disks . . . 139
15.3 Networking Is Not Configured . . . 140
15.4 Error "Using a password on the command line interface can be insecure" . . . 140
15.5 The ON/OFF Switch Is Broken If the Screen Resolution Is 110% . . . 140
15.6 Error When Requesting For Update . . . 141

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 Administration Guide is intended for system administrators and describes the procedure of Advanced Authentication Server appliance configurations and deployment.

Intended Audience

This book provides information for individuals 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:

- Section 1.1, “How Is Advanced Authentication Better Than Other Solutions,” on page 11
- Section 1.2, “Key Features,” on page 11
- Section 1.3, “Advanced Authentication Server Components,” on page 12
- Section 1.4, “Architecture,” on page 14
- Section 1.5, “Terminologies,” on page 18

1.1 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.

1.2 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, 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. You can enable FIPS 140-2 compliant encryption for new installations.
- **Supports Localization**: Advanced Authentication supports several languages such as Arabic, Chinese, Dutch, and Danish.

1.3 Advanced Authentication Server Components

Advanced Authentication server comprises of the following components:

- **Administration Portal**

  For more information, see Section 1.3.1, “Administration Portal,” on page 12
- **Self-Service Portal**

  For more information, see Section 1.3.2, “Self-Service Portal,” on page 13
- **Helpdesk Portal**

  For more information, see Section 1.3.3, “Helpdesk Portal,” on page 13
- **Reporting Portal**

  For more information, see Section 1.3.4, “Reporting Portal,” on page 13

1.3.1 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".

- **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".
- **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".
- **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".
- **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".
- **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".

1.3.2 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 to enable users to access the Self-Service portal. For more information on Self-Service portal, see *Advanced Authentication- User* guide.

1.3.3 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 *Helpdesk Administration* guide.

1.3.4 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".

1.4 Architecture

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

- Basic Architecture

  For more information, see Section 1.4.1, “Basic Architecture,” on page 14
- Enterprise Level Architecture

  For more information, see Section 1.4.2, “Enterprise Level Architecture,” on page 15
- Enterprise Architecture With A Load Balancer

  For more information, see Section 1.4.3, “Enterprise Architecture With A Load Balancer,” on page 17

1.4.1 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.

1.4.2 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 15 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.

  NOTE: If the Global Master is down, new sites cannot be added.

- **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 that can be DB Server 1 and DB Server 2. 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 can interact with every server that contain a database.

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 datacenter with Global Master, you must have LDAP servers for all the used domains.

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.

1.4.3 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 17 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. There is no limit for the number of web servers.
- **Load Balancer**: A load balancer provides an ability to serve authentication requests from **External Endpoints**. A load balancer is a third-party component. It is located in DMZ and can be configured to interact with all Advanced Authentication servers.

NOTE: To view an example of configuring a load balancer for an Advanced Authentication cluster, see "How to Install a Load Balancer for Advanced Authentication Cluster".

1.5 Terminologies

- Section 1.5.1, "Authentication Method," on page 18
- Section 1.5.2, "Authentication Chain," on page 18
- Section 1.5.3, "Authentication Event," on page 18
- Section 1.5.4, "Endpoint," on page 18
- Section 1.5.5, "Tenant," on page 18

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.5.4 Endpoint

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

1.5.5 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.

Installing and Upgrading Advanced Authentication

- Chapter 2, “System Requirements,” on page 21
- Chapter 3, “Installing Advanced Authentication,” on page 23
- Chapter 4, “Upgrading Advanced Authentication,” on page 25

2 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:

NOTE: The server machine must contain only one network interface controller.

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

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

- Microsoft Internet Explorer 10, 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.

3 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**.

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

4 Upgrading Advanced Authentication

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

NOTE: To upgrade Advanced Authentication 5.2 and prior versions, contact NetIQ Technical Support.

To upgrade Advanced Authentication 5.3 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.

   NOTE: An error `Database is restarting (AuError)` might be displayed. Wait to check for updates.

4. Click **Check for updates** and then **Update**.

   NOTE: 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.

WARNING: 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:

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.

II Configuring Advanced Authentication

Advanced Authentication Server Appliance is intended for processing requests for authentication coming from the Advanced Authentication system users.

This chapter contains the following sections:

- Chapter 5, “Configuring the Basic Settings,” on page 29
- Chapter 6, “Configuring Global Master Server,” on page 33
- Chapter 7, “Logging In to the Advanced Authentication Administrative Portal,” on page 35
- Chapter 8, “Configuring Advanced Authentication Server Appliance,” on page 37
- Chapter 9, “Configuring Default Ports for Advanced Authentication Server Appliance,” on page 97
- Chapter 10, “Configuring a Cluster,” on page 99
- Chapter 11, “Authentication Methods Enrollment,” on page 109
- Chapter 12, “Configuring Integrations,” on page 111

5 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:

- Section 5.1, “Configuring Host Name,” on page 29
- Section 5.2, “Configuring HTTP Proxy Server,” on page 30
- Section 5.3, “Configuring Appliance Networking,” on page 30
- Section 5.4, “Configuring Time and NTP Servers,” on page 30
- Section 5.5, “Rebooting Appliance,” on page 30
- Section 5.6, “Shutting Down Appliance,” on page 31

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

5.1 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. Specify an applicable host name and press **ENTER** to apply changes.
4. Restart the server.

5.2 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.

5.3 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.

5.4 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.

5.5 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**.

5.6 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**.

6 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.

6.1 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.

7 Logging In to the Advanced Authentication Administrative Portal

After setting up an applicable server mode, the Advanced Authentication Administrative Portal is displayed. To log in to Advanced Authentication Administrative Portal, perform the following steps:

1. Enter administrator's credentials in the following format: repository\user (**local\admin** by default). Click **Next**.
2. The **Admin Password** chain is selected by default as the only available method. Enter the password you specified while setting up the DB Master server mode and click **Next**.
3. The main page of Advanced Authentication Administrative Portal is displayed.
4. You can change the language from the drop-down list on the top-right corner of the Advanced Authentication Administrative Portal.

   The supported languages are: Arabic, Chinese Simplified, Chinese Traditional, Danish, Dutch, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, Hebrew, and Swedish.

IMPORTANT: Password of **local\admin** account expires by default. For uninterrupted access to the Administration Portal, it is strongly recommended to add authorized users or group of users from a configured repository to the **FULL ADMINS** role. Then you must assign chains, which contain methods that are enrolled for users, to the **AdminUI** event (at a minimum with an LDAP Password).

NOTE: It is not recommended to access the Advanced Authentication Administrative Portal through a load balancer, as the replicated data may not be displayed.

---

8 Configuring Advanced Authentication Server Appliance

In the Administration Portal, you can configure and manage various authentication settings such as methods, events, and so on. You can also configure various policies that are required for authentication.

Advanced Authentication Administrative Portal contains the Help option that guides you on how to configure all settings for your authentication framework. The Help section provides you with information on the specific section you are working on.

This chapter contains the following sections:

- Section 8.1, “Adding a Tenant,” on page 37
- Section 8.2, “Adding a Repository,” on page 38
- Section 8.3, “Configuring Methods,” on page 46
- Section 8.4, “Creating a Chain,” on page 62
- Section 8.5, “Configuring Events,” on page 63
- Section 8.6, “Managing Endpoints,” on page 77
- Section 8.7, “Configuring Policies,” on page 79
- Section 8.8, “Configuring Server Options,” on page 93
- Section 8.9, “Adding a License,” on page 95

8.1 Adding a Tenant

A tenant is a company with a group of users sharing common access with specific privileges. Each company has a Tenant Administrator. Multitenancy is an optional feature where a single instance of Advanced Authentication solution supports multiple tenants.

NOTE: Multitenancy is disabled by default. Before adding a tenant, enable Multitenancy. For more information on enabling multitenancy, see Multitenancy options.

To add a tenant, perform the following steps:

1. Click **Tenants**.
2. Click **Add**.
3. Specify the name, description, and password for the tenant administrator.
4. Click **Save**.

NOTE: For the tenants added, you can view the number of configured repositories and the date of license expiration. Also on the **Edit tenant** page, you can view the number of users and change the password for the tenant administrator.

NOTE: A Tenant administrator can access the Advanced Authentication Administrative Portal with the credentials. A tenant administrator cannot add another tenant and cannot access the **Server options**, **Cluster**, and **Updates** sections. For more information, see Tenant Administration Guide.

8.2 Adding a Repository

A repository is a central location where the user's data is stored. In Advanced Authentication, the existing repository is not changed and is used only to retrieve user information. The authentication templates are stored inside the appliance and are fully encrypted.

Advanced Authentication supports any LDAP compliant directory. This can be Active Directory Domain Services, NetIQ edirectory, Active Directory Lightweight Directory Services, OpenLDAP, and OpenDJ.

When you add a new repository, you can match the users in the repository to authentication chains. You require only read permission to access a repository.

To add a repository, perform the following steps:

1. In the **Repositories** section, click **Add**.
2. Select an applicable repository type from the **LDAP type** list. The options are:
   - **AD** for Active Directory Domain Services
   - **AD LDS** for Active Directory Lightweight Domain Services
   - **eDirectory** for NetIQ eDirectory
   - **Other** for OpenLDAP, OpenDJ and other types

   For **AD**, a repository name is automatically set to NetBIOS name of domain. For other LDAP types, you need to enter it in **Name**.
3. Specify a container for the users in **Base DN**. When you select the **Subtree** option, Advanced Authentication performs a search for users in all the child nodes. You can change the search scope by selecting the **Search one level only** option.
4. Specify a user account in **User** and enter the password of the user in **Password**. Ensure that user's password has no expiry.
5. You can specify a container for the groups in **Group DN (optional)**. When you select the **Subtree** option, Advanced Authentication performs a search for the groups in all the child nodes. You can change the search scope by selecting the **Search one level only** option.
6. If you have selected **AD** as the **LDAP type**, select **DNS discovery** if you want to find LDAP servers automatically. Specify the **DNS zone** and **Site name** (optional) and click **Perform DNS Discovery**.

   NOTE: For LDAPS Servers you must have the SRV records on your DNS server:
   - Name: _ldap
   - Protocol: _tcp
   - Port: 636

   If you want to add LDAP servers manually, select **Manual setting.**
7. Click **Add server**. You can add the different servers in your network. The list is used as a pool of servers, each time the connection is open a random server is selected in the pool and unavailable servers are discarded.

8 Specify an LDAP server's **Address** and **Port**. Turn **SSL** to **ON** to use the SSL technology (if applicable). Click **Save**, next to server's credentials. Add additional servers (if applicable).

9 You can also expand Advanced Settings if you need to configure custom attributes. This is required for OpenDJ, OpenLDAP and in some cases for NetIQ edirectory.

10 Click **Save** to verify and save the specified credentials.

NOTE: If you use NetIQ eDirectory with the option **Require TLS for Simple Bind with Password** enabled, you may get the error: `Can't bind to LDAP: confidentialityRequired`. To fix the error, you must either disable the option or do the following:

1. Set **Client Certificate** to **Not Requested** in the NetIQ eDirectory Administration Portal - **LDAP - LDAP Options - Connections** tab.
2. Ensure that you set a correct port number and select **SSL** in the Repository settings.
3. Click **Sync now** in block with the added repository.

NOTE: You can change the search scope and the **Group DN (optional)** functionality now. In Advanced Authentication 5.2 it you had to specify a common **Base DN** for users and groups.

To check the sync status of a repository, click **Edit** and you can view the information in **Last sync**. Click **Full sync** to perform a complete synchronisation of the repository.

Advanced Authentication performs an automatic synchronization of modified objects (fastsync) on an hourly basis for AD. The complete synchronization (fullsync) is performed on a weekly basis.

NOTE: If an LDAP server is unavailable for 2.5 seconds, Advanced Authentication excludes it from LDAP requests for a period of 3 minutes.

8.2.1 Advanced Settings

Expand **Advanced Settings** by clicking **+**. The settings allow you to customize attributes that Advanced Authentication reads from a repository. The following list describes the different attributes in the Advanced Settings:

- “User lookup attributes” on page 39
- “User name attributes” on page 40
- “User mail attributes” on page 40
- “User cell phone attributes” on page 40
- “Group lookup attributes” on page 40
- “Group name attributes” on page 40
- “Verify SSL Certificate” on page 41
- “Enable paged search” on page 41
- “Enable Nested Groups Support” on page 42

User lookup attributes

Advanced Authentication checks the specified attributes for an entered user name.

For Active Directory (AD), the default attributes are `sAMAccountName` and `userPrincipalName`. For other repositories, `cn` is the default attribute.

User name attributes

Advanced Authentication shows a name from a first non-empty specified field for an entered user name.

For AD, the default attributes are `sAMAccountName` and `userPrincipalName`. For other repositories, `cn` is the default attribute.

User mail attributes

Advanced Authentication checks the specified attributes to get a user's email address.

Default attributes are `mail` and `otherMailbox`.

User cell phone attributes

Advanced Authentication checks the specified attributes to get a user's phone number. These attributes are used for methods such as SMS OTP, Voice, and Voice OTP. Previously, the first attribute of **User cell phone attributes** was used as a default attribute for authenticating with SMS OTP, Voice, and Voice OTP methods. Now users can use different phone numbers for these methods. For example, Bob wants to authenticate with SMS OTP, Voice, and Voice OTP methods. He has a cell pone number, a home phone number, and an ip phone number and wants to use these numbers for each of these methods, which is possible by defining in the respective settings of these methods.

Default attributes: `mobile`, `otherMobile`.

NOTE: If you have multiple repositories, you must use the same configuration of **User cell phone attributes** for all the repositories.

Group lookup attributes

Advanced Authentication checks the specified attributes for an entered group name.

For AD, the default attribute is `sAMAccountName`. For other repositories, `cn` is the default attribute.

Group name attributes

Advanced Authentication shows a name from a first non-empty specified field for an entered group name.

For AD, the default attribute is `sAMAccountName`. For other repositories, `cn` is the default attribute.

Advanced Authentication supports the RFC 2037 and RFC 2037 bis. RFC 2037 determines a standard LDAP schema and contains a `memberUid` attribute (POSIX style). RFC 2037 bis determines an updated LDAP schema and contains a member attribute. AD, LDS, eDir support RFC 2037 bis. `OpenLDAP` contains `posixAccount` and `posixGroup` that follows RFC 2037.

The following attributes are supported:

User object class

Default value: `user`.

Value for OpenDJ, OpenLDAP: `person`.

Group object class

Default value: `group`.

Value for OpenDJ: `groupOfNames`.

Value for OpenLDAP: `posixGroup`.

Group member attribute

Default value: `member`.

Value for OpenDJ: `member`.

Value for OpenLDAP: `memberUid`.

If a required group contains `groupOfNames` class, disable **POSIX style groups**. If the group contains `posixGroup`, enable **POSIX style groups.**

- **User UID attribute**

  This attribute is available only when **POSIX style groups** is **ON**.

  Default value: `uid`.

Object ID attribute

This attribute is available only for **other LDAP type** only.

Default value: `entryUUID`.

NOTE: For information on Logon filter settings (Legacy logon tag and MFA logon tag), see Configuring Logon Filter.

Verify SSL Certificate

Enable **Verify SSL Certificate** to ensure that the LDAP connection to appliance is secured with a valid self-signed SSL certificate. This helps to prevent any attacks on the LDAP connection and ensures safe authentication. Click **Choose File** to browse the self-signed certificate.

Enable paged search

The **Enable paged search** option allows LDAP repositories to support paged search in which the repositories can retrieve a result of a query set in small portions. By default, this option is set to **ON**. For openLDAP (with file-based backend), the option must be set to **OFF.**

NOTE: You must not disable the option for Active Directory repositories. It can also affect the performance on other supported repositories such as NetIQ eDirectory.

Enable Nested Groups Support

This option allows you to enable or disable nested groups support. By default **Enable nested groups support** option is set to **ON.**

If **Enable nested groups support** option is set to **ON,** then Advanced Authentication will authenticate all the users of the group and its nested groups assigned to a chain. If **Enable nested groups support** option is set to **OFF,** then Advanced Authentication will authenticate only the members of the group assigned to the chain. The members of the nested groups cannot access the chain. For example, If there is a group by name **All Users** assigned to **SMS Authentication** chain and All Users group has subgroups **Contractors** and **Suppliers.** When **Enable nested groups support** option is set to **ON,** then Advanced Authentication will authenticate **All Users** group and its nested groups **Contractors** and **Suppliers** for **SMS Authentication** chain. When the option is set to **OFF,** then Advanced Authentication will authenticate only the members of **All Users** group and the nested group members will not have access to **SMS Authentication** chain. This improves the logon performance to the appliance.

8.2.2 Used Attributes

The table describes the attributes used by the appliance in the supported directories.

Attribute Name	LDAP Name	Description	Type	Supported in Active Directory	Supported in LDS	Supported in eDirectory
CN (Common Name)	`CN`	An identifier of an object	String	✓	✓	✓
Mobile	`Mobile`	A phone number of an object's cellular or mobile phone	Phone number	✓	✓	✓
Email Address	`mail`	An email address of a user	Email address	✓	✓	✓
User-Principal-Name (UPN)	`userPrincipalName`	An Internet based format login name for a user	String	✓	✓	✓
SAM-Account-Name	`sAMAccountName`	The login name used to support clients and servers running earlier versions of operating systems such as Windows NT 4.0	String	✓	×	×
GUID	`GUID`	An assured unique value for any object	Octet String	×	×	✓
Object Class	`Object Class`	An unordered list of object classes	String	✓	✓	✓
Member	`Member`	A list that indicates the objects associated with a group or list	String	✓	✓	✓
User-Account-Control	`userAccountControl`	Flags that control the behavior of a user account	Enumeration	✓	×	×

Attribute Name	LDAP Name	Description	Type	Supported in Active Directory	Supported in LDS	Supported in eDirectory
ms-DS-User-Account-Control-Computed	`msDS-User-Account-Control-Computed`	Flags that are similar to `userAccountControl`, but the attribute's value can contain additional bits that are not persisted	Enumeration	✓	✓	×
Primary-Group-ID	`primaryGroupID`	A relative identifier (RID) for the primary group of a user	Enumeration	✓	×	×
Object-Guid	`objectGUID`	A unique identifier for an object	Octet String	✓	✓	×
object-Sid	`objectSid`	A Binary value that specifies the security identifier (SID) of the user	Octet String	✓	✓	×
Logon-Hours	`logonHours`	Hours that the user is allowed to logon to the domain	Octet String	✓	×	×
USN-Changed	`uSNChanged`	An update sequence number (USN) assigned by the local directory for the latest change including creation	Interval	✓	✓	×

NOTE: The `sAMAccountName` and `userPrincipalName` attributes are supported only for AD DS repository. In AD LDS and eDirectory repositories, the attributes are not supported.

1. LDAP queries for repository sync

1.1. AD DS and AD LDS queries

1.1.1. Search users

```
(&(usnChanged>=217368)(&(objectClass=user)(|(cn=*)(sAMAccountName=*)(userPrincipal
Name=*))))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'otherMobile', 'mobile', 'userAccountControl', 'cn', 'usnChanged',
'userPrincipalName', 'msDS-User-Account-Control-Computed', 'objectGUID', 'mail',
'otherMailbox', 'GUID']
```

1.1.2. Search groups

```
(&(usnChanged>=217368)(&(objectClass=group)(|(cn=*)(sAMAccountName=*))))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'userAccountControl', 'cn', 'usnChanged', 'msDS-User-Account-Control-Computed',
'objectGUID', 'GUID']
```

1.2. eDirectory queries

The queries are the same as for AD DS and AD LDS, except for 'usnChanged' (this filter is not used).

1.2.1. Search users

```
(&(objectClass=user)(|(cn=*)(sAMAccountName=*)(userPrincipalName=*)))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'otherMobile', 'mobile', 'userAccountControl', 'cn', 'userPrincipalName', 'msDS-
User-Account-Control-Computed', 'objectGUID', 'mail', 'otherMailbox', 'GUID']
```

1.2.2. Search groups

```
(&(objectClass=group)(|(cn=*)(sAMAccountName=*)))
```

Requested attributes:

```
['objectSID', 'sAMAccountName', 'objectClass', 'logonHours', 'primaryGroupId',
'userAccountControl', 'cn', 'msDS-User-Account-Control-Computed', 'objectGUID',
'GUID']
```

2. LDAP queries during logon

For AD LDS queries the attributes are same as for AD DS except for 'objectSid' (the filter

is not used in queries about membership in groups).

In the examples below, the username is pjones, base_dn is DC=company,DC=com

2.1. AD DS and AD LDS queries

2.1.1. Basic user information

```
(&(objectClass=user)(|(cn=pjones)(sAMAccountName=pjones)(userPrincipalName=pjones)
))
```

Requested attributes:

```
(&(objectClass=user)(objectGUID=\0f\d1\14\49\bc\cc\04\44\b7\bf\19\06\15\c6\82\55))
```

Requested attributes:

```
['otherMobile', 'GUID', 'userAccountControl', 'msDS-User-Account-Control-
Computed', 'mobile', 'primaryGroupId', 'cn', 'objectGUID', 'userPrincipalName',
'objectSID', 'mail', 'sAMAccountName', 'objectClass', 'logonHours',
'otherMailbox']
```

2.1.2 Group membership information for user

AD specific query using objectSid filter:

```
(|(member=CN=pjones,CN=Users,DC=company,DC=com)(objectSid=S-1-5-21-3303523795-
413055529-2892985274-513))
```

Requested attributes:

```
['GUID', 'userAccountControl', 'msDS-User-Account-Control-Computed',
'primaryGroupId', 'objectGUID', 'cn', 'objectSID', 'objectClass',
'sAMAccountName', 'logonHours']
```

2.3 Iteratively query about each group received from above query

```
(member=CN=Performance Monitor Users,CN=Builtin,DC=company,DC=com)
```

Requested attributes:

```
['GUID', 'userAccountControl', 'msDS-User-Account-Control-Computed',
'primaryGroupId', 'objectGUID', 'cn', 'objectSID', 'objectClass',
'sAMAccountName', 'logonHours']
```

2.2. eDirectory queries

2.2.1. Basic user information

```
(&(objectClass=user)(|(cn=pjones)(sAMAccountName=pjones)(userPrincipalName=pjones)
))
```

Requested attributes:

```
['otherMobile', 'GUID', 'userAccountControl', 'msDS-User-Account-Control-
Computed', 'mobile', 'primaryGroupId', 'cn', 'objectGUID', 'userPrincipalName',
'objectSID', 'mail', 'sAMAccountName', 'objectClass', 'logonHours',
'otherMailbox']
```

```
(&(objectClass=user)(GUID=\57\b6\c2\c1\b9\7f\4b\40\b9\70\5f\9a\1d\76\6c\d2))
```

Requested attributes:

```
['otherMobile', 'GUID', 'userAccountControl', 'msDS-User-Account-Control-
Computed', 'mobile', 'primaryGroupId', 'cn', 'objectGUID', 'userPrincipalName',
'objectSID', 'mail', 'sAMAccountName', 'objectClass', 'logonHours',
'otherMailbox']
```

2.2.2. Group membership information for user

```
(member=cn=pjones,o=AAF)
```

Requested attributes:

```
['GUID', 'userAccountControl', 'msDS-User-Account-Control-Computed',
'primaryGroupId', 'objectGUID', 'cn', 'objectSID', 'objectClass',
'sAMAccountName', 'logonHours']
```

8.2.3 Local Repository

To edit a local repository, perform the following steps:

1. Click **Edit** in the **LOCAL** section of **Repositories**.
2. In the **Global Roles** tab, you can manage Helpdesk or Security Officers as **ENROLL ADMINS** and Advanced Authentication Administrators as **FULL ADMINS**.

   By default, there are no ENROLL ADMINS and the account LOCAL\ADMIN is only specified as FULL ADMIN. You can change this by adding the user names from local or the used repositories in **Members**.
3. Click **Save**.
4. In the **Users** tab, you can manage the local users.

   To add the new local account, click **Add** and specify the required information of the user.

8.3 Configuring Methods

The Methods page contains settings that allow you to configure the authentication methods.

To configure an authentication method for Advanced Authentication, perform the following steps:

1. Open the **Methods** section. The list of available authentication methods are displayed.
2. Click **Edit** next to the authentication method.
3. Edit the configuration settings for a specific authentication method.
4. Click **Save**.

You can configure the following methods:

- Bluetooth - Enable reaction on device configuration.
- Card- Tap&Go policy configuration.
- Email OTP - Email message and One-Time Password related settings.
- Emergency Password - security settings of Emergency Password method.
- Fingerprint - a quality of fingerprint recognition settings.
- LDAP Password- an option which allows to save LDAP Password.
- OATH OTP - OATH TOTP/HOTP related settings. Also CSV/PSKC bulk import and token assignment.
- Password - security settings of local password.
- PKI- uploading trusted root certificates.
- Radius Client - settings for to a third-party RADIUS server.
- Security Questions - security questions and its security settings.
- Smartphone - Smartphone method settings.
- SMS OTP - One-Time Password related settings for SMS method.
- Swisscom Mobile ID - settings for the Swisscom mobile ID method.
- FIDO U2F - an option which allows to enable check of attestation certificate.
- Voice - security settings of Voice method.
- Voice OTP - settings for the Voice OTP method.

An authentication method itself cannot be linked to an event. You must create an Authentication Chain in order to configure the authentication for the user. It is also possible to create an Authentication chain with only one method in it.

For example: If you want to create Password and OTP authentication then you would create a chain with the Password and OTP methods in it. However, if you use only OTP for a certain event, then you can make an Authentication Chain using only the OTP in it.

8.3.1 Bluetooth

Advanced Authentication supports authentication using Bluetooth method. The settings allows to enable or disable the **Enable reaction on device removal** option.

By default **Enable reaction on device removal** option is enabled. When the **Enable reaction on device removal** option is enabled and logon to Windows is performed by Bluetooth, then Operating System automatically locks if the Bluetooth device is disabled or it is out of range.

NOTE: It is recommended to have Bluetooth method in a chain with another authentication method to increase security.

8.3.2 Card

Advanced Authentication supports the Microsoft policy Interactive logon: Smart card removal behavior that allows you to specify an action on the card event. You can configure it to perform a force log off or lock a user session when the user inserts a card to the reader. This is supported for Microsoft Windows only.

The **Enable Tap&Go** policy is located on the Card page of **Methods** section. By default, the policy is disabled and the card should be left on the reader when a user logs in. When the user takes off the card from the reader, the Windows Client runs an action that is specified in the Interactive logon: Smart card removal behavior policy. If the **Enable Tap&Go policy** is set to ON, users can tap a card to log in, to lock a session, or to log off (depending on Interactive logon: Smart card removal behavior policy) without leaving their cards on the readers.

NOTE: The policy is supported for Microsoft Windows only and it is not supported for the PKI authenticators.

8.3.3 Email OTP

The Email OTP authentication method sends an email to the user's e-mail address with a One-Time-Password (OTP). The user receives this OTP and needs to enter it on the device where the authentication is happening. This authentication method is best used with a second method like Password or LDAP Password in order to achieve multi-factor authentication and to prohibit malicious users from sending SPAM to a user's email box with authentication requests.

The following configuration options are available:

- **OTP Period**: the lifetime of an OTP token in seconds. By default 120 seconds.The maximum value for the OTP period is 360 seconds.
- **OTP Format**: the length of an OTP token. By default 6 digits.
- **Sender email**: the sender email address.
- **Subject**: the subject of the mail sent to the user.
- **Format**: format of an email message. By default, the plain text format is used. You can switch to HTML. HTML format allows to use embedded images. You can specify an HTML format of the message in the HTML field.
- **Body**: (for plain text format), the text in the email that is sent to the user. The following variables can be used:
  - {user} - the username of the user.
  - {endpoint} - the device the user is authenticating to.
  - {event} - the name of the event where the user is trying to authenticate to.
  - {otp} - this is the actual One-Time-Password.

8.3.4 Emergency Password

The settings allows to configure the Emergency Password authentication method. The method can be used as temporarily solution for the users who forgot smartphone or lost a card. Enrollment of the method is allowed only by security officers. Users are not permitted to enroll it.

WARNING: Enabling this method's use could be abused by an administrator who wants to take over another user's account.

It is possible to manage the following security options:

1. **Minimum password length**. 5 characters by default. Usage of shorter passwords is not allowed.
2. **Password age (days)**. 3 days by default. It means the password will expire in 3 days.
3. **Max logons**. 10 logons by default. The password becomes expired after 10 logons.
4. **Complexity requirements**. The option is disabled by default. If it's enabled the password must complain at least 3 of 4 checks:
   - it should contain at least one uppercase character,
   - it should contain at least one lowercase character,
   - it should contain at least one digit,
   - it should contain at least one special symbol.
5. **Allow change options during enroll**. If the option is enabled a security officer will be able to set **Start date**, **End date** and **Maximum logons** manually. The manual configuration overrides the settings in Emergency Password method.

8.3.5 Fingerprint

The fingerprint authentication method uses a fingerprint scanner to authenticate.

To configure the fingerprint authentication, perform the following steps:

1 Set the **Similarity score threshold** by moving the slider to the desired score.

NOTE: Default and recommended value for Similarity score threshold is 25. Reducing the score may result in different fingerprints getting validated.

---

2 Select the number of fingers to be enrolled.

NOTE: It is recommended to enroll more than one finger as injuries or minor cuts to enrolled finger may make it unusable.

---

3 Select the number of captures for the enrolled fingers.

NOTE: To improve the quality of the fingerprint enrollment, it is recommended to have multiple captures. The total number of captures including all the enrolled fingers cannot exceed 25.

---

4 Click **Save.**

8.3.6 FIDO U2F

You can configure certificate settings for the FIDO U2F authentication method. By default, Advanced Authentication does not require the attestation certificate for authentication by FIDO U2F compliant token. Ensure that you have a valid attestation certificate added for your FIDO U2F compliant tokens, when you configure this method. A Yubico attestation certificate is pre-configured in the Advanced Authentication appliance. Click **Add** to add a device manufacturer certificate that must be in a `PEM` format. To enable check of attestation certificate, switch the **Require attestation certificate** option to **ON**. You can also turn the **Disable built-in certificate** option to **ON** if you do not want to use the built-in Yubico attestation certificate.

IMPORTANT: To use the FIDO U2F authentication in Advanced Authentication Access Manager and for the OAuth2 event it's required to configure an external web service to perform enrollment and authentication for one domain name. Configuring a Web Server in order to use the FIDO U2F authentication

The YubiKey tokens may start to flash with delay when token is initialized in combo-mode (e.g. OTP+U2F). It may decrease user performance, as users have to wait when the token start to flash before enrollment or authentication. Therefore it's recommended to flash the tokens in U2F only mode if the rest modes are not needed.

Configuring a Web Server in order to use the FIDO U2F authentication

---

NOTE: This article is applicable for Debian 8 Jessie. The procedure may differ for other distributives.

These instructions will help you to configure web server in order to use FIDO U2F authentication in NetIQ Access Manager and for OAuth 2.0 event. According to FIDO U2F specification, enrollment and authentication must be performed for one domain name. NetIQ Access Manager and Advanced Authentication appliance are located on different servers, as a result it is required to configure web server which will perform port forwarding to:

- Advanced Authentication appliance for the FIDO U2F enrollment
- NetIQ Access Manager for further authentication using FIDO U2F tokens

Installing Nginx Web Server

To install Nginx web server to use it for URL forwarding, add these two lines to the `/etc/apt/sources.list` file:

```
deb http://packages.dotdeb.org jessie all
deb-src http://packages.dotdeb.org jessie all
```

Preparing SSL Certificate

To prepare SSL certificate, please run these commands:

```
mkdir –p /etc/nginx/ssl
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/
proxy.key -out /etc/nginx/ssl/proxy.crt
```

Nginx Proxy Configuration

To prepare Nginx proxy configuration, add the following to the `/etc/nginx/sites-available/proxy` file:

```
server {
listen 443 ssl;
error_log /var/log/nginx/proxy.error.log info;
server_name nam.company.local;
ssl_certificate /etc/nginx/ssl/proxy.crt;
ssl_certificate_key /etc/nginx/ssl/proxy.key;
location ~ ^/account {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_pass https://<appliance_IP>$uri?$args;
}
location ~ ^/static {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_pass https://<appliance_IP>$uri?$args;
}
location ~ ^/admin {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_pass https://<appliance_IP>$uri?$args;
}
location / {

proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
proxy_read_timeout 300;
proxy_pass https://<NAM_IP>;
}
}
```

Create link and restart nginx service using the following commands:

```
ln -s /etc/nginx/sites-available/proxy /etc/nginx/sites-enabled/proxy
service nginx reload
```

DNS Entries

Please make sure that NAM name server corresponds to IP address of web server.

Enrollment

To enroll U2F, please open link https://<NAM_FQDN>/account. You will be forwarded to the enroll page of Advanced Authentication server appliance.

8.3.7 LDAP Password

The settings allows to configure security options for LDAP passwords (passwords stored in the used repository).

LDAP Password is required for Advanced Authentication Clients, because the Advanced Authentication Clients retrieve password from the Advanced Authentication Server to validate it. If you do not have a LDAP Password method in a used chain, a prompt is displayed to perform the synchronization. A prompt is displayed only for the first time if **Save LDAP password** option is set to **ON** until the password is changed or reset. A prompt for synchronization is displayed each time if the **Save LDAP password** option is set to **OFF.**

8.3.8 OATH OTP

OATH stands for Initiative for Open Authentication and is an industry-wide collaboration to develop an open reference architecture using open standards to promote the adoption of strong authentication using One-Time-Passwords.

Advanced Authentication Framework supports two different types of OATH OTP and these are:

- HOTP: counter based OTP
- TOTP: time based OTP

To access the settings open Advanced Authentication, **Methods** section, click **Edit** button next to OATH OTP.

For the HOTP variant you can specify the following parameters:

1. **OTP format**, it determines how many digits the OTP token has. By default it's 6 digits. It can be changed to 4,6,7 or 8 digits. The value should be the same as the tokens you are using.
2. **OTP window** allows to specify a value, how much OTPs the Advanced Authentication Server will generate starting from the current HOTP counter value to match an HOTP entered by user during authentication. The default value is 10.This is required for the case when users use the tokens not only for authentication using Advanced Authentication, in each case of usage the HOTP counter increases on 1, so the counter will be out of sync between the token and Advanced Authentication Server. Also users can press the token button accidentally. The maximum value for the OTP window is 100000 seconds.

   WARNING: Increasing of HOTP window value to more than 100 is not recommended, because it may decrease security by causing false matches.

During enrollment or HOTP counters synchronization in Self-Service Portal the **Enrollment HOTP window** equal to 100 000 is used. This is necessary because the HOTP tokens may be used during a long period before enrollment in Advanced Authentication and its value is unknown and could be even equal to some thousands. This is secure as users need to provide 3 consequent HOTPs.

The TOTP settings contain the following parameters:

1. **OTP period (sec)** allows to specify how often a new OTP is generated. A default value is 30 seconds. The maximum value for the OTP period is 360 seconds.
2. **OTP format** determines how many digits the OTP token has. By default it's 6 digits. It can be changed to 4,6,7 or 8 digits. The value should be the same as the tokens you are using.
3. **OTP window**, it allows to determine how many period may be used by Advanced Authentication Server for TOTP generation. E.g. we have a period of 30 and a window of 4, then the token is valid for 4*30 seconds before current time and 4*30 seconds after current time, which is 4

minutes. These configurations are used because time can be out-of-sync between the token and the server and that will otherwise impact the authentication.The maximum value for the OTP window is 64 periods.

IMPORTANT: You cannot use OTP window =32 and higher for four digit OTPs as it can lead to false matches and reduce security.

---

4. **Google Authenticator format of QR code (Key Uri)**. By default the Advanced Authentication Auth smartphone app can be used to scan a QR code for enrollment of software token. The format of QR code is not supported by other apps. It's possible to switch Advanced Authentication to use the Google Authenticator or Microsoft Authenticator app instead of Advanced Authentication Authsmartphone app using the option.

IMPORTANT: OTP format must be set to 6 digits when you use the Google Authenticator or Microsoft Authenticator format of QR code.

Advanced Authentication Framework also supports the import of PSKC or CSV files. These are token files with token information in them. To do this follow the instruction below:

1. Go to the **OATH Token** tab.
2. Click **Add** button.
3. Click **Choose File** and add a PSKC or CSV file.
4. Choose a proper **File type**. It can be
   - **OATH compliant PSKC** (e.g. for HID OATH TOTP compliant tokens).
   - **OATH csv**, the CSV must complain the format described Format of CSV file which is supported for import of OATH compliant tokens. It's not possible to use the YubiKey CSV files.
   - **Yubico csv**, it is required to use one of the supported **Log configuration output** (check `YubiKey Personalization Tool - Settings tab - Logging Settings`) formats with comma as a delimiter:
     - Traditional format. **OATH Token Identifier** option should be enabled.
     - Yubico format. It is supported only for **HOTP Length** set to **6 Digits** and **OATH Token Identifier** set to **All numeric**.

     IMPORTANT: **Moving Factor Seed** should not be more than 100000.

     ---
5. It's possible to add the encrypted PSKC files. For the case switch **PSKC file encryption type** from Not Encrypted to **Password** or **Pre-shared key** and provide the information.
6. Click **Upload** to import tokens from the file.

NOTE: Advanced Authentication gets an **OTP format** from the imported tokens file and stores the information in the enrolled authenticator. So it's not required to change the default common value of OTP format on the **Method Settings Edit** tab.

When the tokens are already imported you see the list and it's required to assign the tokens to users. If can be done in two ways:

1. Click **Edit** button next to token and select **Owner**. Click **Save** button to apply the changes.
2. A user can self-enroll a token in the Advanced Authentication Self-Service Portal. Administrator should let the user know an appropriate value from **Serial** column to do it.

Format of CSV file which is supported for import of OATH compliant tokens

A CSV file which is importing as `OATH csv` file type in (Advanced Authentication Administrative Portal - **Methods** - **OATH OTP** - **OATH Tokens** tab) should fields with the following parameters:

- token's serial number,
- token's seed
- a type of the token: TOTP or HOTP (optional, by default HOTP)
- OTP length (optional, by default 6 digits)
- time step (optional, by default 30 seconds)

Comma is a delimiter.

Example of CSV:

```
Token001, 15d2fa517d3c6b791bd4cc2044c241429307001f
Token002, 8c557fc050721037fd31e1d3345b5d3263263e0f, totp, 8
Token003, 658208efea5ac49d5331ba781e66f2c808cccc8e, hotp, 6
Token004, 89f0dfe1c90379da6a11aaca2fc1070f606efe36, totp, 6, 60
```

IMPORTANT: For the YubiKey tokens it's required to use Traditional format of the CSV (check `YubiKey Personalization Tool - Settings tab - Logging Settings`) with comma as a delimiter. Use Yubico csv file type (**Advanced Authentication Administrative Portal - Methods - OATH OTP - OATH Tokens** tab).

8.3.9 Password

The settings allows to configure security options for passwords stored in the appliance. They are applied, for example, for the appliance administrator and other local accounts.

NOTE: It's not recommended to use the Password method in chains which contain one factor. It's secure to combine it with other factors.

It's possible to manage the following settings:

---

1. **Minimum password length**.
2. **Maximum password age**. 42 days by default. It means the password will expire in 42 days. If it's set to 0 the password will not expire.
3. **Complexity requirements**. The option is disabled by default. If it's enabled the password must complain at least 3 of 4 checks:
   - it should contain at least one uppercase character,
   - it should contain at least one lowercase character,
   - it should contain at least one digit,
   - it should contain at least one special symbol.
4. If you need to rename the **Password** method to **PIN**, enable **Rename to PIN** to **ON**. The **Password** method is renamed to **PIN** in the Advanced Authentication Administrative Portal, Helpdesk Portal, Self Service Portal and Windows Client, Mac OS X Client, and the Linux PAM Client.

IMPORTANT: Notifications about expiring passwords are not yet supported. So the local administrator will not be able to sign-in to the Advanced Authentication Administrative Portal and users who use the method will not be able to authenticate after the password expiration. To fix it the administrator/user should go to the Self-Service Portal and change his/her password.

8.3.10 PKI

The section allows you to upload the trusted root certificates. The following requirements for the certificates must be met:

1. **Root CA** certificate must be in the `.pem` format.
2. All certificates in the certification path (except Root CA) must contain **AIA** and **CDP** http link to check revocation status.
3. The certificate for PKI device must contain a key pair: public and private key in the x509 format. The certificates that do not comply with the requirements are ignored (hidden during enrollment).

NOTE: Advanced Authentication supports `p7b` format of parent certificates. They can contain only Certificates and Chain certificates but not the Private key. They are Base64 encoded ASCII files having extensions `.p7b` or `.p7c`

Configuring the Environment for a Standalone Root CA

1. Install **Web Server (IIS) Role**.
2. Create the `CertEnroll` Folder and grant **Share & NTFS** permissions to the **Cert Publishers** group.
3. Create **CertEnroll Virtual Directory** in IIS.
4. Enable **Double Escaping** on IIS Server.
5. Install **Enterprise Root CA** using Server Manager.
6. Enable **Object Access Auditing** on CA.
7. Configure the **AIA** and **CDP**.
8. Publish the Root CA Certificate to AIA.
9. Export **Root CA** in `.der` format and convert the format to `.pem`.
10. Export personal certificate (that was signed by Root CA) with private key and place it on a PKI device.

Configuring the Environment for a Subordinate CA

1. Install **Web Server (IIS) Role**.
2. Create the `CertEnroll Folder` and grant **Share & NTFS** permissions to **Cert Publishers** group.
3. Create **CertEnroll Virtual** Directory in IIS.
4. Enable **Double Escaping** on IIS Server.
5. Install the **Standalone Offline Root CA**.
6. Create a `CAPolicy.inf` for the standalone offline root CA.
7. Installing the **Standalone Offline Root CA**.
8. Enable **Auditing** on the Root CA.
9. Configure the **AIA** and **CDP**.

10. Install Enterprise Issuing CA.
11. Create `CAPolicy.inf` for Enterprise Root CA.
12. Publish the **Root CA Certificate** and **CRL**.
13. Install **Subordinate Issuing CA**.
14. Submit the Request and Issue subordinate **Issuing CA Certificate**.
15. Install the subordinate **Issuing CA Certificate**.
16. Configure **Certificate Revocation** and **CA Certificate Validity Periods.**
17. Enable **Auditing** on the Issuing CA.
18. Configure the **AIA** and **CDP**.
19. Install and configure the **Online Responder Role Service**.
20. Add the **OCSP URL** to the subordinate Issuing CA.
21. Configure and publish the **OCSP Response Signing Certificate** on the subordinate Issuing CA.
22. Configure **Revocation Configuration** on the **Online Responder**.
23. Configure **Group Policy** to provide the OCSP URL for the subordinate Issuing CA.
24. Export **Root CA** in `.der` format and convert the format to `.pem`.
25. Export personal certificate (that was signed by subordinate CA) with private key and place it on a PKI device.

For more information see the articles on Single Tier PKI Hierarchy Deployment and Two Tier PKI Hierarchy Deployment.

To upload a new trusted root certificate:

1. In the **PKI Method Settings Edit** page, click **Add**.
2. Click **Browse**.
3. Choose a `.pem` certificate file and click **Upload**. A message is displayed that the trusted root certificate has been added.
4. Click **Save**.

NOTE: Only **Root CA** must be uploaded on appliance.

8.3.11 Radius Client

With the Radius Client Authentication Method the authentication framework will forward the authentication request to a third party RADIUS server. This can be any RADIUS server. A specific example of when to use this Authentication Method is if you have a working token solution like RSA, or Vasco and want to migrate your users to the Advanced Authentication framework. Some users will be able to still use the old tokens and new users can use any of the other supported Authentication Methods.

To use this method you will need to create an RADIUS Client on the third party RADIUS server with the hostname of IP address of this appliance. If you have multiple appliances you should add them all as RADIUS Clients.

The following configuration options are available:

- **Server**: the hostname or IP address of the third party RADIUS server.
- **Secret**: shared secret between the RADIUS server and the Authentication Framework.

- **Port**: port to where the RADIUS authentication request is sent. The default is 1812.
- **Send repo name**. If it's enabled, a repository name will be automatically used with a username. For example, company\pjones
- **NAS Identifier**, the attribute is optional.

8.3.12 SMS OTP

The SMS OTP authentication method will send an SMS text to the user's mobile phone with a One-Time-Password (OTP). The user will receive this OTP and needs to enter it on the device where the authentication is happening. This authentication method is best used with a second method like Password or LDAP Password in order to achieve multi-factor authentication and to prohibit malicious users from sending SPAM a user's phone with authentication requests.

NOTE: In the user's settings, if the phone number is specified with extension, then SMS will not be delivered. Ensure that a phone number without extension is provided.

The following configuration options are available:

- **OTP Period**: the lifetime of an OTP token in seconds. By default 120 seconds.The maximum value for the OTP period is 360 seconds.
- **OTP Format**: the length of an OTP token. By default 6 digits.
- **Body**: the text in the SMS that is sent to the user. The following variables can be used:
  - {user} - the username of the user
  - {endpoint} - the device the user is authenticating to
  - {event} - the name of the event where the user is trying to authenticate to
  - {otp} - this is the actual One-Time-Password.
- **User cell phone attribute**: the cell phone number of a user that is used to send the OTP through an SMS. You can use custom attributes such as `mobile`, `homePhone`, `ipPhone`, and other attributes of a repository. You must also define the attribute in the "User cell phone attributes" section of Repository configuration.

  NOTE: If you do not configure the attribute in the method settings, then the first attribute defined in the "User cell phone attributes" section of Repository configuration is used when the user tries to authenticate. For example, if you define `mobile` as the first attribute in **User cell phone attribute** and do not configure the attribute in method settings of **SMS OTP**, then while authenticating, the first attribute, which is the `mobile` attribute, is used for the **SMS OTP** method authentication.

8.3.13 Security Questions

This Authentication Method is mostly used in fall-back scenarios where a user does not have access to his normal strong authentication method. The authentication method works in such a way that a user needs to answer a series of questions that are pre-defined in this configuration section. When the user tries to authenticate using the Security Questions he or she will be provided with a random set out of these pre-defined questions. By answering the questions correctly the user will get access. Below you can configure how many of the answers should be correct before the user gains access.

IMPORTANT: This authentication method is not seen as secure and if possible should not be used.

When you decide to use this Authentication Method please follow some guidelines.

It is essential that we use good questions. Good security questions meet five criteria. The answers to a good security question are:

1. **Safe**: cannot be guessed or researched.
2. **Stable**: does not change over time.
3. **Memorable**: can be remembered.
4. **Simple**: is precise, easy, consistent.
5. **Many**: has many possible answers.

Some examples of good, fair, and poor security questions according to goodsecurityquestions.com are given below. For a full list please visit this website.

GOOD

What is the first name of the person you first kissed?

What is the last name of the teacher who gave you your first failing grade?

What is the name of the place your wedding reception was held?

In what city or town did you meet your spouse/partner?

What was the make and model of your first car?

FAIR

What was the name of your elementary / primary school?

In what city or town does your nearest sibling live?

What was the name of your first stuffed animal, doll, or action figure?

What time of the day were you born? (hh:mm)

What was your favorite place to visit as a child?

POOR

What is your pet's name?

In what year was your father born?

In what county where you born?

What is the color of your eyes?

What is your favorite _____?

The following configuration options are available:

- Min. answer length: the minimum number of characters an answer should consist of.
- Correct questions for logon: the number of questions a user should answer correctly to get access.
- Total questions for logon: the number of questions the user needs to answer.

So when Correct questions for logon is set to 3 and the Total questions for logon is set to 5 then the user only needs to enter 3 correct questions out of a set of 5.

8.3.14 Smartphone

The Smartphone authentication method uses an app on your smartphone to do out-of-band authentication. This means that the authentication is happening over a different channel than the initiating authentication request.

For example, if you are logging into a website, then the Smartphone authentication method will send a push message to your mobile phone. When opening the Advanced Authentication app the user will be presented with an Accept and a Reject button where he can decide what to do. If the user pushes the Accept button the authentication request will be sent over the mobile network (secure) back to the Authentication framework. Without typing over an OTP code the user will be granted access.

When the smartphone doesn't have a data connection, a backup OTP authentication can be used.

This Authentication Method is best used in combination with another method like Password or LDAP Password in order to achieve multi factor authentication and protect the user from getting SPAM push messages.

The following configuration options are available:

- **Push salt TTL**: the lifetime of an authentication request sent to the smartphone.
- **Learn timeout**: the time the QR code used for enrolment is valid for the user to scan.
- **Auth salt TTL**: the lifetime in which the out-of-band authentication needs to be accepted before authentication fails.
- **TOTP Length**: the length of the OTP token used for backup authentication
- **TOTP step** : the time a TOTP is shown on screen before the next OTP is generated. Default 30
- **TOTP time window**: the time in seconds in which the TOTP entered is accepted. Default 300
- **Server URL**: URL of Advanced Authentication server to where the smartphone app connects for authentication. For example, `http://<AAServerAddress>/smartphone` (/smartphone cannot be changed). Use http only for testing and https in a production environment. You will need a valid certificate while using https.

You can configure Geo-fencing with the Smartphone method. Geo-fencing allows you to authenticate with the Smartphone method with one more factor, which is the geographical location. When you enable geo-fencing, users will be able to authenticate with Smartphone from only allowed geographical locations. You must enable the policy Geo fencing options to use geo fencing.

To configure geo-fencing, you need to draw a boundary of the location to be authenticated with a polygon. To configure geo-fencing, perform the following steps:

1. Click the **Geo Zones** tab.
2. Click **Add**.
3. Specify the name of the zone.
4. Click the Search icon and specify the address to locate the required geographical location.

   You can click the full screen icon to view the map in the full screen.
5. Click the polygon icon in the menu bar of the map.
6. Click the starting point on the map and draw the boundary of the specific location to be authenticated.
7. Click to mark the end point of the boundary after you have finished drawing the geo zone.

You can also edit the marked polygon by clicking the edit icon.

8 Click **Save**.

NOTE: If you use the geo-fencing feature, then ensure that access to the location is enabled for the NetIQ Advanced Authentication app on the smartphone.

Authentication flow

The following chart demonstrates the authentication flow:

A user is authenticating on endpoint (which can be the user's laptop with Advanced Authentication Windows Client installed or a website etc.) by Smartphone method.

1. The endpoint calls the Advanced Authentication Server.
2. It validates the provided user's credentials.
3. Advanced Authentication Server sends a push message to proxy.authasas.com.
4. It defines an appropriate push service for the using smartphone platform and forwards the push message to it.
5. The push message will be delivered to the user's smartphone. This is not required for a successful authentication and is only to inform the user.

6. When the user opens the app, the app checks at the Advanced Authentication Server if there is an authentication needed. If this is the case it will show the Accept and Reject buttons. This answer is send to the server.
7. Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTPS protocol is used for the communication.

Access configuration

- Advanced Authentication Server must be accessible by the specified **Server URL** address from smartphones (HTTPS, outbound).
- Advanced Authentication Server must have a permitted outbound connection to proxy.authasas.com (HTTPS).

8.3.15 Swisscom Mobile ID

The settings allow you to configure the Swisscom Mobile ID authentication method. This method provides strong authentication based cryptographic materials that are stored and protected in the SIM card of a user's mobile phone.

You can configure the following settings for this method:

1. **Application provider ID**: Identifier of the application provider.
2. **Application provider password**: Password of the application provider.
3. **Swisscom Mobile ID service URL**: Interface of the Swisscom Mobile ID.
4. **Notification message prefix**: Message that will be displayed on the user's mobile as a notification.

The section also allows you to upload the Swisscom client certificates:

1. Choose a **Client SSL certificate**. The required certificate must be in a `.pem` format and should be self-signed certificate with a private key.
2. Specify the **Private key password** for the certificate.
3. Click **Save**.

NOTE: Users must activate the Mobile ID service for the Swisscom SIM card.

For more information on Swisscom Mobile ID, refer to the Mobile ID Reference guide.

8.3.16 Voice

The section contain security settings for Voice authentication method. Advanced Authentication will call user and the user will need to enter a pin code, which should be predefined in Advanced Authentication Self-Service Portal during the authenticator enrollment.

NOTE: Phone number with extensions are also supported for voice method.

Special characters "," and "x" are used to indicate wait time and can be used as separators between phone number and extension.

For example, if +123456789 is the phone number and 123 is the extension, then it can be specified as +123456789,,,,123.

In the above example, “,” is specified 4 times and this multiplied by 0.5 (default value in Twilio) indicates the wait time, which is 2 (4*0.5) seconds. So at first, call is given to the number 123456789 and after a wait period of 2 seconds, the extension 123 is dialled.

It's possible to manage the following settings:

1. **Minimum pin length**. 3 digits by default. Usage of shorter pins is not allowed.
2. **Maximum pin age**. 42 days by default. It means that the pin will expire in 42 days and will need to be changed in the Advanced Authentication Self-Service Portal. If it's set to 0 the pin will not expire.
3. **User cell phone attribute**: the cell phone number of a user that is used to call the user for voice authentication. You can use custom attributes such as `mobile`, `homePhone`, `ipPhone` and other attributes of a repository. You must also define the attribute in the “User cell phone attributes” section of Repository configuration.

   NOTE: If you do not configure the attribute in the method settings, then the first attribute defined in the “User cell phone attributes” section of Repository configuration is used when the user tries to authenticate. For example, if you define `mobile` as the first attribute in **User cell phone attribute** and do not configure the attribute in method settings of **Voice**, then while authenticating, the first attribute, which is the `mobile` attribute, is used for the **Voice** method authentication.

IMPORTANT: Notifications about expiring pins are not supported.

8.3.17 Voice OTP

The settings allow you to configure the Voice OTP authentication method. The user will receive this OTP in a call and the OTP has to be entered on the device where the authentication is happening. This authentication method is best used with a second method like Password or LDAP Password in order to achieve multi-factor authentication.

You can configure the following settings for this method:

1. **OTP period**: The time period for which the Voice OTP is valid. Default time is 120 seconds. The maximum value for the Voice OTP period is 360 seconds
2. **OTP format**: The length of the Voice OTP token. Default length is 4 digits.
3. **Body**: The text/number in the Voice OTP that is sent to the user. Here, you can enter the `{otp}` variable, which is the actual One-Time-Password. To repeat the One-Time Password during the call you may enter: `Use the OTP for authentication: {otp}. OTP: {otp}`.
4. **User cell phone attribute**: the cell phone number of a user that is used to send the OTP through call. You can use custom attributes such as `mobile`, `homePhone`, `ipPhone` and other attributes of a repository. You must also define the attribute in the “User cell phone attributes” section of Repository configuration.

   NOTE: If you do not configure the attribute in the method settings, then the first attribute defined in the “User cell phone attributes” section of Repository configuration is used when the user tries to authenticate. For example, if you define `mobile` as the first attribute in **User cell phone**

attribute and do not configure the attribute in method settings of **Voice OTP**, then while authenticating, the first attribute, which is the `mobile` attribute, is used for the **Voice OTP** method authentication.

8.4 Creating a Chain

Authentication chains are combinations of authentication methods. Users will need to pass all methods in order to be successfully authenticated.

So when you create a chain that has LDAP Password and SMS in it then the user will first need to enter their LDAP Password. When this is correct the system will send an SMS with a One-Time-Password to the mobile phone of the user and the user will need to enter the correct OTP in order to be authenticated.

The following chains are created by default:

1. **LDAP Password Only**: The chain can be used by any user from the repository. It allows to authenticate by the LDAP Password (single-factor) method.
2. **Password Only**: The chain can be used by any user who has a Password authenticator enrolled. It allows to authenticate by the Password (single-factor) method.

It is possible to create any chain you want. For highly secure environments you can assign multiple methods to one chain to achieve better security.

Authentication can consist of 3 different factors. These are:

1. **Something you know**: password, PIN, security questions
2. **Something you have**: smartcard, token, telephone
3. **Something you are**: biometrics like fingerprint or iris

Something is seen as Multi-Factor or Strong Authentication when 2 out of the 3 factors are used. So a password with a token, or a smartcard with a fingerprint are seen as multi-factor. A password and a PIN is not seen as multi-factor as they are in the same area.

Authentication chains are linked to user groups in your repositories. You can allow only a certain group to be able to use the specific authentication chain.

To create a new chain or edit an existing one that Advanced Authentication framework will work with, follow the steps:

1. Open the **Chains** section.
2. Click the **Add** button at the bottom of the **Chains** view to create a new authentication chain (or click the **Edit** button next to an applicable authentication chain).
3. Specify a name of the Chain in the **Name** text field.
4. Specify a **Short name**. The short name used by a user to switch to this chain. For example, if you call LDAP Password & SMS chain "sms" then a user can type in "<username> sms" and he will be forced to use SMS as the chain. This can be helpful in cases when the primary chain is not available.
5. Select whether the current authentication chain is available for use or not available by clicking the **Is enabled** toggle button.
6. The **Methods** section allows to setup a prioritized list of authentication methods. For example, an LDAP Password+ HOTP method first asks the user for the LDAP password and after that for his OTP code. HOTP + LDAP Password first asks for the OTP code and then for the LDAP password.

7. Specify groups that will be allowed to use the current authentication chain in the **Roles & Groups** text field.

IMPORTANT: It's not recommended to use the groups from which you will not be able to exclude users (like `All Users` group in Active Directory), because you will not be able to free up a user's license.

---

8. Expand the **Advanced settings** section. Select **Apply if used by endpoint owner,** if the chain must be used only by an Endpoint owner.

NOTE: The Endpoint Owner feature is supported for Windows Client, Mac OS Client and Linux PAM Client only.

---

9. Set **Required chain** to **Nothing**, if this is a normal (high-security) chain. If you want to configure a simple chain within a specific time period after successful authentication with a high-security chain, choose an appropriate high-security chain. In this case you also need to specify a **Grace period (mins).** Within this time period the chain will be used instead of the appropriate high-security chain. The maximum value for grace period is 44640 min (31 days).

NOTE: You must assign both high-security chain and simple chain to an Event. The simple chain must be higher than the corresponding high-security chain.

The options are available when the **Enable tracking** option is set to **ON**.

For example, `LDAP Password+Card` is a high-security chain and Card is a simple chain. The users must use `LDAP Password+Card` chain once in every 8 hours and within this period, they must provide only the `Card` method to authenticate.

10. Click **Save**.

IMPORTANT: If you have configured more than one chain using one method (e.g. "LDAP Password", "LDAP Password+Smartphone") and assigned it to the same group of users and the same Event, the top chain will be always used if the user has all methods in the chain enrolled.

An exception is usage of a high-security chain and its appropriate simple chain, where the simple chain must be higher than its high-security chain.

8.5 Configuring Events

Here you can configure the supported applications / events to where the Advanced Authentication server will authenticate.

To configure an authentication event for Advanced Authentication, follow the steps:

1. Open the **Events** section.
2. Click the **Edit** button next to an applicable event.
3. Select whether the current event is enabled or disabled by clicking the **Is enabled** toggle button.
4. Select the event type.
5. Select the authenticator category, if applicable.
6. Select chains that will be assigned to the current event.
7. If you want to restrict access of some Endpoints to the Event, add all the Endpoints that must have access to the Endpoint whitelists. The remaining Endpoints are blacklisted automatically. If you leave the Endpoints whitelist blank, all the endpoints are permitted.

8. Select the Geo-fencing option if you want to enable geo-fencing. Add the permitted zones to the **Used** list. To know more on configuring geo-fencing, see the Smartphone method.

   NOTE: You must enable the policy Geo fencing options to use the geo fencing functionality

9. Select **Allow Kerberos SSO,** if you want to enable single sign-on to the Advanced Authentication Portals. Kerberos SSO is supported for AdminUI, Authenticators Management, Helpdesk and Report logon events

   NOTE: To use Kerberos SSO feature, you must configure Kerberos SSO Options policy and upload a keytab file.

10. Click **Save** at the bottom of the **Events** view to save configuration.

If you need to revert the changes to defaults use the **Initialize default chains** button.

NOTE: If you have specified more than one chain with one method (For example "LDAP Password", "LDAP Password+Smartphone") and assigned it to the same group of users and the same Event, the top chain is always used if the user has all the methods in the chain enrolled. An exception is usage of a high-security chain and its appropriate simple chain, where the simple chain must be higher than its high-security chain.

TIP: It's recommended to have a single chain with Emergency Password method at a top of the Used chains list in Authenticators Management event and other events which are used by users. The chain will be ignored while user doesn't have the Emergency Password enrolled. The user will be able to use the Emergency Password immediately when security officer enrolled the user the Emergency Password authenticator.

To create a custom event for a third-party application, click **Add** below the available Events list. Then, perform the following steps:

1. Specify a name for the event.
2. Enable the event by changing **Is enabled** to **ON**.
3. Select one of the following events.
   - Select **OS Logon (domain)** if the third-party application needs to read password of a user after authentication. For example, it is required when Windows Client, Mac OS X Client or Linux PAM Client workstation is joined/bound to a domain.
   - Select **OAuth2** if you need to create an OAuth 2.0 event.
   - Select **SAML2** if you need to create an SAML 2.0 event.
   - Select **Generic** otherwise (including a case if Windows Client, Mac OS X Client or Linux PAM Client workstation is not joined/bound to a domain).
4. Select the Authenticator category.
5. Select the chains that will be assigned to the event.
6. Select the required endpoints from Endpoint whitelist (if applicable). Access to the event from other endpoints will be restricted.
7. Enable/Disable the geo-fencing.

   NOTE: You must enable the policy Geo fencing options to use the geo fencing functionality.

Geo-fencing requires a smart phone. If you use the geo-fencing feature, then ensure that access to the location is enabled for the NetIQ Advanced Authentication app on the smartphone. For more information on enabling geo-fencing on smartphone see Smartphone.

8. Specify the redirect URLs, if you have selected **OAuth2** event. OAuth 2 settings are available only for OAuth2 events.

   IMPORTANT: **WebAuth** feature must be enabled in Server Options before configuring **OAuth2** event.

   NOTE: The client ID and client secret is generate automatically. Client ID, client secret and redirect URL will be consumed by consumer web application. After successful authentication, the redirect URL web page specified in the event is displayed.

9. Enable/disable the **Use for Owner Password Credentials** option. Advanced settings are available only for OAuth2 events.
   - Set the **Use for Owner Password Credentials** option to **ON,** if the consumer web application provides authorization in the form of Resource Owner Password Credentials Grant.
   - Set the **Use for Owner Password Credentials** option to **OFF,** if the consumer web application provides authorization in the form of Authorization Code Grant or Implicit Grant.

   NOTE: If you enable **Use for Owner Password Credentials** option, then you can use only **LDAP Password only** chain for this event. Also, it is recommended to have separate events for Resource Owner Password Credentials Grant (**Use for Owner Password Credentials** option set to **ON)** and Authorization Code Grant / Implicit Grant (**Use for Owner Password Credentials** option set to **OFF**).

10. If you have selected **SAML2** event, then in the **SAML 2.0 settings** section, either insert your Service Provider's SAML 2.0 metadata to the **SP SAML 2.0 metadata** field OR click **Choose File** and select a Service Provider's SAML 2.0 metadata XML file to upload it.

    NOTE: For the SAML2 event to function properly, the SAML 2.0 options policy has to be configured.

11. Click **Save.**

If you have created a custom OAuth 2 event, then perform the following steps to access consumer web application:

1. Specify the client ID, client secret and redirect URLs in the consumer web application.
2. Specify the Appliance end point (Authorization end point) in the web application. For example, `https://<Appliance IP>/osp/a/TOP/auth/oauth2/grant`

   NOTE: Authorization is provided in the form of Authorization Code Grant or Implicit Grant or Resource Owner Password Credentials Grant.

3. Authenticate with the required authentication method(s) to access the consumer web application.

For more information on OAuth 2.0 event, see "OAuth 2.0 Roles" on page 69, "OAuth 2.0 Modes" on page 70, "OAuth 2.0 Sample Web Application" on page 71, and "Exploring Sample Web Application" on page 77.

The following predefined events are available.

- Section 8.5.1, “ADFS,” on page 66
- Section 8.5.2, “AdminUI,” on page 66
- Section 8.5.3, “Authenticators Management,” on page 66
- Section 8.5.4, “Helpdesk,” on page 67
- Section 8.5.5, “Helpdesk User,” on page 67
- Section 8.5.6, “Linux Logon,” on page 67
- Section 8.5.7, “Mac OS logon,” on page 67
- Section 8.5.8, “NAM,” on page 67
- Section 8.5.9, “NCA,” on page 67
- Section 8.5.10, “Report logon,” on page 68
- Section 8.5.11, “Windows logon,” on page 68
- Section 8.5.12, “Radius Server,” on page 68

8.5.1 ADFS

This event is used to configure integration with ADFS.

For more information, see “Configuring Advanced Authentication Server” in the *ADFS Plug-in Installation guide.*

8.5.2 AdminUI

This event is used for accessing this Administrative Portal. You can configure which chains can be used to get access to /admin.

NOTE: You can add authorized users or group of users from a configured repository to the FULL ADMINS role (in Repositories - Local). After this, you must assign the chains in which the methods are enrolled for users with the AdminUI event (at a minimum with an LDAP Password).

8.5.3 Authenticators Management

This event configures the chains that can be used to access the Self-Service Portal. Users can enroll any of the methods that are configured for any chain they are a member of the group assigned to the chain.

You may post a LDAP Password chain to the bottom of the used chains list to secure access to the portal for users who already has enrolled methods.

IMPORTANT: If there are no users in a configured repository which has access to the Administrative Portal, a chain with **Password** only (Authenticators Management - Password) must be enabled for the Authenticators Management event. This helps in accessing the Self-Service Portal when a used password expires and has to be changed.

You can also perform basic authentication with Advanced Authentication.

To achieve basic authentication, in the **Event Edit** screen for Authenticators Management, set the **Allow basic authentication** option to **ON**.

NOTE: The basic authentication is supported only for the **Authentication Management** event and for the Password (PIN), LDAP Password, and HOTP methods.

You must enter `/basic` with the URL to login to the enrollment page. The Login page appears and the format of the Username you must provide is: `username:PASSWORD|LDAP_PASSWORD|HOTP:1.` For example: `admin:PASSWORD:1`.

When you login to the Self Service portal, by default, the chain with the highest priority is displayed. To display the other chains with the enrolled methods, you can turn the **Show chain selection** option to **ON**. This helps you to view the list of available chains and then select one of them.

NOTE: The chains are displayed with the enrolled methods only.

8.5.4 Helpdesk

This event is used for accessing the Helpdesk Portal by Helpdesk/Security officers.

8.5.5 Helpdesk User

This event is used to authenticate users in the Helpdesk portal when the Helpdesk administrator is already authenticated. The event is used when the **Ask credentials of management user** option in the Helpdesk Options policy is enabled.

8.5.6 Linux Logon

This event configures the chains that can be used to log on to Linux. If you want to use Linux Client on non-domain joined workstations, change the **Event type** from **OS Logon (domain)** to **OS Logon (local)**.

8.5.7 Mac OS logon

This event configures the chains that can be used to log on in Apple Mac OS. If you want to use Mac OS Client on non-domain joined workstations, change the **Event type** from **OS Logon (domain)** to **OS Logon (local)**.

8.5.8 NAM

The Advanced Authentication server supports integration with Advanced Authentication Access Manager. Advanced Authentication Access Manager Advanced Authentication plug-in must be installed and configured on a NAM appliance and User Stores must be added for the used repositories.

8.5.9 NCA

The Advanced Authentication server supports integration with Advanced Authentication CloudAccess. CloudAccess must be configured to use Advanced Authentication as an authentication card and User Stores must be added for the used repositories. Check the Advanced Authentication CloudAccess documentation.

Radius Server

The Advanced Authentication server contains a built-in RADIUS server that is able to authenticate any RADIUS client using one of chains configured for the event.

8.5.10 Report logon

This event allows you to configure the chains and user categories that can be used to sign-in to the Advanced Authentication - Reporting Portal.

8.5.11 Windows logon

This event configures the chains that can be used to log on in Microsoft Windows.

In an event you can configure a prioritized list of chains that can be used to get access to that specific event. If you want to use Windows Client on non-domain joined workstations, change the **Event type** from **OS Logon (domain)** to **OS Logon (local)**.

8.5.12 Radius Server

The Advanced Authentication server contains a built-in RADIUS server that is able to authenticate any RADIUS client using one of chains configured for the event.

IMPORTANT: Currently the built-in RADIUS Server supports only PAP.

The RADIUS Server supports all authentication methods except Card, FIDO U2F, Fingerprint, Notaris ID, and PKI.

Single-factor authentication with a Smartphone method is not supported for RADIUS by the in-built design. It is recommended to use it in a two-factor chain with LDAP Password method.

To configure an authentication event for Advanced Authentication, follow the steps:

1. Open the **Events** section.
2. Click the **Edit** button next to the Radius Server event.
3. Ensure that the event has **Is enabled** option set to ON.
4. Select chains that will be assigned to the event*.
5. Select Radius from **Endpoint whitelists**.
6. Click **Add** button to add a Radius Client assigned to the event:
   - Specify the Radius Client name in the **Name** text field.
   - Enter an **IP address** of the Radius Client.
   - Enter the Radius Client **Secret** and **Confirmation**.
   - Ensure that the Radius Client is set to **ON**.
   - Click the save button next to the Radius Client.
   - Add more Radius Clients if necessary.
7. Click **Save** at the bottom of the **Events** view to save configuration.

IMPORTANT: When you specify more than one Chain to use with the Radius Server, follow one of the described ways:

1. Each assigned Chain of the RADIUS event may be assigned to a different LDAP group. E.g. LDAP Password+Smartphone chain is assigned to a Smartphone users group, LDAP Password+HOTP chain is assigned to a HOTP users group. If a RADIUS user is a member of the both groups, a top group will be used.
2. It's possible to use the RADIUS authentication using any Chain when entering `<username> <chain shortname>` in username field. E.g. `pjones sms`. Ensure that you have the short names specified for the used Chains. Usage of the option may be not admissible in your RADIUS client (like in FortiGate).

IMPORTANT: If you use the LDAP Password+Smartphone chain it is possible to use an offline authentication by entering the following data in the password field: <LDAP Password>&<Smartphone OTP>. E.g. Q1w2e3r4&512385. The same use case is supported for LDAP Password+OATH TOTP, LDAP Password+OATH HOTP, Password+Smartphone, Password+OATH TOTP, Password+OATH HOTP.

NOTE: When multitenancy is enabled, you can use one of the following forms of user name:

- <repository_name>\<username>
- <tenant_name>\<repository_name>\<username>
- <username>@<tenant_name>
- <repository_name>\<username>@<tenant_name>

NOTE: The Advanced Authentication Framework stores the Radius Event settings only on a server where administrator performs the configuration (usually this is DB Master server). After conversion of DB Slave server to DB Master server the configuration may be lost. Open the Radius Event settings and click Save to apply the configuration.

For information on how to configure integrations with the third-party solutions, see “Chapter 12, “Configuring Integrations,” on page 111”.

OAuth 2.0 Event

This section describes the roles and modes used in OAuth 2.0 event.

OAuth 2.0 Roles

OAuth 2.0 event consists of the following 4 roles:

- **Resource Owner:** An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an end-user.
- **Resource Server:** The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.
- **Client:** An application making protected resource requests on behalf of the resource owner and with its authorization. The term "client" does not imply any particular implementation characteristics.
- **Authorization Server:** The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

OAuth 2.0 Modes

For more information on OAuth 2.0 modes, see the website.

Authorization Code

The workflow for authorization code involves the following steps:

1. The OAuth client initiates the flow when it directs the user agent of the resource owner to the authorization endpoint. The OAuth client includes its client identifier, requested scope, local state, and a redirection URI.
2. The authorization server authenticates the resource owner through the user agent and establishes whether the resource owner grants or denies the access request.
3. If the resource owner grants access, the OAuth client uses the redirection URI provided earlier to redirect the user agent back to the OAuth client. The redirection URI includes an authorization code and any local state previously provided by the OAuth client.
4. The OAuth client requests an access token from the authorization server through the token endpoint. The OAuth client authenticates with its client credentials and includes the authorization code received in the previous step. The OAuth client also includes the redirection URI used to obtain the authorization code for verification.
5. The authorization server validates the client credentials and the authorization code. The server also ensures that the redirection URI received matches the URI used to redirect the client in Step 3. If valid, the authorization server responds back with an access token.

Implicit Grant

The workflow for implicit grant involves the following steps:

1. The OAuth client initiates the flow by directing the user agent of the resource owner to the authorization endpoint. The OAuth client includes its client identifier, requested scope, local state, and a redirection URI. The authorization server sends the user agent back to the redirection URI after access is granted or denied.
2. The authorization server authenticates the resource owner through the user agent and establishes whether the resource owner grants or denies the access request.
3. If the resource owner grants access, the authorization server redirects the user agent back to the client using the redirection URI provided earlier. The redirection URI includes the access token in the URI fragment.
4. The user agent follows the redirection instructions by making a request to the web server without the fragment. The user agent retains the fragment information locally.
5. The web server returns a web page, which is typically an HTML document with an embedded script. The web page accesses the full redirection URI including the fragment retained by the user agent. It can also extract the access token and other parameters contained in the fragment.
6. The user agent runs the script provided by the web server locally, which extracts the access token and passes it to the client.

OAuth 2.0 Sample Web Application

To create a sample web application you need Python v3 (the sample script prepared on v3.4.3).

The following web application demonstrates all the functionalities supported by OAuth 2.0 integration. OAuth 2.0 server is an authorization and resource server. As an authorization server the user has to go through authentication chains. As a resource server some user details are provided.

You have to create the following 5 files:

- **Sample script (oauth2_test.py)**

```
1.  from bottle import Bottle, request, run, redirect, SimpleTemplate, template
2.from urllib.parse import urlparse, urlunparse, urlencode,quote
3.  import urllib.request
4.import base64
5.  import ssl
6.import json
7.
8.app = Bottle()
9.
10.client_id = 'id-rSCzuBLQgXCATfkXZ4fsedAo8sPsWxSs'
11.  client_secret = 'secret-91DpzWFD26RriURR7KJ1pryFx7V9QeDm'
12.redirect_uri = 'http://localhost:8088/'  # this app callback URI
13.  authorization_endpoint = 'https://192.168.0.151/osp/a/TOP/auth/oauth2/
grant'
14.  attributes_endpoint = 'https://192.168.0.151/osp/a/TOP/auth/oauth2/
getattributes'
15.  state = {}
16.
17.  @app.get('/getattr')
18.def get_attributes():
19.      params = urlencode({
20.        'attributes': 'client username userRepository user_dn user_cn mail
sid upn netbiosName',
21.        'access_token': state['access_token']
22.      })
23.    url = attributes_endpoint + '?' + params
24.      print('getattr url: {}\n'.format(url))
25.    req = urllib.request.Request(url)
26.     gcontext = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)  # avoid cert checking
27.    with urllib.request.urlopen(req, context=gcontext) as response:  #
perform GET request and read response
28.        rsp = response.read()
29.      attributes = json.loads(rsp.decode('utf-8'))
30.    return template('attributes.html', items=attributes.items(),
refresh_token=urllib.parse.quote(state['refresh_token']))
31.
32.
33.@app.get('/')
34.  def do_get():
35.    code = request.query.get('code')
36.      if code:
37.        # got code from OAuth 2 authentication server
38.          token = get_token_code(code)
39.        state.update(token)
40.          return template('token.html', items=token.items(),
refresh_token=urllib.parse.quote(token['refresh_token']))
41.      else:
42.        return template('main.html')
43.
44.
45.  @app.get('/logon')
46.def do_logon():
```

```
47.      pr=list(urlparse(authorization_endpoint))
48.    # set query
49.      pr[4]=urlencode({
50.        'response_type': 'code',
51.          'client_id': client_id,
52.        'redirect_uri': redirect_uri
53.      })
54.    # perform redirection to OAuth 2 authentication server
55.      redirect(urlunparse(pr))
56.
57.  @app.get('/logon-implicit')
58.def do_logon_implicit():
59.      # parse authorization_endpoint URL
60.    pr = list(urlparse(authorization_endpoint))
61.      # set query
62.    pr[4] = urlencode({
63.          'response_type': 'token',
64.        'client_id': client_id,
65.      })
66.    # perform redirection to OAuth 2 authentication server
67.      redirect(urlunparse(pr))
68.
69.  @app.get('/logon-creds')
70.def do_logon_creds():
71.      return template('logonform.html')
72.
73.  @app.post('/logon-creds')
74.def do_logon_creds_post():
75.      username = request.forms.get('username')
76.    password = request.forms.get('password')
77.      token = get_token_password(username, password)
78.    state.update(token)
79.      return template('token.html', items=token.items(),
refresh_token=urllib.parse.quote(token['refresh_token']))
80.
81.def get_token_password(username, password):
82.      # prepare POST parameters - encode them to urlencoded
83.    data = urlencode({
84.          'grant_type': 'password',
85.        'username': username,
86.          'password': password
87.    })
88.      data = data.encode('ascii')  # data should be bytes
89.    resp_text = post_data(data, prepare_headers())
90.      print(resp_text)
91.    return json.loads(resp_text)
92.
93.@app.get('/refresh')
94.  def do_refresh():
95.    token = refresh_access_token(request.query.get('refresh_token'))
96.      state.update(token)
97.    return template('token.html', items=token.items(),
refresh_token=state.get('refresh_token', ''))
98.
99.  def get_token_code(code):
100.    # prepare POST parameters - encode them to urlencoded
101.      data = urlencode({
102.        'grant_type': 'authorization_code',
103.          'code': code,
104.        'redirect_uri': redirect_uri
```

```
105.      })
106.    data = data.encode('ascii')  # data should be bytes
107.      resp_text = post_data(data, prepare_headers())
108.    print(resp_text)
109.      return json.loads(resp_text)
110.
111.  def refresh_access_token(refresh_token):
112.    print('refresh_token: {}'.format(refresh_token))
113.      # prepare POST parameters - encode them to urlencoded
114.    data = urlencode({
115.          'grant_type': 'refresh_token',
116.        'refresh_token': refresh_token,
117.      })
118.    data = data.encode('ascii')  # data should be bytes
119.      resp_text = post_data(data, prepare_headers())
120.    print(resp_text)
121.      return json.loads(resp_text)
122.
123.  def prepare_headers(use_content_type_hdr = True):
124.    hdrs = {
125.          'Authorization': 'Basic {}'.format(base64.b64encode(
126.            '{}:{}'.format(quote(client_id, safe=''), quote(client_secret,
safe='')).encode('ascii')).decode(
127.             'ascii')),
128.      }
129.    if use_content_type_hdr:
130.          hdrs.update({'Content-type': 'application/x-www-form-
urlencoded'})
131.      return hdrs
132.
133.  def post_data(data, headers):
134.      print('post_data\nheaders:\n{}\ndata:\n{}'.format(headers, data))
135.      req = urllib.request.Request(authorization_endpoint, data, headers)
136.      gcontext = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)  # avoid cert
checking
137.    with urllib.request.urlopen(req, context=gcontext) as response:  #
perform POST request and read response
138.        rsp = response.read()
139.      return rsp.decode('utf-8')
140.
141.  run(app, host='0.0.0.0', port=8088)
```

NOTE: In the script you need to change values for client_id, client_secret, and Advanced Authentication Server address in authorization_endpoint and attributes_endpoint (lines 10-14).

- **Main menu (main.html)**

```
1.  <!DOCTYPE html>
2.<html>
3.  <head lang="en">
4.    <meta charset="UTF-8">
5.      <title></title>
6.    <script type="text/javascript">
7.           //<![CDATA[
8.            function getHashParam(name) {
9.                  var hash = window.location.hash;
10.                if (hash) {
11.                   if (name = (new RegExp('[#&]' + encodeURIComponent(name)
+ '=([^&]*)')).exec(hash))
12.                      return decodeURIComponent(name[1]);
13.                }
14.              }
15.            function showResult() {
16.                  if (window.location.hash) {
17.                    document.getElementById('result').innerHTML = '<table
border="1">'+
18.                        '<tr><td>access_token</
td><td>'+getHashParam('access_token')+'</td></tr>'+
19.                        '<tr><td>token_type</
td><td>'+getHashParam('token_type')+'</td></tr>'+
20.                        '<tr><td>expires_in</
td><td>'+getHashParam('expires_in')+'</td></tr>'+
21.                        '</table>';
22.                  } else {
23.                    document.getElementById('result').innerHTML = 'Implicit
granted token is not found';
24.                }
25.              }
26.          // ]]>
27.          </script>
28.</head>
29.  <body onload="showResult();">
30.<div id="result">result</div><br/>
31.  <br/>
32.Click <a href="/logon">here</a> to obtain an authentication token through
Authorization Code Grant<br/>
33.Click <a href="/logon-implicit">here</a> to obtain an authentication token
through Implicit Grant (the token will be received in hash part of THIS
page)<br/>
34.  Click <a href="/logon-creds">here</a> to obtain an authentication token
through Resource Owner Password Credentials Grant<br/>
35.  </body>
36.</html>
```

- **Token information (token.html)**

```
1.  <!DOCTYPE html>
2.<html>
3.  <head lang="en">
4.    <meta charset="UTF-8">
5.      <title></title>
6.</head>
7.  <body>
8.Token<br/>
9.  <table border="1">
10.    % for k, v in items:
11.      <tr>
12.        <td>{{k}}</td>
13.          <td>{{v}}</td>
14.    </tr>
15.      % end
16.</table>
17.  <br/>
18.<a href="/getattr">Get attributes</a><br/>
19.  <a href="/refresh?refresh_token={{refresh_token}}">Refresh token</a>
20.</body>
21.  </html>
```

- **Attributes information (attributes.html)**

```
1.  <!DOCTYPE html>
2.<html>
3.  <head lang="en">
4.    <meta charset="UTF-8">
5.      <title></title>
6.</head>
7.  <body>
8.Attributes<br/>
9.  <table border="1">
10.    % for k, v in items:
11.      <tr>
12.        <td>{{k}}</td>
13.          <td>{{v}}</td>
14.    </tr>
15.      % end
16.</table>
17.  <br/>
18.<a href="/refresh?refresh_token={{refresh_token}}">Refresh token</a>
19.  </body>
20.</html>
```

- **Logon form for Resource Owner Password Credentials Grant mode (logonform.html)**

```
1.  <!DOCTYPE html>
2.<html>
3.  <head lang="en">
4.    <meta charset="UTF-8">
5.      <title></title>
6.</head>
7.  <body>
8.<form method="post" action="/logon-creds">
9.      User name: <input type="text" name="username"><br/>
10.    Password: <input type="password" name="password"><br/>
11.      <input type="submit">
12.</form>
13.  </body>
14.</html>
```

Exploring Sample Web Application

1. Run the script: python oauth2_test.py.
2. Open the URL: http://localhost:8088.

   A message is displayed with the following modes to select:

   - Authorization Code Grant
   - Implicit Grant (the token will be received in hash part of THIS page)
   - Resource Owner Password Credentials Grant (is not supported by default but it can be activated in AAF)
3. Use the required grant based on your requirement.

   Authorization Code Grant

   a. Ensure that **Use for Owner Password Credentials** option is set to **OFF** in Advanced settings section for the used OAuth2 event.

   b. Click the first link. NetIQ Access page will be displayed with Username request.

   c. Enter the Username.

   d. Click **Next.**

   e. Authenticate using all required methods of used chain. The result page shows the access_token, token_type and expires_in.

      - Click Get attributes to look at the attributes.
      - Click Refresh token to refresh token. The access_token value will be updated.

   Implicit Grant

   a. Ensure that **Use for Owner Password Credentials** option is set to **OFF** in Advanced settings section for the used OAuth2 event.

   b. Click the second link. NetIQ Access page will be displayed with Username request.

   c. Enter the Username.

   d. Click **Next.**

   e. Authenticate using all required methods of used chain. The result page shows the access_token, token_type and expires_in.

   Resource Owner Password Credentials Grant

   a. Open Advanced settings section for the used OAuth2 event.

   b. Set **Use for Owner Password Credentials** option is to **ON.**

   c. Click the third link. A request for Username and Password will be displayed.

   d. Enter the username and password and then click **Submit.** The result page shows the access_token, token_type and expires_in.

8.6 Managing Endpoints

In this section you can manage existing endpoints. Endpoint means a place where the Advanced Authentication server will authenticate. It can be a certain workstation with Microsoft Windows for Windows Client endpoint, or Advanced Authentication Access Manager appliance for NAM endpoint.

Such endpoints will be automatically added during installation of NAM Advanced Authentication plug-in or after installation of Windows Client.

Only the Radius endpoint is predefined and available in Endpoints section by defaut.

The following endpoint types are supported:

1. NAM
2. NCA
3. Radius
4. Mac OS X Client (Local Hostname will be used as endpoint name)
5. OSP Endpoint (used for OAuth 2.0 and SAML 2.0 events)
6. Windows Client (DNS name will be used as endpoint name)
7. Other (can be used by third-party applications)

To manage an authentication endpoint for Advanced Authentication, follow the steps:

1. Open the **Endpoints** section.
2. Click the **Edit** button next to an applicable endpoint.
3. It's possible to rename the endpoint, change its description or endpoint type.
4. Select whether the current endpoint is enabled or disabled by clicking the **Is enabled** toggle button.
5. Specify an **Endpoint Owner** if you have configured a specific chain to be used by Endpoint owner only. This is a user account who should be able to use a different Creating a Chain other than regular users use for authentication.

   NOTE: The Endpoint Owner feature is supported for Windows Client, Mac OS Client and Linux PAM Client only.

6. Click **Save** at the bottom of the **Events** view to save configuration.

You can create an endpoint manually. This can be used for the third-party applications that do not support the creation of endpoints.

To create an endpoint manually, perform the following steps:

1. Click **Add**.
2. On the **Add endpoint** page, specify a **Name** of the endpoint and its **Description**.
3. Set the **Type** to **Other**.
4. Set **Is enabled** to **ON** to enable the endpoint.
5. Leave **Endpoint Owner** blank.
6. Click **Save**. The **New Endpoint secret** window is displayed.
7. Grab the values specified in **Endpoint ID** and **Endpoint Secret** and place them in a secure place in your application.

   NOTE: You will not be able to get the Endpoint ID and Endpoint Secret later on the appliance.

8. Click **OK**.

The following legacy endpoints are presented to you:

- **Endpoint41**

  Description: Well-known endpoint (id 41414141)

  Type: Other

  Purpose: support of legacy NetIQ CloudAccess plug-in.

- **Endpoint42**

  Description: Well-known endpoint (id 42424242)

  Type: Other

  Purpose: support of legacy NetIQ Access Manager plug-in.

The NetIQ Access Manager and NetIQ Cloud Access plug-ins work with the hard coded endpoint ID and secret. In 5.2 and higher, endpoints must be registered. This breaks the backward compatibility with old plug-ins. These two legacy endpoints allow to keep the old plug-ins working.

IMPORTANT: You must ensure not remove an endpoint that has at least one component running on it such as Windows Client, Logon Filter, RD Gateway plug-in, or ADFS plug-in. Endpoint is removed automatically when you uninstall Windows Client. However you must remove the endpoint manually when you uninstall Logon Filter, RD Gateway plug-in or ADFS plug-in.

If you remove an endpoint accidentally, ensure to remove the records with prefix **endpoint*** from the `%ProgramData%\NetIQ\Windows Client\config.properties` file and restart the machine. This recreates the endpoint.

8.7 Configuring Policies

To configure an applicable policy for Advanced Authentication, follow the steps:

1. Open the **Policies** section. The list of available authentication methods will be displayed.
2. Click the **Edit** button next to an applicable policy.
3. Edit configuration settings for a specific policy.
4. Click **Save** at the bottom of the **Policies** view to save changes.

In the section you can find the following settings:

- Admin UI Whitelist: security settings which allows to limit using of Advanced Authentication Administrative Portal only for permitted IP addresses.
- Authenticator management options: setting that allows a helpdesk (security officer) to link authenticators of a user to help authenticate to another user's account. This policy also allows you to disable re-enrollment of authenticators by users in the Self-Service portal.
- Cache options: security settings which allows to disable local caching of authenticators.
- CEF log forwarding: settings to configure an external syslog server.
- Delete me options: Enable/Disable delete me option.
- Endpoint management options: an option to require authentication data for Endpoint creation. It must be disabled when installing Advanced Authentication Access Manager Advanced Authentication plug-in.
- Event categories: Allows you to add categories, which can be used in an event to support multiple enrollments for a method.
- Geo fencing options: setting that helps to create authentication zones by drawing boundaries for a geographical location.
- HTTPS Options: setting that allows administrators to configure policies to ensure that appliance is safe from security vulnerabilities.
- Helpdesk Options: a security option which allows to disable asking for user's credential when a security officer is managing the user's authenticators.
- Kerberos SSO Options: Allows you to select a repository for Kerberos single sign-on.

- Last Logon Tracking Options: allows to enable tracking for last logon to configure and use simple chain corresponding to a high-security chain.
- Lockout Options: security settings which allows to lock user after some authentication failures.
- Login Options: allows to specify the default repositories, to avoid of necessity to enter a repository name in username field.
- Logo: setting that allows you to set an image or alternate text as a logo for the Administration and Self-Service portal.
- Logon Filter for AD: Enable/Disable logon filter for Active Directory.
- Mail sender: SMTP server settings.
- Multitenancy Options: Enable/Disable multitenancy mode in the appliance.
- Password Filter for AD: Enable/Disable password filter for Active Directory.
- SAML 2.0 options: settings that allows you to add external URL and to download identity provider's SAML 2.0 Metadata.
- SMS sender: settings for external SMS service provider, contains predefined settings for Twilio, MessageBird.
- Services Director Options: setting to enable the integration with Services Directory.
- Voice sender: Twilio settings for Voice and Voice OTP method; an option to allow enrollment for users without telephone number.

IMPORTANT: The configured policies will be applied for all servers.

NOTE: A tenant administrator will not have access to CEF log forwarding and Multitenancy Options.

8.7.1 Admin UI Whitelist

The **Admin UI whitelist** settings are located in the **Policies** section.

The settings allows to configure access to the Advanced Authentication Administrative Portal only for permitted IP addresses. By default the restrictions are not set. To configure the restrictions click **Add** button. Enter address in format 10.20.30.0/255.255.255.0 or 10.20.30.0/24. Advanced Authentication has an automatic check which allows to prevent administrators from losing access to the Administrative Portal. If your IP address is out of the range you will see a message: `Your IP address is not whitelisted. You will lose access! Please add your IP.`To apply the changes click **Save** button.

8.7.2 Authenticator management options

This policy allows you to configure two settings:

- **Enable sharing**: This setting allows a user to authenticate with his/her authenticator to another user's account. The helpdesk admin will be able to link an authenticator of one user to another user.

  To enable sharing authenticators, turn **Enable sharing** to **ON**.

  NOTE: Only online logon by linked authenticators is supported. Cached logon is not supported.

NOTE: The supported methods for sharing authenticators are TOTP, HOTP, Password, Fingerprint, Card and FIDO U2F.

- **Disable re-enrollment**: This setting allows you to restrict users from re-enrolling, editing, and deleting the enrolled authenticators in the Self-Service portal.

  To disable re-enrollment or removal of authenticators, turn **Disable re-enrollment** to **ON**.

  NOTE: This setting disables re-enrollment and removal of the authenticators only in the Self-Service portal. The setting has no effect on the Helpdesk portal.

8.7.3 Cache Options

The Cache options are located in the Policies section.

NOTE: This functionality is supported for Windows Client, Mac OS X Client, Linux PAM Client for chains which use the methods: LDAP Password, Password, HOTP, TOTP, Smartphone (offline mode), Card, FIDO U2F, Fingerprint and PKI.

The caching functionality allows to store credentials on client side for offline authentication when the Advanced Authentication Server is not available. This helps a user who performed a successful logon with the Advanced Authentication Server when the server was available, to use the offline authentication during a business trip or access the system from home.

By default the **Enable local caching** option is enabled. To disable the caching switch option to **OFF** and click **Save**.

NOTE: To cache Fingerprint data, you need to install Microsoft.NET Framework 4 or higher on your workstation.

The caching period cannot be configured. Cache will be cleared only if the **Enable local caching** option is disabled.

8.7.4 CEF log forwarding

The **CEF log forwarding** settings are located in the **Policies** section.

The settings allows to configure forwarding of logs to an external Syslog server. The central logging server may be used for log forwarding. To configure it, follow the steps:

1. Open the **Policies** section.
2. Click the **Edit** button next to the **CEF log forward** policy.
3. Select the **Enable** check box.
4. Specify the IP address of the remote logging server in the **Syslog server** text field.
5. Specify the port of the remote logging server in the **Port** text field.
6. Select an applicable transfer protocol from the **Transport** drop-down list.
7. Click **Save** at the bottom of the **Policies** view to save changes.

IMPORTANT: The same Syslog configuration is used for each server type. Each server type in the appliance records its own log file.

Events from all facilities are recorded to syslog. E.g., Advanced Authentication Server Core, Kernel, Daemon, etc.

The following Server Core events are being recorded in the log file:

- Failed to join endpoint
- No rights to join endpoint
- Endpoint joined
- Failed to remove endpoint
- No rights to remove endpoint
- Endpoint remove
- Failed to create endpoint session
- Endpoint session ended
- Failed to create endpoint session
- Invalid endpoint secret
- Endpoint session started
- Failed to create local user
- Local user was created
- Failed to remove local user
- Local user was removed
- Repository configuration was changed
- Failed to add repository
- New repository was added
- Request failed
- Server started
- Server stopped
- Server unexpectedly stopped
- Failed to assign template to the user
- Template was assigned to the user
- Failed to change template
- Template was changed
- Failed to enroll template for the user
- Template was enrolled for the user
- Failed to link template
- Template was linked
- Failed to remove template link
- Template link was removed
- Failed to remove template
- Template was removed
- Failed to create user
- User was created
- User can't enroll the assigned template

- User enroll the assigned template
- User was failed to authenticate
- User logon started
- User was successfully logged on
- User was switched to different method
- User do not want logon by phone but Twilio calling
- User read app data
- User write app data

8.7.5 Delete me options

The **Delete me options** allow you to enable/disable Advanced Authentication users with **Delete me** option, which can be used to delete all user data including enrolled methods and all data from the repository.

If **Enable delete me feature** is set to **ON,** then Advanced Authentication users will get **Delete me** option by clicking on the user name drop-down list in top right corner of the Self-Service portal. By clicking **Delete me** and then clicking **OK**, all the user data from the repository including the enrolled methods are deleted.

If **Enable delete me feature** is set to **OFF**, then Advanced Authentication users will not get **Delete me** option in the Self-Service portal.

8.7.6 Endpoint Management Options

The **Endpoint management options** are located in the **Policies** section.

If the option **Require admin password to register endpoint/workstation** is enabled, the Advanced Authentication will require endpoints to provide the local administator's credentials during installation of endpoint component.

The option must be disabled when installing the Access Manager Advanced Authentication plug-in or Advanced Authentication Windows Client or Advanced Authentication MacOS Client. Otherwise the endpoints will not be created.

8.7.7 Helpdesk Options

The **Helpdesk options** are located in the **Policies** section.

The options provide security settings for security officers who manage users' authenticators in Helpdesk Portal.

With the enabled **Ask credentials of management user** option the security officers should provide credentials of users before its management. This authentication uses the Helpdesk User event. Ensure that you have specified a chain for the Helpdesk User event.

When the option is set to OFF a security officer doesn't need to provide credentials of managed user. This may be not secure, but user management can be done much faster when the option is disabled.

8.7.8 HTTPS Options

This policy allows you to configure two settings:

- **Enable TLS 1.0**: Advanced Authentication recommends to keep the option disabled by default to ensure security vulnerabilities are prevented as TLS 1.0 is considered as an unsafe protocol. In some cases, you may enable the option to support old versions of browsers. For more information on browser support for TLS, see TLS support for web browsers.
- **Enable HTTP compression**: This setting allows you to enable HTTP compression to accelerate performance in the scenarios of low band with or when the network connectivity is very slow.

8.7.9 Kerberos SSO Options

The **Kerberos SSO options** policy allows you to select an Active Directory repository, which points to a domain for which you want to configure single sign-on.

Perform the following steps:

1. Select a required repository.
2. Click **Save.** A message `Policy "Kerberos SSO options" saved` is displayed.
3. Wait for 2-3 minutes for the changes to apply.

NOTE: This feature works only for a single Active Directory repository at a time and is disabled in multitenancy mode.

Generate a keytab file for each Advanced Authentication Server and upload them in appliance for each server. For more information, see Uploading Keytab File.

After configuring the Kerberos SSO options and uploading the keytab files, enable **Allow kerberos SSO** option for the required event. Kerberos SSO is supported for AdminUI, Authenticators Management, Helpdesk and Report logon events. For more information on configuring an event, see Configuring Events.

By default, basic authentication window is displayed in your browser while accessing a configured Advanced Authentication portal. Advanced Authentication Servers' sites must be added to the Local intranet in browser on the domain-joined workstations to avoid it. Perform the following steps to do it for Internet Explorer:

1. From the **Start** menu, navigate to **Control Panel** > **Network and Internet** > **Internet Options.**
2. In the **Internet Properties** window, click **Security** tab and then select **Local intranet.**
3. Click **Sites.**
4. In the **Local intranet** window, click **Advanced.**
5. Add the Advanced Authentication Servers' sites to the zone. For example: `https://v5.netiq.loc` or `v5.netiq.loc`
6. Click **Close** and save the changes.

NOTE: Basic authentication window is displayed while accessing a configured Advanced Authentication portal, if **Kerberos SSO** option is enabled for Authenticators Management event and security is set to High for **Local intranet** in Internet Explorer.

NOTE: By default, Firefox browser does not support single sign-on. If you are using Firefox browser, then you can enable single sign-on by performing the steps suggested in the website.

8.7.10 Last Logon Tracking Options

The **Last Logon Tracking options** allow you to enable tracking for the last logon. You can simplify multi-factor authentication by automatically switching to another (simple) chain (that contains less factors) within few hours of authentication by a high-security chain. For example, if a user authenticates by the `LDAP Password+Card` methods once in a day, the user can further use only `Card` without the `LDAP Password` method, or if a user authenticates by the `Fingerprint+SMS methods` once in every four hours, the user can further use Smartphone authentication only.

To enable tracking, switch the **Enable tracking option** to **ON**.

To configure a high-security chain and the corresponding simple chain, see Creating Chains.

8.7.11 Lockout Options

The **Lockout options** are located in the **Policies** section.

The options allows to configure the user account lockout in case of reaching limit on failure attempts. It may be used to prevent of guessing the one-time passwords. It's possible to configure the following settings:

1. **Enable**: The option enables the lockout settings.
2. **Failed attempts**: The option allows to setup a limit of authentication attempt failures after which the user account will be locked. 3 attempts by default.
3. **Lockout period**: The option allows to configure a period within which the user will be locked and not possible to authenticate. 300 seconds by default.
4. **Lock in repository**: The option allows to lock the user account in repository. The Lockout period option is not used for the case. It will be required for system administrator to unlock the user manually in the repository.

   IMPORTANT: You need to configure the appropriate settings in your repository, for the options to function correctly.

   For Active Directory Domain Services, the Account lockout threshold policy must be enabled on Domain Controllers.

   For NetIQ eDirectory the Intruder Detection must be properly configured.

It's possible to manage the locked users (only the users who are not locked in repository). To do it switch to the **Repositories** section. Click **Edit** button for the used repository. Switch to **Locked Users** tab. Click **Remove** button next to account name to unlock the user account.

8.7.12 Login Options

The **Login options** are located in the **Policies** section.

Here it's possible to configure the **Default** repositories. Using the Default repositories it's not required to enter repository name before a username for authentication. So instead of `company\pjones` it will be possible to enter only `pjones`, instead of `local\admin` it will be possible to use `admin`.

8.7.13 Logo

This policy allows you to set and customize an image as a logo for the Administration and Self-Service portal. You can also set an alternate text instead of an image as logo.

To set a logo for the Administration and Self-Service portal, perform the following steps:

1. In the **Logo** page, set **Use image** to **ON**.
2. Specify an alternate text for the image in **Image ALT text**.
3. Specify the **URL** that is displayed when you click on the logo.
4. Select an image for the logo. The image resolution must be `230x50` pixels. The supported formats are `jpg` and `png`.
5. You can also set a mini logo with an image. This mini logo is displayed when the navigation pane on the left is collapsed. The image resolution for the mini logo must be `50x50` pixels.
6. Click **Save**.

NOTE: The logo is applied for all the tenants. A tenant administrator cannot customize the logo.

8.7.14 Logon Filter for AD

The **Logon Filter for AD** is located in the **Policies** section.

This policy enables use of Logon Filter which must be installed on all Domain Controllers in the domain and must be properly configured. Logon Filter allows you to prohibit authentications of users without the Advanced Authentication solution.

For information to configure Logon Filter, see Configuring Logon Filter.

8.7.15 Mail Sender

The **Mail sender** settings are located in the **Policies** section.

The section contains the mail server settings. It's used by Email OTP to send the email messages with one-time passwords to users.

It's required to configure the following settings:

1. **Host**, the outgoing mail server name (e.g. smtp.company.com)
2. **Port**, the used port number (e.g. 465)
3. **Username**, username of an account which will be used to send the authentication email messages (e.g. noreply or noreply@company.com)
4. **Password**, password for the specified account
5. **TLS** and **SSL** is used to specify a cryptographic protocol used by the mail server.

Click **Save** to apply the changes.

Authentication flow

The following chart demonstrates the authentication flow:

A user is authenticating on endpoint (which can be the user's laptop with Advanced Authentication Windows Client installed or a website etc.) by Email method.

1. The endpoint calls the Advanced Authentication Server.
2. It validates the provided user's credentials and gets an email address of the user from a used Repository.
3. Advanced Authentication Server sends the request to a configured Mail Server to send an Email message with generated content which includes a one-time password (OTP) for authentication.
4. Mail Server sends the message to the user's email address.
5. Mail Server sends the 'sent' signal to the Advanced Authentication Server.
6. Advanced Authentication Server sends a request to enter an OTP on the endpoint side.
7. The user enters an OTP from the email message. The Advanced Authentication Server gets the OTP.
8. Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTPS protocol is used for the internal communication.

Access configuration

Advanced Authentication Server - Mail Server (SMTP, outbound).

8.7.16 Multitenancy Options

A tenant is a company with a group of users sharing common access with specific privileges. Multitenancy options allows you to have a single instance of Advanced Authentication solution supporting multiple tenants. You can enable Multitenancy Options when you need to support more than one tenant on a single appliance.

You can enable or disable multitenancy option.

IMPORTANT: If you have the workstations with Windows Client, Mac OS X Client or Linux PAM Client installed, then perform the following steps before enabling Multitenancy Option:

1. Upgrade the client components to 5.4 or above.
2. Configure the clients to point to a tenant. For more information on configuring in Windows Client, refer to Configuration Settings for Multitenancy. For more information on configuring in Mac OS X Client, refer to Configuration Settings for Multitenancy. For more information on configuring in Linux PAM Client, refer to Configuration Settings for Multitenancy.

The steps listed above are critical and if not performed, the users on the workstations will not be able to login.

8.7.17 Password Filter for AD

Password Filter automatically updates the LDAP Password stored inside Advanced Authentication, whenever the password is changed or reset in the Active Directory. This helps you to authenticate without getting any prompt to synchronize the password after it is changed or reset.

Set **Update password on change** option to **ON,** to enable updating of the LDAP password in Advanced Authentication, when it is changed in the Active Directory. This helps you to authenticate without getting any prompt to synchronize the password after it is changed. If **Update password on change** is set to **OFF,** user will get a request to synchronize the password while logging in to Windows, if he/she changed his/her password where the user will need to enter an actual password.

Set **Update password on reset** option to **ON,** to enable updating of the LDAP password in Advanced Authentication, when it is reset in the Active Directory. This helps you to authenticate without getting any prompt to synchronize the password it is reset. If **Update password on reset** is set to **OFF,** user will get a request to synchronize the password while logging in to Windows, if administrator has reset the user's password where the user will need to enter an actual password.

NOTE: Endpoint for Password Filter should be trusted. To set this option, open the Advanced Authentication - Administrative Portal > **Endpoints** section, edit an endpoint of the Password Filter, set **Is trusted** flag to **ON** and add a description. Save the changes.

8.7.18 SMS Sender

The **SMS sender** settings are available in the **Policies** section.

This section contains the SMS service provider settings. It is used by SMS OTP to send the SMS messages with one-time passwords to users. Advanced Authentication contains the predefined settings for Twilio and MessageBird services.

To configure SMS sender settings for **Twilio** service select Twilio in **Sender service** drop down list and fill or set the following fields:

1. Account sid
2. Auth token
3. Use Copilot
4. Sender phone
5. Messaging Service SID

NOTE: **Messaging Service SID** option is enabled only when **Use Copilot** option is set to **ON.**

You can find more information on the Twilio website.

For more information on Copilot and its features, visit the following websites:

https://www.twilio.com/copilot#phone-number-intelligence

https://www.twilio.com/docs/api/rest/sending-messages-copilot#features

To configure SMS sender settings for **MessageBird** service, select Messagebird in **Sender service** drop down list and fill the following fields:

1. Username
2. Password
3. Sender name

You can find more information on the MessageBird website.

IMPORTANT: MessageBird API v2 is not supported. To activate MessageBird API v1, go to the MessageBird account, click **Developers** from the left navigation bar and open the API access tab. Click **Do you want to use one of our old API's (MessageBird V1, Mollie or Lumata)? Click here**.

To configure SMS sender manually, select **Generic** in **Sender service** drop down list and perform the following steps:

1. Specify a **Service URL** value. For example: Clickatell http://api.clickatell.com/http/sendmsg?.
2. Leave the **HTTP Basic Auth Username** and **HTTP Basic Auth Password** text boxes blank.
3. Select **POST** from the **HTTP request method** drop down list.
4. Click **Add** and create the following parameters in **HTTP request body** section.
   - name: **user**

     value: name of your account
   - name: **to**

     value: {phone}
   - name: **text**

     value: {message}
   - name: **api_id**, this is a parameter issued upon addition of an HTTP sub-product to your Clickatell account. A single account may have multiple API IDs associated with it.
   - name: **from**

     value: sender's phone number
5. Click **Add secure** and create the following parameter in HTTP request body section.
   - name: **password**

     value: current password that is set on the account

   For more information on additional parameters for Clickatell, refer to the Clickatell documentation.

   NOTE: The parameters may differ for different SMS service providers. But the `{phone}` and `{message}` variables are obligatory.

   ---
6. Click **Save** at the bottom of the view to save changes.

Authentication flow

The following chart demonstrates the authentication flow:

A user is authenticating on endpoint (which can be the user's laptop with Advanced Authentication Windows Client installed or a website etc.) by SMS method.

1. The endpoint calls the Advanced Authentication Server.
2. It validates the provided user's credentials and gets a phone number of the user from a used Repository.
3. Advanced Authentication Server sends the request to a configured SMS Service Provider to send an SMS message with generated content which includes a one-time password (OTP) for authentication.
4. SMS Service Provider sends the SMS message to the user's phone.
5. SMS Service Provider sends the 'sent' signal to the Advanced Authentication Server.
6. Advanced Authentication Server sends a request to enter an OTP on the endpoint side.
7. The user enters an OTP from the SMS message. The Advanced Authentication Server gets the OTP.
8. Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTP/HTTPS protocol is used for the communication.

Access configuration

Advanced Authentication Server - SMS Service Provider (HTTP/HTTPS, outbound).

8.7.19 Services Director Options

This policy allows you to integrate with the Services Director.

To enable the integration of Advanced Authentication with Services Director, turn **Enable integration** to **ON**.

Enter the **Public DNS name** of Advanced Authentication, **Services Director DNS Name, Tenant Admin Name** and **Tenant Admin Password** of Services Director to integrate it with Advanced Authentication.

NOTE: You cannot integrate Services Director with Advanced Authentication when Multitenancy is enabled.

8.7.20 Voice Sender

The **Voice sender** settings are located in the **Policies** section.

The section contains the Voice and Voice OTP method settings. It is used by Voice and Voice OTP. Advanced Authentication supports the Twilio service.

The following fields must be filled in **Twilio** section:

1. Account sid
2. Auth token
3. Sender phone
4. Public server url

The information regarding fields 1-3 you may get on the Twilio website. The **Public server url** must contain a public URL to where the Twilio service will connect for authentication. It's possible to use http protocol for testing purposes, but for production environment it's recommended to use https protocol. You need to have a valid certificate when using https.

The **Enroll without phone** section allows to configure behavior when a user is trying to enroll the Voice authenticator, but the user's repository data doesn't contain a phone number. If **Allow enroll user w/o phone** option is set to OFF such user will not be able to enroll the Voice authenticator and the user will get an error message, which can be specified in **Error message** field.

Click **Save** to apply the changes.

IMPORTANT: The users may get the calls with voice speaking `Application error`. It may happen because of not correct settings or invalid certificate. Ensure that the certificate is valid and not expired. Invalid certificate cannot be applied by Twilio.

Authentication flow

The following chart demonstrates the authentication flow:

A user is authenticating on endpoint (which can be the user's laptop with Advanced Authentication Windows Client installed or a website etc.) by SMS method.

1. The endpoint calls the Advanced Authentication Server.
2. It validates the provided user's credentials and gets a phone number of the user from a used Repository.
3. Advanced Authentication Server sends the request to a configured Voice Call Service Provider (Twilio) to call the user.
4. Voice Call Service Provider calls the user.
5. The user picks up the phone, listens to the answerphone and enters the PIN code followed by hash sign.
6. Voice Call Provider sends the entered PIN code to the Advanced Authentication Server.
7. Advanced Authentication Server validates the authentication. The authentication is done/ forbidden.

HTTP/HTTPS protocol is used for the communication.

Access configuration

Advanced Authentication Server - Voice Call Service Provider (HTTP/HTTPS, inbound/ outbound).

8.7.21 Geo fencing options

This policy allows you to create authentication zones by drawing boundaries for a geographical location. When you enable geo-fencing, users will be able to authenticate with Smartphone from only allowed geographical locations.

To enable geo-fencing, turn **Enable geo fencing** to **ON**.

NOTE: When you enable Geo-fencing, the functioning of the TOTP mode of the Smartphone method, which is used in the offline mode, is affected. An error message `TOTP login is disabled` is displayed to the users when they try to authenticate with this method.

8.7.22 Event categories

This policy allows you to add categories, which can be used in an event to support multiple enrollments for a method.

To add a category, click **Add** and then enter a name and description for the category. Click **Save** to save the category.

NOTE:

- It is possible to enroll only one authenticator of one type per category.
- The Categories functionality is disabled when no category is created.

8.7.23 SAML 2.0 options

This policy allows you to enter Identity Provider's URL and to download SAML 2.0 Metadata file. The downloaded SAML 2.0 Metadata file is used to configure the service provider.

IMPORTANT: WebAuth feature must be enabled in Server Options before configuring the policy.

Perform the following steps in SAML 2.0 options:

1. Enter the Identity Provider's URL, if required.
2. Click **Download IdP SAML 2.0 Metadata** to open the Metadata.

   IMPORTANT: At least one SAML 2.0 event must be created before downloading a metadata file in the policy.

   ---

3. The Metadata opens in a new browser page. Save the Metadata (XML text) from the browser.
4. Use the downloaded metadata file in your Service Provider, if required.

For information on how to configure Advanced Authentication integration with Salesforce using SAML2, see "Configuring Integration with Salesforce".

8.8 Configuring Server Options

Advanced Authentication Server uses an HTTPS protocol. You should create a certificate file (PEM or CRT or PFX) and apply the existing SSL certificate on the server.

NOTE: The certificate must not contain any of the encrypted private keys.

IMPORTANT: Smartphone and Voice Call authentication providers work only with valid SSL certificate, self-signed certificate will not work.

To specify the protocol that will be used by Advanced Authentication Server, follow the steps:

1. Open the **Server Options** section.
2. Click the **Choose File** button and select a new SSL certificate. The file must contain the both certificate and private key.

Intermediate certificates should also be placed in the certificate file (PEM or CRT or PFX), if they are present.

3. Click **Upload** to upload the selected SSL certificate.

NOTE: A valid connection to Certification Authority is required to apply the certificate.

It's possible to set a custom login page background. It should be a JPEG or PNG image, a recommended resolution is 1920x774 px, 72 dpi. It's not recommended to use backgrounds which size exceeds 100KB. To apply a custom login page background, follow the steps:

1. Click **Choose File** in **Login page background** section.
2. Select the background file.
3. Click **Upload** to upload and apply the custom background.

If you want to revert the settings to original click the **Revert to original** button.

8.8.1 Enabling Web Authentication

Strong Web Authentication is used for OAuth2 and SAML2 events. By default it is disabled to free some RAM. If you need to use OAuth2 or SAML, enable it.

To enable web authentication, perform the following steps:

1. Open the **Server Options** section.
2. Click **Enable** for **WebAuth** option.
3. Click **OK.**

NOTE: The changes done to **WebAuth** settings do not replicate to other servers.

8.8.2 Uploading Keytab File

The **Keytab file** option located in **Server Options** of Advanced Authentication - Administrative Portal allows you to upload a keytab file. The keytab file contains the encrypted files required for the Advanced Authentication Server to authenticate to the selected Active Directory using Kerberos.

Generate a keytab file for Kerberos authentication to the Advanced Authentication server on a Domain Controller. For information on generating a keytab file, see the website.

Sample command to create the keytab file: `ktpass /princ HTTP/aas1.netiq.loc@NETIQ.LOC /map user aas1srv@authasas.local /crypto ALL /ptype KRB5_NT_PRINCIPAL /mapop set /pass Q1w2e3r4 /out C:\Temp\keytab_aas1srv`

Some information about the sample command:

- HTTP in upper-case is mandatory in the parameter for keytab file. For more information, see the website.
- "aas1" is a server name (according to record in DNS), the domain name is "netiq.loc"
- "aas1srv" is a service account specially created in Active Directory for the Advanced Authentication Server, "Q1w2e3r4" is it's password.
- The keytab file "keytab_aas1srv" will be created in C:\Temp

IMPORTANT: If there are multiple Advanced Authentication Servers in the cluster, then generate a keytab file for each Advanced Authentication Server. Please note that different users must be used for the keytab file generation for each server.

Click **Upload** to select and upload the keytab file.

NOTE: Keytab file can be removed only when an Active Directory repository is selected in Kerberos SSO Options policy.

8.9 Adding a License

IMPORTANT: The temporary license is active for 30 days and will expire at the specified date. Authentication and access to the Advanced Authentication Authentication Methods Enrollment will be inaccessible when the license is expired. Please contact your seller in advance to get and apply a permanent license.

If you need more time to get a permanent license, before expiration of the temporary license log on by local admin to the Advanced Authentication Authentication Methods Enrollment to change the administrator's password. Otherwise in 42 days after the appliance deployment access to the appliance will be lost (Password).

To add the license for Advanced Authentication, follow the steps:

1. Open the **Licenses** section.
2. Click the **Choose File** button and select the valid license.
3. Click **Upload** to upload the license.

Advanced Authentication takes a user's license within a first authentication. It occurs also if a user is logging in to the Self-Service Portal for a first time or a security officer is logging in to manage the user's authenticators.

TIP: To free up a user's license, exclude the user from a group that is assigned to used chains. Then switch to **Repositories**, edit a used repository and click **Full sync** to perform a full synchronization of the repository. The existing user's authenticators are removed.

9 Configuring Default Ports for Advanced Authentication Server Appliance

IMPORTANT: Ports 443 and 80 are used inside the Advanced Authentication Server appliance and cannot be changed.

Port forwarding is supported but is not recommended. In this case the entire appliance will be available via the Internet. It is recommended to use reverse proxy to map only specific URLs.

Advanced Authentication Server Appliance uses the following RFC standard ports by default:

Service	Port	Protocol	Usage
REST	443	HTTPS	All Communications
Administrative portal, Self-Service portal, Helpdesk portal, Reporting 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: This port is required only for the installation of a new DB Server. Then the port must be closed.	TCP, UDP	Database replication between DB servers
Database replication	8080	TCP, UDP	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)

Advanced Authentication Server Appliance uses the following ports required 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
Swisscom Mobile ID	Variable	HTTPS	Communication to the specified Swisscom Mobile ID service URL
Voice OTP Service	Variable	HTTPS	All Communications (<AAServer>/twilio/otp)

IMPORTANT: Any port can be used in case of reverse proxying. E.g., https://dnsname:888/smartphone. There is reverse proxy redirect from port 888 to port 443 internally to appliance. Port 888 is used from outside, but port 443 is used inside the appliance.

10 Configuring a Cluster

This chapter contains the following sections:

- Section 10.1, “Registering a New Site,” on page 100
- Section 10.2, “Registering a New Server,” on page 101
- Section 10.3, “Resolving Conflicts,” on page 103
- Section 10.4, “How to Install a Load Balancer for Advanced Authentication Cluster,” on page 104
- Section 10.5, “Restoring Operability When a Global Master Server is Broken,” on page 107

The Advanced Authentication Server that is deployed first gets the Global Master and Server Registrar roles.

In a production environment, you must use more than one Advanced Authentication Server for fault tolerance, load balancing, and redundancy. To configure an Advanced Authentication Cluster, switch to the **Cluster** section in the Advanced Authentication Administrative Portal.

On the Advanced Authentication Server Registrar, a message `Replication not configured` is displayed along with the following text:

```
Click the button below to start new cluster. This server will then become the
Global Master. It will register new servers.
```

- `The cluster consists of Sites.`
- `Every site has DB Master, DB Server and Web Servers, located in same data center. The site is "web farm" or "server pool" in terms of load balancing.`
- `Global Master is first Master of first Site. There is one Global Master in the cluster. It manages all the sites.`

To configure the Global Master, perform the following steps:

1. Click **Set up Global Master**.
2. Specify the Global site name in **Enter name of the site. Renaming not supported**. The Global site name must be in lower case and can contain latin characters, digits, and underscores. Click **OK**.
3. A message `This server` block is displayed that contains the following information:

Mode:	**Global Master, <site name>**
Replication:	**replicating**
	Configured and running.
DB in use:	**127.0.0.1**
	Master connects to local DB always. DB Servers and Web Servers connect to Master DB. They connect to DB Server when Master is not accessible
DB available:	<Registrar_host_name> (Global Master)

Below the block, a table **DB servers** table is displayed with only one server (Global Master). For each server in the list, the following information is displayed:

- Site name
- Mode (Global Master, DB Master, DB Server-1, DB Server-2)
- Host name
- Description. Click edit icon to add or edit the description.
- Heartbeat. Each server is pinged for every 5 minutes. The time of the last ping is displayed.

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/remove servers in the cluster.

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

To view the list of all the servers including Global Master, DB servers and Web Servers, click **All servers**. For each server in the list, the following information is displayed:

- Mode (Global Master, DB Server, Web Server)
- Host name
- Comments. Click edit icon to add or edit the comment.

If your company is geographically distributed and you want to deploy the Advanced Authentication Servers to every site, click Registering a New Site.

If you want to register a new server in one of the existing sites, click Registering a New Server.

If you have already configured a cluster and you are receive a replication conflict, click Resolving Conflicts.

10.1 Registering a New Site

To register a new site and deploy a DB Master server in the site, perform the following steps:

1. Ensure that you have administrator privileges to access the Advanced Authentication Server Registrar and you have installed but not configured an Advanced Authentication server appliance for a DB Server in the new site.
2. Open the database port `<Registrar_host_name>:5432` on your NAT/Firewall.
3. Open the Advanced Authentication Configuration Wizard for a new installed server: https://<New_Server_host_name>.
4. In the first **Server Mode** step of the Configuration Wizard, select **Existing cluster**. Click **Next.**
5. In the **DNS hostname** step, specify the server DNS hostname in **My DNS hostname**. Click **Next**.

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

   ---

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

7. In the **Import database information** step, a message `Waiting for Global Master....` is displayed.
8. Switch to the Advanced Authentication - Administrative Portal of the Advanced Authentication Server Registrar and in the **Cluster** section, click **Register new site**.
9. In the **Register new site** window, specify a host name for the new DB Server in the new site in **Master server host**.

   TIP: If the new server is behind NAT, you can forward its port 443 on a temporary basis and enter external hostname:port. Do not forget to close the port after installation.

10. Specify a name of the new site in **Site name**.
11. Click **Register**.
12. After successfully registering, a message `Success! Continue server install` is displayed. In the DB servers list, DB Master server for the newly created site is displayed. The record is marked by red and `Waiting this node to contact me` is displayed in its description.
13. Switch to the new server and click **Next**.
14. In the **Copy database** step click **Copy**.
15. Wait until the database is copying from a Global Master server. The server is automatically restarted within 60 seconds once the copying is completes.
16. Switch to the Advanced Authentication Server Registrar. The newly deployed server is displayed in the DB servers list and may appear in red within 5 minutes after installation.

    NOTE: Each of the DB servers in the list are pinged for every 5 minutes. In the case of an issue, the server is marked by red in the list and you can get the details of connectivity issues by clicking **View log** and replication issues by clicking **Conflicts**.

17. Close the database port `<Registrar_host_name>:5432` on your NAT/Firewall.

    NOTE: You must install the new servers one at a time. Simultaneous installations may cause replication issues.

    The inter-site replication interval is 10 seconds.

    NOTE: It is possible to specify different LDAP servers in Repository configuration on Advanced Authentication servers of different sites.

    All changes are replicated only inside a site.

10.2 Registering a New Server

To deploy a new DB Server or a Web Server in an existing site, perform the following steps:

1. Ensure that you have administrator's privileges to access the Advanced Authentication Server Registrar and you have installed but not configured the Advanced Authentication server appliance for a new server.
2. Open the database port `<Registrar_host_name>:5432` on your NAT/Firewall if you are deploying a DB Server.
3. Open the Advanced Authentication Configuration Wizard for a new installed server: https://<New_Server_host_name>.
4. In the first **Server Mode** step of the Configuration Wizard, select **Existing cluster**. Click **Next**.

5. In the **DNS hostname** step, specify the server DNS hostname in **My DNS hostname**. Click **Next**.

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

---

6. Specify a password for the LOCAL\admin account and click **Next** on the **Password** screen.
7. In the **Import database information** step, a message `Waiting for Global Master....` is displayed.
8. Switch to the Advanced Authentication - Administrative Portal of the Advanced Authentication Server Registrar and in the **Cluster** section, click **Register new site**.
9. In the **Register new server** window, specify the new server's host name in **Server host**.

TIP: If the new server is behind NAT, you can forward its port 443 on a temporary basis and enter external hostname:port. Do not forget to close the port after installation.

---

10. Select one of the following servers:
    - **Web Server:** It does not contain a database. It responds to authentication requests and connects to the DB Master database. You need more Web Servers to serve more workload.
    - **DB Server**: It provides a DB Slave database that is used for backup and fail-over. Two DB Slave servers are allowed within the site. When the DB Master is unavailable, the DB Slave node responds to the database requests. When the DB Master becomes available again, the DB Slave node synchronizes with the DB Master and the DB Master becomes the primary point of contact for database requests again.

NOTE: If you have selected the DB Server, you must copy database from Global Master. Open database port `<Registrar_host_name>:5432` on your NAT/Firewall. Do not forget to close the port after installation.

---

11. Select the site to which you want to add the new server from the **Add server to the site** drop-down menu.
12. Click **Register**.
13. Switch to the new server and click **Next**.
14. If you have selected the DB Server, in the **Copy database** step click **Copy**. Wait until the database is copying from a Global Master server.
15. The server is automatically restarted within 60 seconds when the copying completes.
16. If you have selected the DB Server, switch to Advanced Authentication Server Registrar. The newly deployed server is displayed in the DB servers list. The newly deployed server is displayed in the DB servers list and may appear in red within 5 minutes after installation.

NOTE: Each of the DB servers in the list are pinged for every 5 minutes. In the case of an issue, the server is marked as red in the list and you can get the details of connectivity issues by clicking **View log** and replication issues by clicking **Conflicts**.

---

17. Close the database port `<Registrar_host_name>:5432` on your NAT/Firewall if you opened it.

NOTE: You must install the new servers one at a time. Simultaneous installations may cause replication issues.

10.3 Resolving Conflicts

If a conflict occurs, then the replication between conflicting servers stops. Replication uses "last-write-wins" policy. Conflict can occur for one of the following reasons:

- During upgrade: when a new server communicates with the old server.
- When two unique objects have been added.

Outgoing conflict indicates an incoming conflict on the destination server. Unique object collision causes two corresponding conflicts: incoming and outgoing on both the source and target servers.

An example of a collision: MasterX and MasterY create a same login chain 'Visitor'. This can lead to a conflict because both try to send ‘Visitor’ to each other.

You can resolve the conflict with one of the following ways:

Simplest way: `two fixes remove two objects`:

- Remove Visitor chain on both the servers: Press "Fix incoming" on both.
- "Forget outgoing" on both the servers.
- Use INSERT conflicts. You must be careful of "fixing" UPDATE conflict. You could have renamed two different objects to the same name. It is better to rename them and forget conflicts on both servers and avoid fixing them.

Smarter way: `fix one, forget another`:

- Remove Visitor on MasterY: Press "Fix incoming"
- "Forget outgoing" on MasterY. It does not retry to send conflicting Visitor anymore.
- "Forget incoming" on MasterX.
- Wait for half a minute. MasterY accepts outgoing Visitor from MasterX.

Possible way: `two outgoing forgets - two independent objects`:

Use for UPDATE conflicts. Object changes will be lost but will sync on next object change.

Zero way: `two incoming forgets`:

Do nothing. Source server re-sends the changes until you forget the outgoing conflict.

Purge working tables: This is last resort. If you see low-level errors in replication log, if conflict resolution does not work for you, then you may force replication system to forget all pending replicas and re-initialize.

The server will stay out-of-sync. Eventually it will normalize - changes will replicate and overwrite each other. If you feel some administrative option is wrong (such as Event definition), go to server where the option is "right" and press Save in option editor. Thus, re-saving an object re-replicates it to all servers.

Advanced Authentication scans for the replication conflicts, automatically. To resolve existing conflicts, in the **Cluster** section of the Advanced Authentication Server Registrar, click **Conflicts** above the DB servers list. If no conflicts are detected, only the information is displayed. If there are any conflicts, the details and controls to resolve the conflicts are displayed. You will get a confirmation request with each action. The confirmation contains notes that help you to resolve the conflicts.

10.4 How to Install a Load Balancer for Advanced Authentication Cluster

You can install a Load balancer and configure it through a third party software. The following example guides you on how to install and configure nginx as a load balancer on Ubuntu 16.04.

NOTE: Advanced Authentication supports DNS round-robin and third party VIP, but only with Sticky sessions. In this case, DNS Discovery mechanism is excluded from the workflow. Advanced Authentication clients are pointed to a Load balancer that manages all traffic.

Target configuration:

	Hostname	IP address	Role	Operation System
Domain controller	win-dc.utopia.locl	192.168.1.56	AD DS, DNS	Windows Server 2012 R2
Advanced Authentication 5.5	aaf-clu-gm.utopia.locl	192.168.1.70	Global Master	Advanced Authentication 5.5
Advanced Authentication 5.5	aaf-clu-gs.utopia.locl	192.168.1.71	Slave	Advanced Authentication 5.5
Load balancer	llb.utopia.locl	192.168.1.138	Nginx load balancer	Ubuntu 16.04
Client	windows7v5.utopia.locl	192.168.1.61	AA Client	Windows 7 x64

Before you start the configuration, ensure that the following requirements are met:

- Repository is configured in Advanced Authentication appliance.
- Both Advanced Authentication servers are installed and configured as Master and Slave.
- Appropriate entries are added to DNS.
- Ubuntu 16.04 is installed.

10.4.1 Installing nginx on Ubuntu 16.04

1. Update repository and install nginx:
   - **1a** apt-get update
   - **1b** apt-get install nginx
2. Start nginx and make sure that web server is working:
   - **2a** sudo service nginx restart
3. Open your browser and go to web server http://192.168.1.138.

10.4.2 Configuring nginx

The following load balancing mechanisms/methods are supported in nginx:

- **round-robin** - requests to the application servers that are distributed in a round-robin fashion

- **least-connected** - next request assigned to the server with the least number of active connections
- **ip-hash** - a hash-function that is used to determine what server should be selected for the next request (based on the client's IP address)

This article describes the ip-hash configuration because the REST queries that are balancing require sticky-session enabled and ip-hash is a similar mechanism. To configure nginx, perform the following steps:

1. Backup original configuration file: `sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf_original`.
2. Copy the certificate from any Advanced Authentication server in a cluster from the directory `/etc/nginx/cert.pem` to the same directory on load balancer.
3. Open the `nginx.conf` file and replace with following:

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;

events {
  worker_connections 768;
# multi_accept on;
}

http {

  ##
# Basic Settings
  ##

sendfile on;
  #tcp_nopush on;
#tcp_nodelay on;
  keepalive_timeout 65;
types_hash_max_size 2048;
  # server_tokens off;

# server_names_hash_bucket_size 64;
  # server_name_in_redirect off;

#include /etc/nginx/mime.types;
  #default_type application/octet-stream;

##
  # SSL Settings
##

  ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # Dropping SSLv3, ref: POODLE
ssl_prefer_server_ciphers on;
  ssl_certificate /etc/nginx/cert.pem;
ssl_certificate_key /etc/nginx/cert.pem;

  ##
# Logging Settings
  ##

access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;
```

```
##
  # Gzip Settings
##

  gzip on;
gzip_disable "msie6";
  gzip_vary on;
gzip_proxied any;
  gzip_comp_level 6;
gzip_buffers 16 8k;
  gzip_http_version 1.1;
gzip_types text/plain text/css application/json application/javascript text/
xml application/xml application/xml+rss text/javascript;

##
  # Virtual Host Configs
##

  include /etc/nginx/conf.d/*.conf;
include /etc/nginx/sites-enabled/*;
  resolver 192.168.1.56 valid=300s ipv6=off; # ip address of DNS
resolver_timeout 10s;
  upstream aaf-clu {
ip_hash; # Type of load balancing mechanism
      server aaf-clu-gm.utopia.locl:443 #192.168.1.70:443;
server aaf-clu-gs.utopia.locl:443 #192.168.1.71:443;
    }

server {
          listen 443 ssl;
        # Rule for REST
          location ~ ^/api/v1 {
  proxy_set_header X-Real-IP $remote_addr;
                  proxy_set_header X-Forwarded-Server $host;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                  proxy_set_header Host $host;
                proxy_pass https://aaf-clu$uri?$args;
              }
location ~ ^/admin {
            proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-Server $host;
                  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header Host $host;
                  proxy_pass https://aaf-clu$uri?$args;
            }
            location ~ ^/static {
proxy_set_header X-Real-IP $remote_addr;
          proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
          proxy_set_header Host $host;
proxy_pass https://aaf-clu$uri?$args;
        }
location ~ ^/helpdesk {
          proxy_set_header X-Real-IP $remote_addr;
```

```
proxy_set_header X-Forwarded-Server $host;
          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
          proxy_pass https://aaf-clu$uri?$args;
}
      location ~ ^/enroll {
proxy_set_header X-Real-IP $remote_addr;
          proxy_set_header X-Forwarded-Server $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
          proxy_set_header Host $host;
proxy_pass https://aaf-clu$uri?$args;
        }
}
}
```

This configuration file allows to balance REST, administration, and Self-Service portal requests.

10.4.3 Configuring Advanced Authentication Client

To point the Advanced Authentication client to a Load balancer, you need to make some changes after installing the client on a workstation:

1. Install Windows Client. To install Windows Client, see the section "Installing Windows Client" in the *Advanced Authentication - Windows Client* guide.
2. Open the configuration file: `C:\ProgramData\NetIQ\Windows Client\config.properties`.
3. Set the parameter `discovery.host = <IP_address/hostname_loadbalancer>`.

   This configuration points Advanced Authentication Client to a Load balancer that manages the traffic between the Advanced Authentication server and Advanced Authentication Client (REST API).

10.5 Restoring Operability When a Global Master Server is Broken

When a GMS (Global Master Server) is broken, try to restore it from backup or a snapshot. If this does not work, perform the following steps to convert an existing DB server from the same site as GMS to a new GMS and then deploy a new DB server.

1. Ensure that GMS is turned off.
2. Open Advanced Authentication Administrative Portal on the DB server.
3. Browse the **Cluster** section.

   A message is displayed: `Please wait. Configuration/loading in progress… Maximum loading time is 5 minutes. Usually it takes 40-60 seconds.`
4. Wait until you see the **Cluster** section updated.

   GMS is displayed in red as a list of servers after more than 15 minutes of unavailability.
5. Click **Failover**.
6. Open database port 5432 (TCP/UDP) on your NAT/Firewall for a time of conversion.
7. Click **Convert to Global Master**.
8. Click **OK**.

   Wait a few minutes while Advanced Authentication is performing the conversion.

9 When you again see the **Cluster** section, close the database port.

10 If you have been using RADIUS server, those settings need to be reconfigured. In the Advanced Authentication Administrative Portal, switch to **Events** and edit the **Radius Server** event. Check the configuration including the **Clients** section and click **Save** to reconfigure the RADIUS server.

11 Update DNS so that the DNS name of lost GMS resolves the IP address of the server being converted.

IMPORTANT: Do not change the IP addresses of working servers.

---

12 Update the Load Balancer configuration if required.

13 Install a new server with an `ISO` file of the same version as on the new GMS and configure a new DB server instead of the converted one.

14 Login to the Administrative Portal on Web servers. If you are not able to do it, try to reboot the Web servers. If you are still unable to login to Administrative Portal on Web servers, redeploy the Web servers.

11 Authentication Methods Enrollment

Advanced Authentication Server supports the following ways to enroll the authentication methods:

- **Automatic enrollment** which is supported for **SMS**, **Email**, **RADIUS**, **LDAP Password**, and **Swisscom Mobile ID** methods.

  The methods will be enrolled automatically if Chains containing them are assigned to any Event.

- **Enrollment by Administrator** is supported for **OATH Tokens**.

  An administrator can import tokens from PSKC or CSV files in Advanced Authentication **Administrative Portal** - **Methods** - **OATH OTP** - **OATH Tokens** tab. From the same view it's possible to assign tokens to the specific users.

- **Enrollment by Security Officer**

  A Helpdesk/Security officer can access the Advanced Authentication **Helpdesk Portal** by the following address: https://<NetIQ Server>/helpdesk where it's possible to enroll the authentication methods for users. A Helpdesk/Security officer must be a member of **Enroll Admins** group (**Repositories** - click **Edit** on **LOCAL** - **Global Roles** tab) to perform management of users' authenticators.

- **Enrollment by User**

  A user can access the Advanced Authentication **Self-Service Portal** by the following address: https://<NetIQ Server>/account where it's possible to enroll any of permitted authentication methods.

12 Configuring Integrations

- Section 12.1, “Configuring Integration with Barracuda SSL VPN,” on page 111
- Section 12.2, “Configuring Integration with Citrix NetScaler,” on page 113
- Section 12.3, “Configuring Integration with Dell SonicWall SRA EX-Virtual appliance,” on page 114
- Section 12.4, “Configuring Integration with FortiGate,” on page 116
- Section 12.5, “Configuring Integration with OpenVPN,” on page 117
- Section 12.6, “Configuring Integration with Salesforce,” on page 119
- Section 12.7, “Configuring Integration with NetIQ Access Manager (SAML),” on page 121

12.1 Configuring Integration with Barracuda SSL VPN

These instructions will help you to configure integration of Advanced Authentication Appliance Edition with the Barracuda SSL VPN virtual appliance to refuse non-secure passwords in Barracuda SSL VPN connection.

The advanced authentication in Barracuda SSL VPN is represented on the following diagram.

To get started, ensure that you have:

- Barracuda SSL VPN appliance v380 or above (Firmware version 2.6.1.7 was used to prepare these instructions)
- Advanced Authentication v5 appliance with the already configured repository

Configure the Advanced Authentication RADIUS server:

1. Open the Advanced Authentication Admin Interface.
2. Go to the **Events** section.
3. Open properties of the **Radius Server** event.
4. Set the **Radius Server** event to the **ON** mode.
5. Select one or more chains from the list of **Used** chains (make sure that they are enabled and set to the users group in the **Chains** section).
6. Add a **Client**, enter an IP address of the Barracuda SSL VPN appliance, specify a secret, confirm it and set the **Enabled** option.
7. Click the **Save** button in the **Client** string. Click the **Save** button at the bottom of the **Events** view to save changes.

Configure the Barracuda SSL VPN appliance:

1. Sign-in to the Barracuda SSL VPN Configuration portal as **ssladmin**.
2. Browse menu **Access Control -> Configuration**.

3. Scroll down to **RADIUS** section.
4. Enter Advanced Authentication appliance IP address in the **RADIUS Server** text field.
5. Specify a shared secret in the **Shared Secret** text field.
6. Set **Authentication Method** to **PAP**.
7. Set **Reject Challenge** to **No** to allow challenge response.
8. Click **Save Changes**.
9. Switch to **Access Control -> User Databases**.
10. Create User Database using the same storage as you are using in the Advanced Authentication.
11. Switch to **Access Control - Authentication Schemes**.
12. In the bottom of the view, click **Edit** in front of **Password** scheme for the added User Database.
13. Move **RADIUS** from **Available modules** to **Selected modules**.
14. Remove the **Password** module from the **Selected modules**.
15. Apply the changes.

How to authenticate in Barracuda SSL VPN using the Advanced Authentication:

1. Enter user's credentials.
2. Click **More** and select the configured User Database (if the database is not selected by default).
3. Click **Log In** and approve the authentication on the user's smartphone.

NOTE: Advanced authentication can be configured with other authentication chains.

12.2 Configuring Integration with Citrix NetScaler

These instructions will help you to configure integration of Advanced Authentication Appliance Edition with the Citrix NetScaler VPX to refuse non-secure passwords.

The advanced authentication in Citrix NetScaler is represented on the following diagram.

To get started, ensure that you have:

- Citrix NetScaler VPX (version NS11.0 was used to prepare these instructions)
- Advanced Authentication v5 appliance

Configure the Advanced Authentication RADIUS server:

1. Open the Advanced Authentication Admin Interface.
2. Go to the **Events** section.
3. Open properties of the **Radius Server** event.
4. Set the **Radius Server** event to the **ON** mode.
5. Select one or more chains from the list of **Used** chains (make sure that they are enabled and set to the users group in the **Chains** section).
6. Add a **Client**, enter an IP address of the Citrix NetScaler VPX, specify a secret, confirm it and set the **Enabled** option.
7. Click the **Save** button in the **Client** string. Click the **Save** button at the bottom of the **Events** view to save changes.

Configure the Citrix NetScaler appliance:

1. Sign-in to the Citrix NetScaler configuration portal as **nsroot**.
2. Browse menu **Configuration -> Authentication -> Dashboard**.
3. Click **Add**.
4. Select **RADIUS** from the **Choose Server Type** dropdown menu.

5. Specify the **Name** of the Advanced Authentication server, its **IP Address**, **Secret Key** and **Confirm Secret Key**, change **Time-out (seconds)** to 120-180 seconds in case of usage of the Smartphone, SMS, Email or Voice methods.
6. Click **More** and ensure that **pap** is selected in the **Password Encoding** dropdown menu.
7. Click **Create**. If connection to the RADIUS server is valid, the **Up** status will be displayed.
8. Browse menu **Configuration -> System -> Authentication -> RADIUS -> Policy**.
9. Click **Add**.
10. Specify the **Name** of the Authentication RADIUS Policy, select the created RADIUS server from the **Server** dropdown menu, select **ns_true** from the **Saved Policy Expressions** list.
11. Click **Create**.
12. Select the created policy and click **Global Bindings**.
13. Click the **Select Policy** field.
14. Select the created policy.
15. Click **Bind**.
16. Click **Done**. The check mark will be displayed in the **Globally Bound** column.

How to authenticate in Citrix NetScaler using the Advanced Authentication:

1. Enter user's credentials and click **Login**.
2. Accept authentication on your smartphone.

NOTE: Advanced authentication can be configured with other authentication chains.

12.3 Configuring Integration with Dell SonicWall SRA EX-Virtual appliance

These instructions will help you to configure integration of Advanced Authentication Appliance Edition with the Dell SonicWall SRA EX-Virtual appliance to refuse non-secure passwords in Dell SonicWall SRA connection.

The advanced authentication in Dell SonicWall is represented on the following diagram.

To get started, ensure that you have:

- Dell SonicWall SRA EX-Virtual appliance v11.2.0-258
- Advanced Authentication v5 appliance

Configure the Advanced Authentication RADIUS server:

1. Open the Advanced Authentication Admin Interface.
2. Go to the **Events** section.
3. Open properties of the **Radius Server** event.
4. Set the **Radius Server** event to the **ON** mode.
5. Select one or more chains from the list of **Used** chains (make sure that they are enabled and set to the users group in the **Chains** section).
6. Add a **Client**, enter an IP address of the Dell SonicWall SRA appliance, specify a secret, confirm it and set the **Enabled** option.
7. Click the **Save** button in the **Client** string. Click the **Save** button at the bottom of the **Events** view to save changes.

Configure the Dell SonicWall SRA appliance:

1. Sign-in to the Dell SonicWall SRA Management Console as **admin**.
2. Browse menu **User Access -> Realms**.
3. Create **New realm**.
4. Create a **New Authentication Server**, set the **Radius** authentication directory.
5. Set **Radius Server** and **Shared key**.
6. Save and apply configuration.
7. Browse menu **User Access -> Realms**. Review realm diagram.

How to authenticate in Dell SonicWall workspace using the Advanced Authentication:

1. Open browser and go to workplace. Enter your username and ldap password.

2. Enter **SMS OTP** and click **OK**.
3. You are successfully logged in to the workplace.

12.4 Configuring Integration with FortiGate

These instructions will help you to configure integration of Advanced Authentication Appliance Edition with the Fortinet FortiGate to refuse non-secure passwords.

The advanced authentication in Fortinet FortiGate is represented on the following diagram.

To get started, ensure that you have:

- Fortinet FortiGate virtual appliance v5 (Firmware version 5.2.5, build 8542 was used to prepare these instructions)
- Advanced Authentication v5 appliance

Configure the Advanced Authentication RADIUS server:

1. Open the Advanced Authentication Administrative Portal.
2. Go to the **Events** section.
3. Open properties of the **Radius Server** event.
4. Set the **Radius Server** event to the **ON** mode.
5. Select one or more chains from the list of **Used** chains (make sure that they are enabled and set to the users group in the **Chains** section).

6. Add a **Client**, enter an IP address of the FortiGate appliance, specify a secret, confirm it and set the **Enabled** option.
7. Click the **Save** button in the **Client** string. Click the **Save** button at the bottom of the **Events** view to save changes.

Configure the FortiGate appliance:

1. Sign-in to FortiGate configuration portal as admin.
2. Check which Virtual Domain bound to the network interface.
3. Open Radius Server configuration for an appropriate Virtual Domain and setup required settings.
4. Click **Test Connectivity** button, enter credentials of Advanced Authentication Framework administrator to test the connection.
5. Create a user group and bind it to remote authentication server.
6. Create user and place is in the created group.

How to authenticate in FortiGate using the Advanced Authentication:

1. Enter user's credentials and click **Login**.
2. Enter OTP and click **Login**.

NOTE: The Token Code field has a 16 digits limitation, so you may get problems when using the YubiKey tokens which enters 18-20 digits code.

12.5 Configuring Integration with OpenVPN

These instructions will help you to configure integration of Advanced Authentication Appliance Edition with the OpenVPN virtual appliance to refuse non-secure passwords in OpenVPN connection.

The advanced authentication in OpenVPN is represented on the following diagram.

To get started, ensure that you have:

- OpenVPN v2 appliance (version 2.0.10 was used to prepare these instructions)
- Advanced Authentication v5 appliance with the already configured repository

Configure the Advanced Authentication RADIUS server:

1. Open the Advanced Authentication Admin Interface.
2. Go to the **Events** section.
3. Open properties of the **Radius Server** event.
4. Set the **Radius Server** event to the **ON** mode.
5. Select one or more chains from the list of **Used** chains (make sure that they are enabled and set to the users group in the **Chains** section).
6. Add a **Client**, enter an IP address of the OpenVPN appliance, specify a secret, confirm it and set the **Enabled** option.
7. Click the **Save** button in the **Client** string. Click the **Save** button at the bottom of the **Events** view to save changes.

Configure the OpenVPN appliance:

1. Open the **OpenVPN Access Server** site.
2. Go to the **Authentication** - **RADIUS** section.
3. Enable the **RADIUS** authentication.
4. Select **PAP** authentication method.
5. Add an IP address of the Advanced Authentication v5 appliance and enter the secret.

If you have one **Used** chain selected in the **Radius Server** settings, to connect to OpenVPN, please enter the <repository name>\<username> or only <username> if you have set the default repo name in **Policies - Login options** section of the Advanced Authentication v5 appliance.

If you have multiple **Used** chains selected, to connect to OpenVPN, in the username field after the entered <username> and space you need to enter a **Short name** of the necessary chain (the **Short name** can be selected in **Chains** section of the Advanced Authentication v5 appliance).

Please note that some of the available authentication methods require correct time on the OpenVPN appliance. You can sync the time of the OpenVPN appliance using the following commands:

```
/etc/init.d/ntp stop
```

```
/usr/sbin/ntpdate pool.ntp.org
```

12.5.1 User Account Locks After Three Successful Authentications with SMS AP to OpenVPN

Issue Description:

We are using SMS authentication method to connect to OpenVPN. But after 3 successful authentications the user account was locked by OpenVPN.

Solution:

This problem is not related to Advanced Authentication. OpenVPN supposes each attempt of challenge response (request of additional data in chain) as an error.

The solution is to change acceptable number of failures. Check the Authentication failure lockout policy article for more information.

12.6 Configuring Integration with Salesforce

Perform the following steps to configure the integration of Advanced Authentication appliance with Salesforce using SAML2:

1. Login to your Salesforce account.
2. Create a domain, if not created.
   a. In Lightning Experience interface click the Gear button and select **Setup Home**.
   b. Scroll down the Setup toolbar and navigate to **Company Settings.**
   c. Click **My Domain.**

      Enter your own domain name and then click **Save.** The domain will be activated. Use your domain name to open Salesforce. For example, https://CompanyName.my.salesforce.com/

      SAML provider requires the domain name.
3. Configure SAML provider.
   a. From the Settings menu navigate to **Identity** > **Single Sign-On Settings.**
   b. Create a new text file and add the Identity Provider Certificate to it.


```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIESsmdMzANBgkqhkiG9w0BAQsFADB6MRAwDgYDVQQGEwdVbmtub3duMR
Aw
DgYDVQQIEwdVbmtub3duMRAwDgYDVQQHEwdVbmtub3duMREwDwYDVQQKEwhBdXRoYXNhczESMB
AG
A1UECxMJQXV0aGFzYXNhMRswGQYDVQQDExJvc3AuYXV0aGFzYXMubG9jYWwwHhcNMTYwNTI2MD
Uz
NjI0WhcNMjYwNDA0MDUzNjI0WjB6MRAwDgYDVQQGEwdVbmtub3duMRAwDgYDVQQIEwdVbmtub3
du
MRAwDgYDVQQHEwdVbmtub3duMREwDwYDVQQKEwhBdXRoYXNhczESMBAGA1UECxMJQXV0aGFzYX
Nh
MRswGQYDVQQDExJvc3AuYXV0aGFzYXMubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwgg
EK
AoIBAQCw3YLz03qhSZPXjBc/Ws+cZ2/
E5oogqKeJ3p4RR6USOoarjnmvQPq+maRfvexriwQjRDgS
OFRb58cert/
misqzsHBVmQDnfMwicFVzuuKjDEbWFp9vL1gRkDzIlpCyl3eNmBWuWXM49Z6mm8XS
fIwlAoydNp5DK0o0Yrk6FNOi0nOrnI5kHGVD0bd5SpDtvXSF1WLfc5YT9UBUpfZneKsVPWSkbe
BX
F84hYJWBtdzcTEyjdso9Ra7UtxLIUW0UH3LWTgn9zS97nLkmhetmD1I3mEAeAE9SAmqTRyH1FN
XZ
```

```
ZOfi/
BJF4+sz86f6pBbwYM2KTvXaABgzSpZpJ1pQrZKPAgMBAAGjITAfMB0GA1UdDgQWBBTL8PbA
+e6YkBIk4yELTZ+AbfdA6DANBgkqhkiG9w0BAQsFAAOCAQEAm87lNyAO8CtN5jlLe3CupLAAbU
WR
NY6av7LpPail1JRIw+uvddMyOz1vOS1IwpDDNtcPtxGXsaZI1CKgNPBpLvSxePVUXNfFgUCtu+
bT
cuUtiQbkiDWwFLmAS6KeA+EBFOeqBiudEfkAZZT87DF9gKvM6VWdzJ7BvWi2YPbH/
FRM82fLoyAd
RbphF215we3rvsfeWbwXw70UGNyBUTb3zUcAmB3sHbcZiXJZj3pJYgDaN9Ss60sz/
yG1ZLEYluvL
R1T2PPEfEcA1Eij0R1A31Z5hJ3zDlXoCeNYLoMg4522QYekTwvQeWkeYejBXEcxdL7VP6F91zm
fZ
bm1A4PY5jw==
-----END CERTIFICATE-----
```


c. In the **Single Sign-On Settings** screen, click **New** and enter the required details.

   i. Name: Advanced Authentication

   ii. API Name: AAF

   iii. Issuer: https://AdvancedAuthenticationServerAddress/osp/a/TOP/auth/saml2/metadata, where replace AdvancedAuthenticationServerAddress with domain name or IP address of your Advanced Authentication Server.

   iv. Entity ID: https://CompanyName.my.salesforce.com/

   v. Click **Choose File** to open the Identity Provider Certificate.

   vi. SAML Identity Type: Select **Assertion contains the Federation ID from the User object** option.

   vii. SAML Identity Location: Select **Identity is in an Attribute element** option.

   viii. Attribute Name: upn.

   ix. Service Provider Initiated Request Binding: Select **HTTP Redirect** option.

   x. Identity Provider Login URL: https://AdvancedAuthenticationServerAddress/osp/a/TOP/auth/saml2/sso

   xi. Select **User Provisioning Enabled** option.

   xii. Click **Save.**

d. Click **Edit** for Federated Single Sign-On Using SAML.

e. Select **SAML Enabled** option.

f. Click **Save.**

g. From the Settings menu click **Users.**

h. Click **Edit** for the required Salesforce users by adding **Federation ID** for the user accounts. The Federation ID corresponds to `userPrincipalName` attribute in Active Directory. For example, pjones@company.com.

NOTE: The name that you specify in **Federation ID** is case sensitive. The following error may occur, if you ignore the case:

```
We can't log you in. Check for an invalid assertion in the SAML Assertion
Validator (available in Single-Sign On Settings) or check the login history
for failed logins.
```

---

i. Click your profile icon and then click **Switch to Salesforce Classic** option. This mode is required to tune domain options.

j. Click **Setup** from the top menu and navigate to **Administrator** > **Domain Management** > **My Domain** and then click **Edit** to access **Authentication Configuration** screen.

k. Select **Login Page** and **osp** options and then click **Save.**

4. Configure Advanced Authentication SAML Event.

   a. Click username and then click **Switch to Lightning Experience.**

   b. Click the gear button and select **Setup Home**.

   c. Navigate to **Identity** - **Single Sign-On Settings**.

   d. Click the created configuration (not for Edit).

   e. Click **Download Metadata.**

   f. Open **Advanced Authentication** > **Administrative Portal**.

   g. Switch to **Server Options**.

   h. Enable WebAuth.

   i. Switch to **Events** section.

   j. Click **Add** to add a new event.

   k. Create an event with the following parameters.

      Name: Salesforce

      Chains: select the required chains.

      Click **Choose File** to Upload SP SAML 2.0 metadata file. Open the Salesforce metadata file and then click **Save.**

5. Switch to **Policies** section.

6. Set External URL to https://AdvancedAuthenticationServerAddress/ and replace AdvancedAuthenticationServerAddress with domain name or IP address of your Advanced Authentication Server.

   IMPORTANT: The server name or IP address used in Issuer field in Salesforce has to be used.

7. Open your URL https://CompanyName.my.salesforce.com/ and click Advanced Authentication to check the SAML2 authentication.

12.7 Configuring Integration with NetIQ Access Manager (SAML)

The following video describes how to integrate Advanced Authentication with NetIQ Access Manager using SAML.

http://www.youtube.com/watch?v=qA7kZQht7Oc

III Maintaining Advanced Authentication

This section is intended for system administrators and contains information about maintenance of environment which contains the solution.

To restart the Advanced Authentication Server appliance open the Advanced Authentication Administrative Portal and use a menu of top right corner. Right click the user name and click **Reboot**.

Using the **Profile** menu item you can also switch to the Self-Service Portal. To log out from the Administrative Portal use the **Log Out** button.

This chapter contains the following sections:

- Chapter 13, “Reporting,” on page 125
- Chapter 14, “Logging,” on page 127
- Chapter 15, “Troubleshooting,” on page 139

13 Reporting

The Advanced Authentication provides a reporting functionality. To log in to the Advanced Authentication Reporting Portal, open the following address: https://<NetIQServer>/report and sign-in using your account.

NOTE: It is required to assign chains to the **Report logon** event in the **Events** section.

The following data is displayed:

Failed authentications per event

- Logon failed per event - 1
- Logon failed per event - 2
- Logon failed (total)
- Events failed
- Logon failed per user for the top 25 failed users in the **AuCore stats 2** dashboard

Successful authentications per event

- Logon succeeded per repo
- Events succeeded
- Logon succeeded per user for the top 25 successful users in the **AuCore stats 2** dashboard

List of endpoints connecting to an event

- Endpoints activity for the top 50 most active in the **AuCore stats 2** dashboard

System

- CPU load in the AuCore stats 3 dashboard
- Memory load in the AuCore stats 3 dashboard

You can select **Last N minutes** in the top-right corner to change the period of the report. To switch dashboard, click **Load saved dashboard** icon in the toolbar and select a required dashboard.

FULL ADMINS can view the reports from all tenants. To view the reports of a specific tenant, you must login to the Reporting portal as the tenant admin.

14 Logging

The **Logs** section contains the following logs:

- System log
- Web server log
- RADIUS Server log
- Replication log
- Superuser commands
- Background tasks log

NOTE: A tenant administrator will not have access to Web server log, Replication log, Superuser commands and Background tasks log.

The System log contains the following information events:

Code	Name	Class	Severity	Optional Parameters	Example
1	New Request	Operational	1	None	June 10 20:10:11 host CEF:0|AAA|Core|5.0|1|New Request|1|
2	Request failed	Operational	1	None	June 10 20:10:11 host CEF:0|AAA|Core|5.0|1|Request failed|1|
10	Server started	Operational	4	None	June 10 20:10:11 host CEF:0|AAA|Core|5.0|1|Server started|4|
12	Server stopped	Operational	7	None	June 10 20:10:11 host CEF:0|AAA|Core|5.0|2|Server stopped|7|
13	Server unexpectedly stopped	Operational	10	None	June 10 20:10:11 host CEF:0|AAA|Core|5.0|3|Server unexpectedly stopped|10
50	Server Message	Operational	5	Message	June 10 20:10:11 host CEF:0|AAA|Core|5.0|4|Server Message|4|This is my message

Code	Name	Class	Severity	Optional Parameters	Example
100	User logon started	Security	4	Username Ep Ep_addr Sid Unit_id Session_id Event Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|4|User logon started|4|username=Mycompany\\demo sid=S-1-5-XXX session_id=123 event=Windows Logon ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 tenant_name=Mycompany
101	User was successfully logged on	Security	7	Username Ep Ep_addr Sid Session_id method_name method_comment method_infoEvent Tenant_name Template_owner	June 10 20:10:11 host CEF:0|AAA|Core|5.0|5|User was successfully logged on|7|username=Mycompany\\demo sid=S-1-5-XXX session_id=123 method_name=card method_comment=white card method_info=YYY password ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 event=Windows Logon template_owner=Mycompany\\demo tenant_name=Mycompany
102	User was failed to authenticate	Security	9	Username Ep Ep_addr Sid Session_id Method_name Tenant_name Template_owner	June 10 20:10:11 host CEF:0|AAA|Core|5.0|6|User was failed to authenticate|9|Username=Mycompany\\demo sid=S-1-5-XXX session_id=123 method_name=card ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 template_owner=Mycompany\\demo tenant_name=Mycompany
103	User was switched to different method	Security	2	Username Ep Ep_addr Sid Session_id New_method_name Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|7|User was switched to different method|2|username=Mycompany\\demo sid=S-1-5-XXX new_method_name=fingerprint session_id=123 ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
104	User logon session was ended	Security	2	Username Ep Ep_addr Sid Session_id Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|8|User logon session was ended|2|username=Mycompany\\demo sid=S-1-5-XXX session_id=123 ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 tenant_name=Mycompany
105	User logon unwanted	Security	9	Username Ep Ep_addr Method_name Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|8|User logon session was ended|9|username=Mycompany\\demo sid=S-1-5-XXX session_id=123 ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 method_name=voice tenant_name=Mycompany
200	User read app data	Security	3	Username Ep Ep_addr Sid Session_id Data_id Record_id Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|9|User read app data|3|username=Mycompany\\demo sid=S-1-5-XXX session_id=123 data_id=Windows Logon record_id=password ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 tenant_name=Mycompany
201	User write app data	Security	4	Username Ep Ep_addr Sid Session_id Data_id Record_id Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|10|User write app data|4|username=Mycompany\\demo sid=S-1-5-XXX session_id=123 data_id=Windows Logon record_id=password ep=aaadev1.Mycompany.local ep_addr=192.168.91.1 tenant_name=Mycompany
300	Endpoint joined	Security	4	Ep_name Ep_addr Ep_id Username Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|11|Endpoint joined|4|ep_name=xp_client ep_id=123 username=Mycompany\Admin ep_addr=192.168.91.1 tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
301	No rights to join endpoint	Security	7	Ep_name Ep_addr Ep_id Username Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|12|No rights to join endpoint|7|ep_name=xp_client ep_id=123 username=Mycompany\Admin ep_addr=192.168.91.1 tenant_name=Mycompany
302	Failed to join endpoint	Operational	7	Ep_name Ep_addr Ep_id Username Reason Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|13|Failed to join endpoint |7|ep_name=xp_client ep_id=123 username=Mycompany\Admin ep_addr=192.168.91.1 reason=Duplicated tenant_name=Mycompany
303	Endpoint remove	Security	4	Ep_name Ep_addr Ep_id Username Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|14|Endpoint remove|4|ep_name=xp_client ep_id=123 username=Mycompany\Admin ep_addr=192.168.91.1
304	No rights to remove endpoint	Security	7	Ep_name Ep_addr Ep_id Username Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|15|No rights to remove endpoint|7|ep_name=xp_client ep_id=123 username=Mycompany\Admin ep_addr=192.168.91.1 tenant_name=Mycompany
305	Failed to remove endpoint	Operational	7	Ep_name Ep_addr Ep_id Username Reason Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|16|Failed to remove endpoint |7|ep_name=xp_client ep_id=123 username=Mycompany\Admin ep_addr=192.168.91.1 reason=Duplicated tenant_name=Mycompany
306	Endpoint session started	Operational	2	Ep_name Ep_addr Ep_id Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|17|Endpoint session started|2|ep_name=xp_client ep_id=123 ep_addr=192.168.91.1 tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
307	Endpoint session ended	Operational	2	Ep_name Ep_addr Ep_id Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|18|Endpoint session ended|2|ep_name=xp_client ep_id=123 ep_addr=192.168.91.1 tenant_name=Mycompany
308	Invalid endpoint secret	Security	7	Ep_name Ep_addr Ep_id Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|17|Invalid endpoint secret|2|ep_name=xp_client ep_id=123 ep_addr=192.168.91.1 tenant_name=Mycompany
309	Failed to create endpoint session	Operational	7	Ep_name Ep_addr Ep_id Reason Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|18| Failed to create endpoint session|7|ep_name=xp_client ep_id=123 ep_addr=192.168.91.1 reason=No memory tenant_name=Mycompany
310	Failed to end endpoint session	Operational	7	Ep_name Ep_addr Ep_id Reason Tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|18| Failed to create endpoint session|7|ep_name=xp_client ep_id=123 ep_addr=192.168.91.1 reason=No memory tenant_name=Mycompany
401	New repository was added	Operational	4	repo_name repo_type session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|19|New repository was added |4|repo_name=Mycompany repo_type=LDAP session_id=123 tenant_name=Mycompany
402	Failed to add repository	Operational	7	repo_name repo_type session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|20| Failed to add repository|7|repo_name=Mycompany repo_type=LDAP session_id=123 reason=repo already exists tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
403	Repository was removed	Operational	4	repo_name repo_type session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|21|Repository was removed|4|repo_name=Mycompany repo_type=LDAP session_id=123 tenant_name=Mycompany
404	Failed to remove repository	Operational	7	repo_name repo_type session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|22|Failed to remove repository|7| repo_name=Mycompany repo_type=LDAP session_id=123 reason=not empty tenant_name=Mycompany
405	Repository configuration was changed	Operational	4	repo_name repo_type session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|23|Repository configuration was changed|4| repo_name=Mycompany repo_type=LDAP session_id=123 tenant_name=Mycompany
501	Local user was created	Operational	4	user_name session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|24|Local user was created|4|user_name=admin session_id=123 tenant_name=Mycompany
502	Local user was removed	Operational	5	user_name session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|25|Local user was removed|5|user_name=admin session_id=123 tenant_name=Mycompany
503	Failed to create local user	Operational	4	user_name session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|26|ailed to create local user|4|user_name=admin session_id=123 reason=already exists tenant_name=Mycompany
504	No rights to remove local user	Security	7	user_name session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|26|ailed to create local user|4|user_name=admin session_id=123 reason=already exists tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
505	Failed to remove local user	Operational	5	user_name session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|28|Failed to remove local user|5|user_name=admin session_id=123 reason=can't remove currently logged on user tenant_name=Mycompany
506	No rights to create local user	Security	7	user_name session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|29|Failed to create local user|7|user_name=admin session_id=123 tenant_name=Mycompany
601	User was created	Operational	4	user_name session_id repo_name tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|30|User was created|4|username=Someone session_id=123 repo_name=Mycompany tenant_name=Mycompany
602	No rights to create user	Security	7	user_name session_id repo_name tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|31|No rights to create user|7|username=Someone session_id=123 repo_name=Mycompany tenant_name=Mycompany
603	Failed to create user	Operational	4	user_name session_id repo_name reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|32|Failed to create user|4|user_name=someone session_id=123 repo_name=123 reason=already exists tenant_name=Mycompany
604	User was removed	Operational	5	user_name session_id repo_name tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|33|User was removed|5|username=Someone session_id=123 repo_name=Mycompany tenant_name=Mycompany
605	No rights to remove user	Security	7	user_name session_id repo_name tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|34No rights to remove user|7|username=Someone session_id=123 repo_name=Mycompany tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
606	Failed to remove user	Operational	5	user_name session_id repo_name reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|35|Failed to remove user|5|user_name=someone session_id=123 repo_name=123 reason=not found tenant_name=Mycompany
701	Template was assigned to the user	Security	7	user_name session_id ap_name comment tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|36|Template was assigned to the user|7|user_name=Mycompany\some session_id=123 ap_name=Card comment=white card tenant_name=Mycompany
702	Template was enrolled for the user	Security	7	user_name session_id ap_name comment tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|37|Template was enrolled for the user|7|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand tenant_name=Mycompany
703	User enroll the assigned template	Security	7	user_name session_id ap_name comment tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|38|User enroll the assigned template|7|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand tenant_name=Mycompany
704	Template e was linked	Security	8	user_name target_user_name session_id ap_name comment tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|39|Template was linked|8|user_name=Mycompany\some target_user_name=Mycompany\boss session_id=123 ap_name=hand 3D comment=left hand tenant_name=Mycompany
705	Failed to assign template to the user	Security	7	user_name session_id ap_name comment reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|40|Failed to assign template to the user|7|user_name=Mycompany\some session_id=123 ap_name=Card comment=white card reason=no license tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
706	Failed to enroll template for the user	Security	7	user_name session_id ap_name comment reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|41|Failed to enroll template for the user|7|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand reason=ap error tenant_name=Mycompany
707	User can't enroll the assigned template	Security	7	user_name session_id ap_name comment reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|41|User can't enroll the assigned template|7|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand reason=AP not installed on client side tenant_name=Mycompany
709	Failed to link template	Security	8	user_name target_user_name session_id ap_name comment reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|42|Failed to link template|8|user_name=Mycompany\some target_user_name=Mycompany\boss session_id=123 ap_name=hand 3D comment=left hand reason=target user can't be found tenant_name=Mycompany
709	Template link was removed	Security	6	user_name target_user_name session_id ap_name comment tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|43|Template link was removed|6|user_name=Mycompany\some target_user_name=Mycompany\boss session_id=123 ap_name=hand 3D comment=left hand tenant_name=Mycompany
710	Failed to remove template link	Security	6	user_name target_user_name session_id ap_name comment reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|44|Failed to remove template link|6|user_name=Mycompany\some target_user_name=Mycompany\boss session_id=123 ap_name=hand 3D comment=left hand reason=too small carma tenant_name=Mycompany

Code	Name	Class	Severity	Optional Parameters	Example
711	Template was removed	Security	6	user_name ap_name comment session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|45|Template was removed|6|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand tenant_name=Mycompany
712	Failed to remove template	Security	6	user_name ap_name comment session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|46|Failed to remove template|6|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand reason=only owner can remove template tenant_name=Mycompany
713	Template was changed	Security	7	user_name ap_name comment session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|47|Template was changed|7|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand tenant_name=Mycompany
714	Failed to change template	Security	6	user_name ap_name comment session_id reason tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|48|Failed to change template|6|user_name=Mycompany\some session_id=123 ap_name=hand 3D comment=left hand reason=only owner can change template tenant_name=Mycompany
715	Template was changed during logon	Security	5	user_name ap_name comment session_id tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|49|Template was changed during logon|7|user_name=Mycompany\some session_id=123 ap_name=TOTP comment=ASA (iPhone) tenant_name=Mycompany
801	Policy was changed	Security	7	session_id scope comp_name policy_name old_value new_value	June 10 20:10:11 host CEF:0|AAA|Core|5.0|50|Policy was changed|7|session_id=123 scope=global comp_name=password poliices policy_name=minimal password length old_value=4 new_value=8

Code	Name	Class	Severity	Optional Parameters	Example
802	No rights to change policy	Security	8	session_id scope comp_name policy_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|51|No rights to change policy|8|session_id=123 scope=global comp_name=password poliices policy_name=minimal password
803	Failed to change policy	Operational	7	session_id scope comp_name policy_name reason	June 10 20:10:11 host CEF:0|AAA|Core|5.0|52|Failed to change policy|7|session_id=123 scope=global comp_name=password poliices policy_name=minimal password reason=policy not found
901	New license was added	Operational	3	session_id license_id users_count enabled_features expire_date	June 10 20:10:11 host CEF:0|AAA|Core|5.0|53|New license was added|3|session_id=123 license_id=111 users_count=101 enabled_features=client,rte,nps expire_date=31/12/2014
902	Failed to add license	Operational	8	session_id license_id users_count enabled_features expire_date reason	June 10 20:10:11 host CEF:0|AAA|Core|5.0|54|Failed to add license|8|session_id=123 license_id=111 users_count=101 enabled_features=client,rte,nps expire_date=31/12/2013 reason=already expired
1001	Global setting was changed	Security	9	session_id setting_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|55|Global setting was changed|9|session_id=123 setting_name=syslog_server
1002	No rights to change global setting	Security	9	session_id setting_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|56|No rights to change global setting|9|session_id=123 setting_name=syslog_server
1003	Failed to change global setting	Operational	9	session_id setting_name reason	June 10 20:10:11 host CEF:0|AAA|Core|5.0|57|Failed to change global setting|9|session_id=123 setting_name=syslog_server reason=server is unavailable

Code	Name	Class	Severity	Optional Parameters	Example
1101	Password was changed	Security	5	user_name ep ep_addr tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|15|Password was changed|5|ep=xp_client user_name=Mycompany\Admin ep_addr=192.168.91.1 tenant_name=Mycompany
1102	Password was reset	Security	8	user_name ep ep_addr tenant_name	June 10 20:10:11 host CEF:0|AAA|Core|5.0|15|Password was reset|8|ep=xp_client user_name=Mycompany\Admin ep_addr=192.168.91.1 tenant_name=Mycompany

You can change a time zone in the top-right section that displays your local time zone. The changes are applied for only the logs displayed and are not applied for the exported logs. Advanced Authentication resets the time zone when you switch from the **Logs** section or close the Administrative Portal.

You can export the log files. To export logs, perform the following steps:

1. In the **Logs** page, click **Export**.
2. Specify a **Start date** and **End date** to determine the required logging period.
3. Click **Export**. A **File Name** block appears.
4. Click on a name of the logs package (aucore-logs_<logging_period>.tar) to download it.

To configure logs forwarding to a third-party syslog server, see CEF log forwarding.

NOTE: A tenant administrator will not have the option to export logs.

There is a hard coded log rotation based on the file size. The maximum size of a log file is 20 MB. Advanced Authentication stores last ten log files of each type.

You can clear all the logs on the server that you are currently logged on. To clear the logs, perform the following steps:

1. In the **Logs** page, click **Clear**.

   A message appears to confirm that you want to continue clearing the logs.

   NOTE: It is a good practice to export the logs to save as backup before you delete them.

2. Click **OK** to clear the logs.

15 Troubleshooting

NOTE: This chapter provides solutions for known issues. If you encounter any problems that are not mentioned here, please contact the support service.

In this chapter:

- Section 15.1, “Fatal error while trying to deploy ISO file and install in graphic mode,” on page 139
- Section 15.2, “Partition Disks,” on page 139
- Section 15.3, “Networking Is Not Configured,” on page 140
- Section 15.4, “Error "Using a password on the command line interface can be insecure"," on page 140
- Section 15.5, “The ON/OFF Switch Is Broken If the Screen Resolution Is 110%,” on page 140
- Section 15.6, “Error When Requesting For Update,” on page 141

15.1 Fatal error while trying to deploy ISO file and install in graphic mode

Description:

While trying to install Advanced Authentication Server appliance, we get the following fatal error: `"Server is already active for display 0. If this server is no longer running, remove /tmp/ .X0-lock and start again"`.

Solution:

This message is asking to cancel installation. You clicked **Continue** without selecting **I agree** at the bottom of **End User License Agreement**. As a result **I don't agree** was automatically preselected and **Yes** was selected on the next screen. Please run the installer, select **I agree** and continue installation.

15.2 Partition Disks

Description:

The following dialog box is installed during the installation of the Advanced Authentication Server:

Cause:

You are installing Advanced Authentication Server on the drive which contains data already.

Solution:

Advanced Authentication Server installer suggests you to perform disk partitioning. It will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted. To perform disk partitioning, select **Yes** and click **Continue**.

15.3 Networking Is Not Configured

Description:

After the installation of Advanced Authentication Server appliance, the following error is displayed:

Cause:

Your network is not using DHCP protocol.

Solution:

Select **OK** and configure networking manually using the **Configuration Console**. For more information, the Configuring Appliance Networking chapter.

15.4 Error "Using a password on the command line interface can be insecure"

Description:

I have set up DB Master and proceeded to setting up DB Slave. While copying the DB Master database, the following error is displayed: `"Error. (Exception) Warning: Using a password on the command line interface can be insecure. Warning: Using a password on the command line interface can be insecure. mysqldump: Got error: 1045: Access denied for user 'aunet'@'192.168.3.47' (using password: YES) when trying to connect"`. 192.168.3.47 is the IP address of DB Slave.

Cause:

The error occurs due to the incorrect reverse DNS and incorrect hostname specified during installation:

- while installing the DB Master, the pre-populated **aucore.your-router** DNS hostname was selected
- DB Slave is up and re-registered the **aucore** host in DHCP/DNS on the router
- the pre-populated **aucore.your-router** DNS hostmane was selected on DB Slave

Solution:

The pre-populated DNS names cannot be used during the installation. In such case you must enter IP address. DNS hostnames should be specified on the corporate DNS server.

15.5 The ON/OFF Switch Is Broken If the Screen Resolution Is 110%

Description:

While trying to edit the **Lockout options** policy, the ON/OFF switch is broken when the screen resolution is 110%.

Solution:

Change the screen resolution to 100%.

15.6 Error When Requesting For Update

Description:

When requested for the update following error is displayed:

```
E: Could not get lock /var/lib/apt/lists/lock - open (11: Resource temporarily
unavailable)
```

```
E: Unable to lock directory /var/lib/apt/lists/ (AuCore)
```

After rebooting, the following error is displayed and the problem repeats:

```
Command '('sudo','apt-get','update')' timed out after 28 seconds (AuError)
```

Solution:

Ensure that you have a working internet connection on the appliance. This may be a DNS issue.