Administration Guide

Advanced Authentication

Version 5.4

Legal Notice

Contents

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

About this Book

This Guide is intended for tenant administrators and describes the procedure of configuring Advanced Authentication Server appliance and enrolling authentication methods.

Intended Audience

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

1 Advanced Authentication Overview

This chapter contains the following sections:

1.1 About Advanced Authentication

Advanced Authentication™ is a software solution that enhances the standard user authentication process by providing an opportunity to logon with various types of authenticators.

Why choose Advanced Authentication™?

Advanced Authentication™...

- ...makes the authentication process easy and secure (no complex passwords, “secret words”, etc.)
- ...prevents unauthorized use of your computer
- ...protects you from fraud, phishing and similar illegal actions online
- ...can be used to provide secure access to your office

1.2 Advanced Authentication Server Appliance Functionality

Benefits of using Advanced Authentication Server appliance are evident. Advanced Authentication Server appliance...

- ...is cross-platform
- ...contains an inbuilt RADIUS server
- ...supports integration with Advanced Authentication Access Manager
- ...does not require scheme extending
- ...provides administrators with a capability of editing the configured settings through web-based Advanced Authentication Administrative Portal

1.3 Architecture

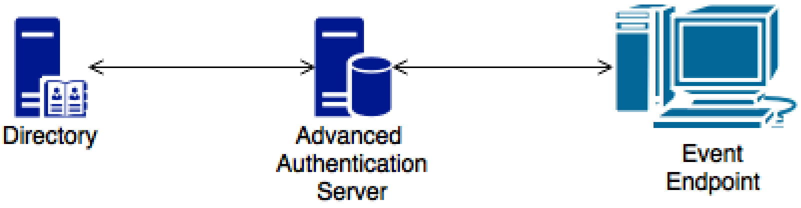
In this chapter:

- Basic Architecture
- Enterprise Architecture
- Enterprise Architecture with Load Balancer

1.3.1 Basic Architecture

The basic architecture of the Advanced Authentication is simple and requires only one Advanced Authentication Server. You can use it for testing and proof of concepts.

Advanced Authentication Server is connected to a Directory that can be an 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.



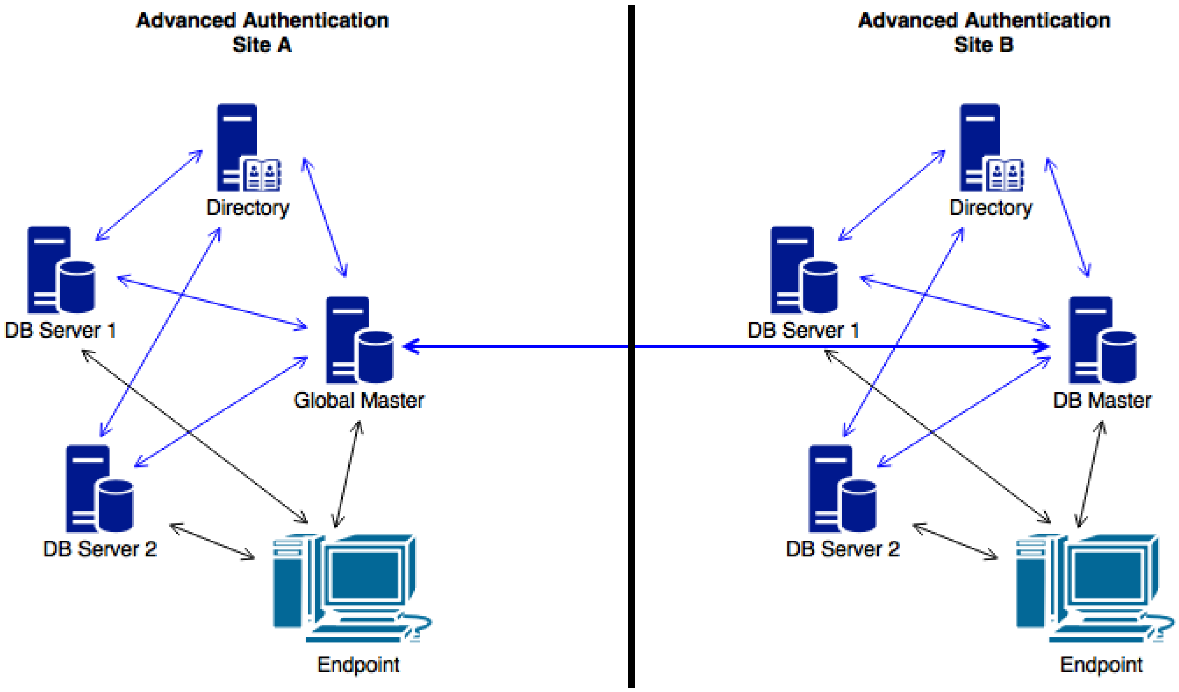
1.3.2 Enterprise Architecture

The Enterprise architecture of the Advanced Authentication contains sites that can be created for different geographical locations. For example, the following illustration displays two Advanced Authentication sites. Site A is the first site created for headquarters in New York. Site A's first Advanced Authentication Server contains the **Global Master** and **Registrar** roles. This server contains a master database and it can be used to register new sites and servers.

Site B is created for the office in London and it contains the identical structure. The master server in another site has **DB Master** role. DB Masters interacts with the Global Master.

DB Server provides a DB Slave database that is used for backup and fail-over. You can create a maximum of two DB Slave Servers per site that can be DB Server 1 and DB Server 2. 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.

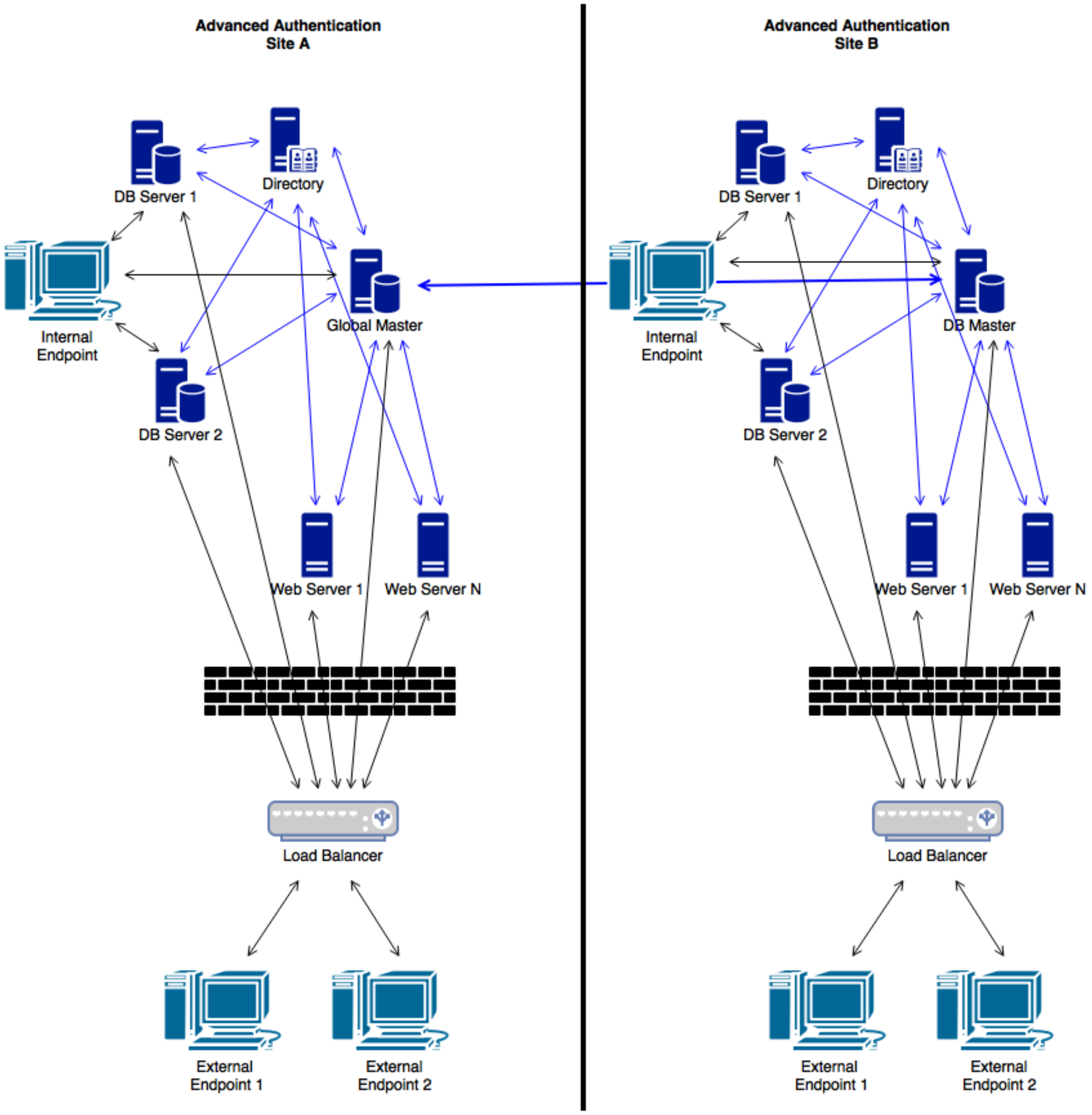
Endpoints can interact with every server that contain a database.



1.3.3 Enterprise Architecture with Load Balancer

The Enterprise architecture with Load balancer contains a more complicated architecture in comparison with the Enterprise Architecture. The architecture contains the following components:

- **Web Servers**: Web Server does not contain a database. It responds to the authentication requests and connects to the DB Master database. You need more Web Servers to serve more workload. There is no limitation for Web Servers.
- **Load Balancer**: It provides an ability to serve authentication requests from the **External Endpoints**. Load Balancer is a third-party component. It is located in DMZ and can be configured to interact with all the Advanced Authentication Servers.



1.3.4 How to Configure Load Balancer for Advanced Authentication Cluster

Load balancer can be installed and configured via third party software. Below is an example of how to install and configure nginx as load balancer on Ubuntu 14.

Target configuration:

	Hostname	IP address	Role	Operation System
Domain controller	win-dc	192.168.1.42	AD DS, DNS	Windows Server 2008 R2
AA v5 master	naafmaster	192.168.1.43	AA Master server	AA v5

	Hostname	IP address	Role	Operation System
AA v5 slave	naafslave	192.168.1.41	NAAF Slave server	AA v5
Load balancer	loadbalancer	192.168.1.40	Nginx load balancer	Ubuntu 14

Before starting the configuration, please make sure that the following requirements are fulfilled:

- 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 14 is installed.

To configure Load Balancer for Advanced Authentication cluster, it is required to install nginx on Ubuntu 14 and configure it.

Installing nginx on Ubuntu 14

To install nginx on Ubuntu 14, follow the steps:

1. Open the following source list:
   - sudo nano /etc/apt/sources.list
2. Add necessary entries:
   - `deb http://nginx.org/packages/ubuntu/ trusty nginx`
   - `deb-src http://nginx.org/packages/ubuntu/ trusty nginx`
3. Update repository and install nginx:
   - apt-get update
   - `apt-get install nginx`
4. Start nginx and make sure that web server is working:
   - `sudo service nginx restart`
5. Open your browser and go to web server http://192.168.1.40 or http://loadbalancer.

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 only round-robin configuration. To configure nginx, follow the steps:

1. Backup original configuration file: `sudo cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf_original`.
2. Open the *nginx.conf* file and replace with following:

```
user nginx;
error_log /var/log/nginx/error.log warn; # error log location
pid /var/run/nginx.pid; # process id file
# limit number of open sockets. Debian default max is 1024, ensure nginx not
open all the sockets.
worker_processes 1;
events {
worker_connections 900; # 512 is default
}
# worker_processes auto; # ssl needs CPU
http {
include /etc/nginx/mime.types;
default_type application/octet-stream;
log_format main '$remote_addr - $remote_user [$time_local] "$request" '
'$status $body_bytes_sent "$http_referer" '
'"$http_user_agent" "$http_x_forwarded_for"';
access_log /var/log/nginx/access.log main; # access log location
sendfile on;
# keepalive default is 75
# keepalive_timeout 10;
gzip on;
gzip_static on;
gzip_comp_level 5;
gzip_disable msie6;
gzip_min_length 1000;
gzip_proxied expired no-cache no-store private auth;
gzip_vary on;
gzip_types text/plain text/css application/json application/javascript
text/xml application/xml application/rss+xml application/atom+xml;
ssl_certificate /etc/nginx/cert.pem;
ssl_certificate_key /etc/nginx/cert.pem;
ssl_session_cache shared:SSL:2m; # 1m stores 4000 sessions, default expire 5
min
ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # disable TLSv3 - POODLE vulnerability
resolver 192.168.1.42 valid=300s ipv6=off; # ip address of DNS
resolver_timeout 10s;
upstream web {
#server naafmaster.company.local:443 resolve;
#server naafslave.company.local:443 resolve;
server 192.168.1.43:443;
server 192.168.1.41:443;
}
server {
#listen 80;
listen 443 ssl;
location / {
proxy_pass https://web;
proxy_set_header HOST $host;
proxy_set_header X-Forwarded-Proto $scheme;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
}
}
}
```

3. Copy certificate from any Advanced Authentication server in cluster from the directory */etc/nginx/cert.pem* to the same directory on load balancer.
4. Go to https://loadbalancer/admin page and make sure that connection was redirected to Advanced Authentication cluster.

IMPORTANT: Nginx can be installed and configured on any Linux supported by nginx.

Additional information on nginx configuration can be found at http://nginx.org/en/docs/.

1.4 Terms

This chapter contains the following terms:

- Authentication Method
- Authentication Chain
- Authentication Event

1.4.1 Authentication Method

Authentication Method verifies the identity of someone who wants to access data, resources, or applications. Validating that identity establishes a trust relationship for further interactions.

1.4.2 Authentication Chain

Authentication Chain is a combination of authentication methods. User needs to pass all methods in order to be successfully authenticated. E.g., if you create a chain which has LDAP Password and SMS in it, the user will first need to enter his/her LDAP Password. If the password is correct, the system will send SMS with an One-Time-Password to the mobile of the user. The user needs to enter the correct OTP in order to be authenticated.

It is possible to create any chain. So for high secure environments it is possible to assign multiple methods to one chain to achieve better security.

Authentication can consist of 3 different factors. These are:

- Something you know: password, PIN, security questions
- Something you have: smartcard, token, telephone
- Something you are: biometrics like fingerprint or iris

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

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

1.4.3 Authentication Event

Authentication Event is triggered by an external device or application which needs to perform authentication. It can be triggered by a RADIUS Client (Citrix Netscaler, Cisco VPN, Juniper VPN, etc) or API request. Each event can be configured with one or more authentication chains which will provide user with a capability to authenticate.

Within the Advanced Authentication framework, an authentication event is configured in the Events section. It is possible to enable or disable an event, and to add method-chains to the event. With specific events it is possible to assign clients to the event.

2 Advanced Authentication Server Appliance Deployment

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

This chapter contains the following sections:

2.1 First Login To Advanced Authentication Administrative Portal

To log in to Advanced Authentication Administrative Portal, follow the steps:

1. Enter the tenant name and then administrator's login in the following format: repository\user (**local\admin** by default). Click **Next** to continue.
2. The **Admin Password** chain is automatically selected by the system as the only available method. Enter the tenant administrator password.
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 languages supported are: Arabic, Chinese Simplified, Chinese Traditional, Danish, Dutch, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, Hebrew, and Swedish.

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

2.2 Configuring Advanced Authentication Server Appliance

IMPORTANT: Advanced Authentication Administrative Portal contains the Help option which contains detailed instructions on how to configure all settings for your authentication framework. You are provided with a capability to call the Help option by clicking the ? icon in the upper right corner of Advanced Authentication Administrative Portal. The Help section provides you with information on the specific section you are working on.

After the installation of Advanced Authentication Server appliance and configuring an applicable server mode, administrator is provided with a capability to configure Advanced Authentication Server appliance through Advanced Authentication Administrative Portal. To configure Advanced Authentication Server, it is required to follow the steps:

1. Adding Repository
2. Configuring Methods
3. Creating Chain
4. Configuring Events
5. Managing Endpoints
6. Configuring Policies
7. Configuring Server Options
8. Adding License

2.2.1 Adding Repository

A repository is the place where your users are stored. Advanced Authentication will not change your existing repository. It is only used to read user information. The storage of authentication templates and configuration settings all happens inside the appliance and is 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 adding a new repository the users in that repository can be matched to authentication chains. Only read rights are needed for the repository.

Please fill in the correct credentials and click **Add Server**. Here you can add the different servers in your network. The list will be used as a pool of servers, each time the connection is open a random server is chosen in the pool and unavailable servers will be discarded.

After you click **Save**, all information will be verified and saved.

To add repository that will be used for Advanced Authentication, follow the steps:

1. Open the **Repositories** section.
2. Click **Add**.
3. Select an applicable repository type from the **LDAP type** drop-down list. It can be 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.
4. For AD a repository name will be automatically set to NetBIOS name of domain. For other LDAP types you need to enter it manually in the **Name** field.
5. Specify a container for the users in the **Base DN** text box. When you select the **Subtree** option, Advanced Authentication performs a search for users in all children nodes. You can change the search scope by selecting the **Search one level only** option.
6. Specify a user account in the **User** text box and enter the password of the user in the **Password** text box. Ensure that the user's password has no expiry.
7. You can specify a container for the groups in the **Group DN (optional)** text box. When you select the **Subtree** option, Advanced Authentication performs a search for the groups in all children nodes. You can change the search scope by selecting the **Search one level only** option.

8. In case if you use AD, switch to DNS discovery option if you want to find LDAP servers automatically. In this case you will need to fill the DNS zone and Site name (optional) fields and click the Perform DNS Discovery button.
9. If you want to add the LDAP servers manually leave the **Manual setting** option checked and click **Add server**.
10. Specify an LDAP server's address and port. Select the **SSL** check box to use SSL technology (if applicable). Click **Save**, next to server's credentials. Add additional servers (if applicable).
11. You can also expand the Advanced Settings section if you need to configure custom attributes. This is required for OpenDJ, OpenLDAP and in some cases for NetIQ edirectory.
12. 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 v5.2 it is required that you specify a common Base DN for users and groups in the **Base DN** field.

You can later change the existing repositories by clicking **Edit** and you can add a new repository by clicking **Add**.

To check the sync status click **Edit** for the used Repository and see information in the **Last sync** section. Click **Full sync** to perform the full sync.

NOTE: Advanced Authentication performs automatic synchronization of changed objects (fastsync) hourly (for AD only), the complete synchronization (fullsync) is performed weekly.

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

Advanced Settings

To access the section of Repository configuration expand the Advanced Settings by clicking the **+** button. The settings allow to customize attributes which Advanced Authentication reads from repository.

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 Active Directory (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: mail, otherMailbox.

User mobile phone attributes

Advanced Authentication checks the specified attributes to get a user's phone number.

Default attributes: mobile, otherMobile.

Group lookup attributes

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

For Active Directory (AD), the default attributes 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 Active Directory (AD), the default attributes 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 which 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, POSIX style must be disabled. If it contains posixGroup it must be enabled. To enable POSIX style groups switch the appropriate option to ON.

User UID attribute

Available when POSIX style groups is ON.

Default value: uid.

Object ID attribute

Available for other LDAP type only.

Default value: entryUUID.

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

Used Attributes

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

Name of the Attribute	LDAP Name	Description	Type	Supported in Active Directory	Supported in LDS	Supported in eDirectory
CN (Common Name)	CN	An identifier of an object	String	Yes	Yes	Yes
Mobile	Mobile	A phone number of an object's cellular or mobile phone	Phone number	Yes	Yes	Yes
Email Address	mail	An email address of a user	Email address	Yes	Yes	Yes
User-Principal-Name (UPN)	userPrincipalName	An Interne based format login name for a user	String	Yes	Yes	Yes
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	Yes	No	No
GUID	GUID	An assured unique value for any object	Octet String	No	No	Yes
Object Class	Object Class	An unordered list of object classes	String	Yes	Yes	Yes
Member	Member	A list that indicates the objects associated with a group or list	String	Yes	Yes	Yes

Name of the Attribute	LDAP Name	Description	Type	Supported in Active Directory	Supported in LDS	Supported in eDirectory
User-Account-Control	userAccountControl	Flags that control the behavior of the user account	Enumeration	Yes	No	No
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	Yes	Yes	No
Primary-Group-ID	primaryGroupID	A relative identifier (RID) for the primary group of a user	Enumeration	Yes	No	No
Object-Guid	objectGUID	A unique identifier for an object	Octet String	Yes	Yes	No
object-Sid	objectSid	A Binary value that specifies the security identifier (SID) of the user	Octet String	Yes	Yes	No
Logon-Hours	logonHours	Hours that the user is allowed to logon to the domain	Octet String	Yes	No	No
USN-Changed	uSNChanged	An update sequence number (USN) assigned by the local directory for the latest change including creation	Interval	Yes	Yes	No

NOTE: The sAMAccountName and userPrincipalName attributes are supported for only 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']
```

Local Repository

To access the Local repository settings click **Edit** in LOCAL repository block of Repository section.

On the **Global Roles** tab it's possible to manage Helpdesk/Security Officers (ENROLL ADMINS) and Advanced Authentication Administrators (FULL ADMINS).

By default there are no ENROLL ADMINS and LOCAL\ADMIN is only one account specified as FULL ADMIN. You may change this by adding the user names from local or the used repositories in Members fields. Then click **Save** to apply the changes.

On the **Users** tab it's possible to manage the local users.

To add the new local account click **Add** button. Then you will need to specify a user name, first name, last name, description and the user's password.

2.2.2 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:

- 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.
- FIDO U2F - an option which allows to enable check of attestation certificate.
- Voice Call - security settings of Voice Call method.
- Swisscom Mobile ID - settings for the Swisscom mobile ID 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.

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.

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.

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.

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.**

FIDO U2F

The section contains certificate settings related to FIDO U2F authentication method. By default Advanced Authentication doesn't require the attestation certificate for authentication by FIDO U2F compliant token. If you plan to enable the feature, ensure that you have a valid attestation certificate added for your FIDO U2F compliant tokens. A Yubico attestation certificate is preconfigured in the Advanced Authentication appliance. Use **Add** button to add a device manufacturer certificate, which must be in PEM format. To enable check of attestation certificate switch the **Require attestated device** option to ON.

IMPORTANT: To use the FIDO U2F authentication in Advanced Authentication Access Manager 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 in Advanced Authentication Access Manager

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 in Advanced Authentication Access Manager

---

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 Advanced Authentication Access Manager. According to FIDO U2F specification, enrollment and authentication must be performed for one domain name. Advanced Authentication 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
- Advanced Authentication 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.

LDAP Password

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

The option allows to save LDAP Password in user data during a first logon, so the further authentications using chains without LDAP Password can be performed using only Advanced Authentication authentication method until the password will be expired and changed.

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's required to use the default Traditional format of the CSV (check `YubiKey Personalization Tool - Settings tab - Logging Settings`) with comma as a delimiter.

  IMPORTANT: Yubico csv with the tokens which personalized not to input the OATH Token Identifier is not supported.

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).

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.

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).

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.

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.

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.

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.

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.

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 to where the smartphone app will connect for authentication. Please use http only for testing and use https in a production environment. You will need a valid certificate when 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.

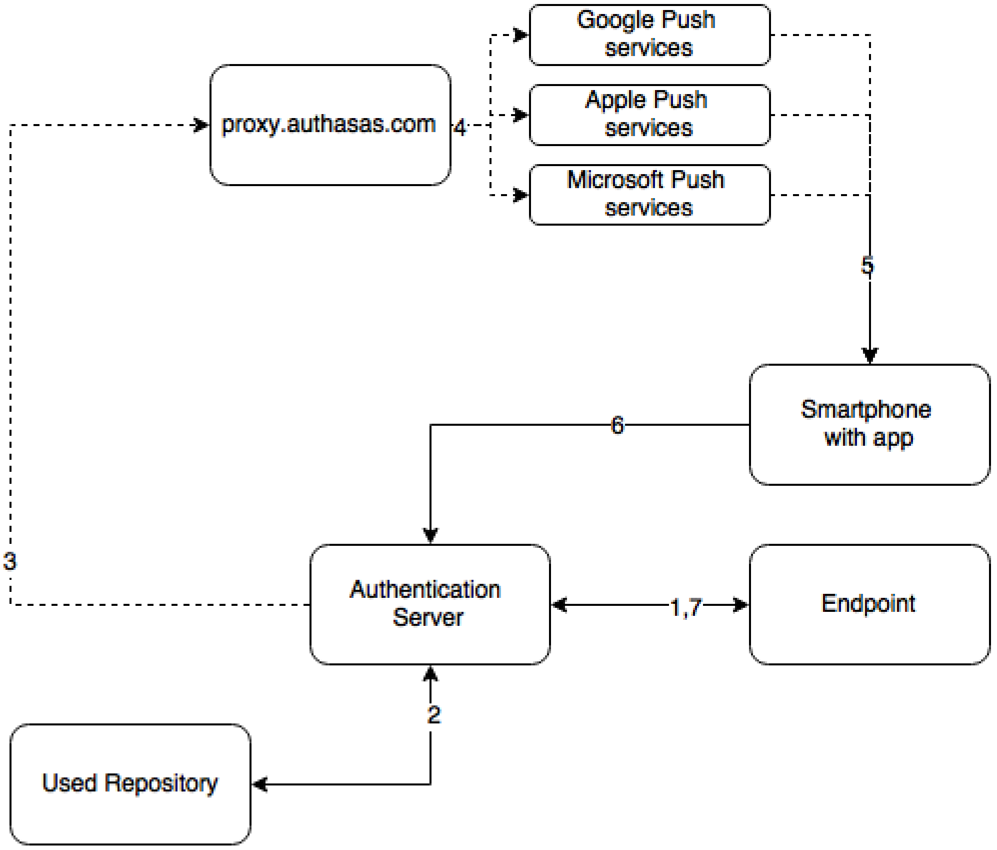
8 Click **Save**.

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).

Voice Call

The section contain security settings for Voice Call 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.

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.

IMPORTANT: Notifications about expiring pins are not supported.

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. **AP ID**: Identifier of the application provider.
2. **AP 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.

2.2.3 Creating 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.

2.2.4 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 chains that will be assigned to the current event.
5. 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.
6. 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

7. 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.
   - Select **OAuth2** if you need to create an OAuth 2.0 event.
   - Select **Generic** otherwise.
4. Select the chains that will be assigned to the event.
5. Select the required endpoints from Endpoint whitelist (if applicable). Access to the event from other endpoints will be restricted.
6. 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.
7. Specify the redirect URLs, if you have selected OAuth2 event. OAuth 2 settings are available only for OAuth2 events.

   NOTE: The client ID and client secret is generate automatically. Client ID, client secret and redirect URL will be consumed by consumer web application for accessing OSP6 interface. After successful authentication using OSP interface, the redirect URL web page specified in the event is displayed.

   The Open Settlement Protocol 6(OSP6) is a client/server protocol used to exchange authorization between the appliance and the consumer web application. OSP 6 acts as an interface for authentication between the consumer web application and the appliance.

8. 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**).

9. Click **Save.**

If you have created a custom OAuth 2 event, then perform the following steps to get the OSP6 page and 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<Default Tenant>/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) in the OSP6 login page to access the consumer web application.

The following predefined events are available.

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.*

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).

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.

Helpdesk

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

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)**.

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)**.

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.

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.

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.

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)**.

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.

Synchronization of RADIUS Server configuration between Advanced Authentication servers is not supported. You can configure the RADIUS Server on all servers manually.

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's 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: 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.

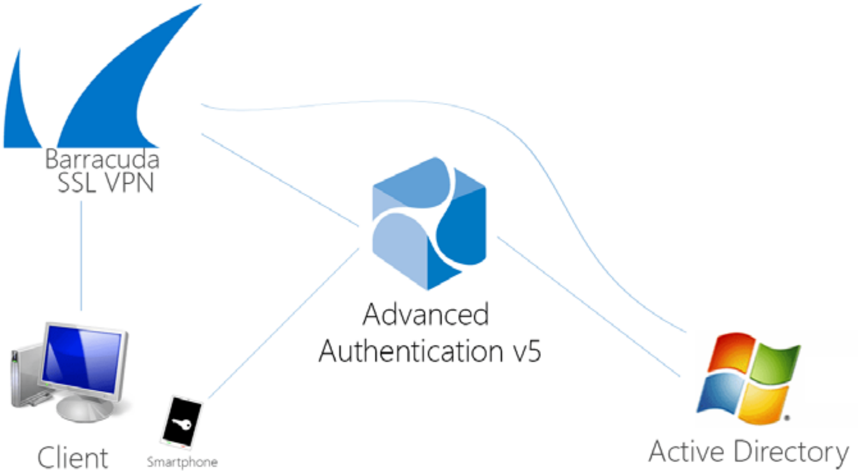
The related articles:

- Configuring integration with Barracuda SSL VPN
- Configuring integration with Citrix NetScaler
- Configuring integration with Dell SonicWall SRA EX-Virtual appliance
- Configuring integration with FortiGate
- Configuring integration with OpenVPN

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:

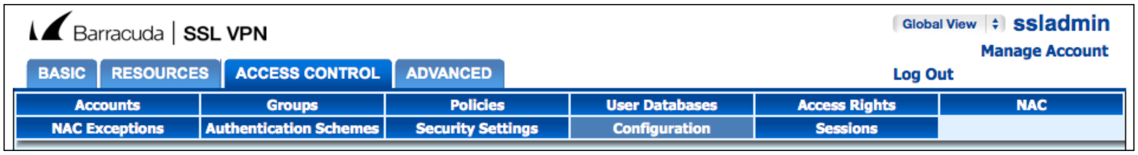
- Barracuda SSL VPN appliance v380 or above (Firmware version 2.6.1.7 was used to prepare these instructions)
- Advanced Authentication v5 appliance with the already configured repository

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:

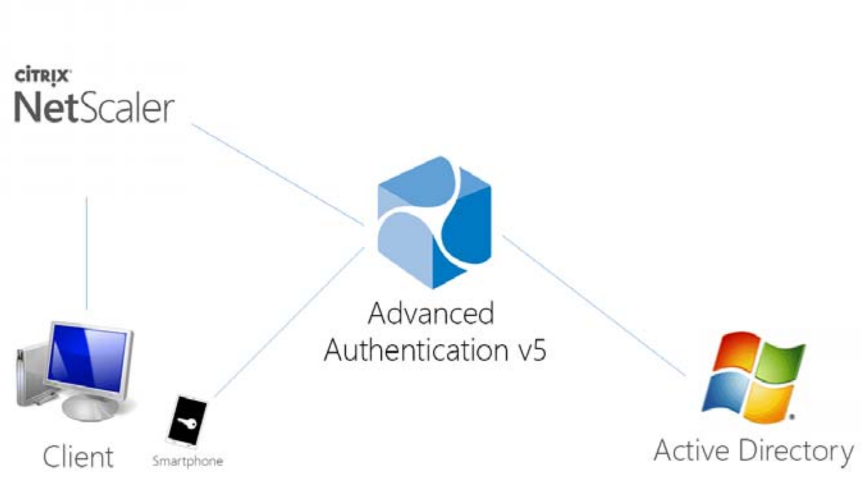
1. Enter user's credentials.
2. Click **More** and select the configured User Database (if the database is not selected by default).
3. Click **Log In** and approve the authentication on the user's smartphone.

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

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 Call 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:

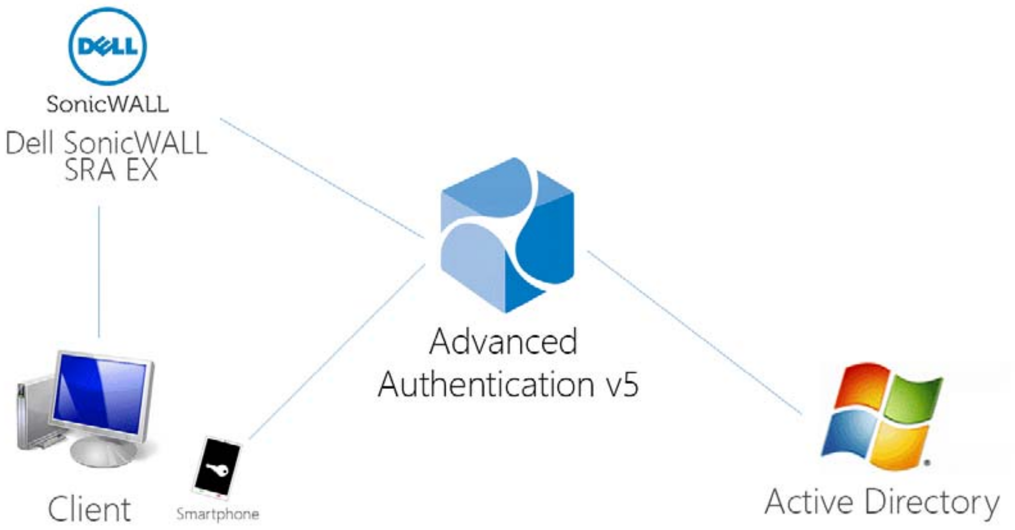
1. Enter user’s credentials and click **Login**.
2. Accept authentication on your smartphone.

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

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:

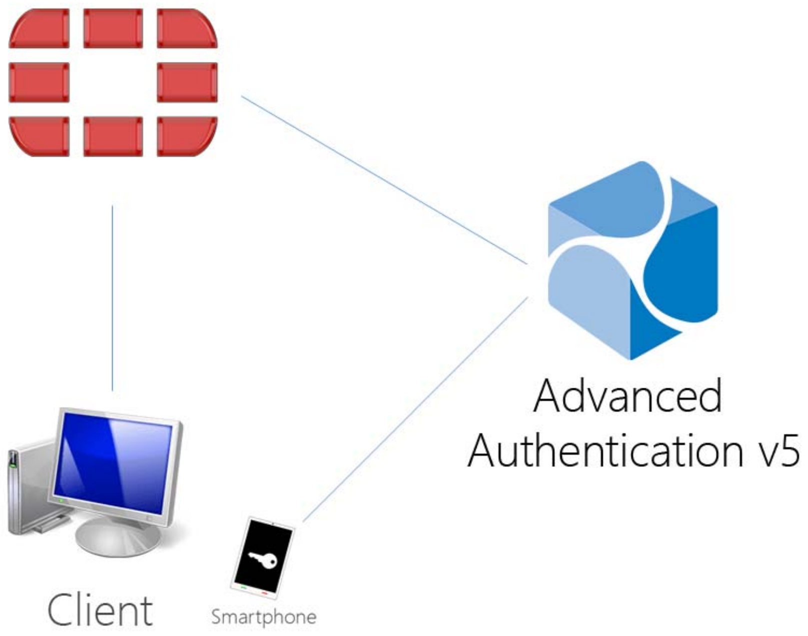
1. Open browser and go to workplace. Enter your username and ldap password.

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

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:

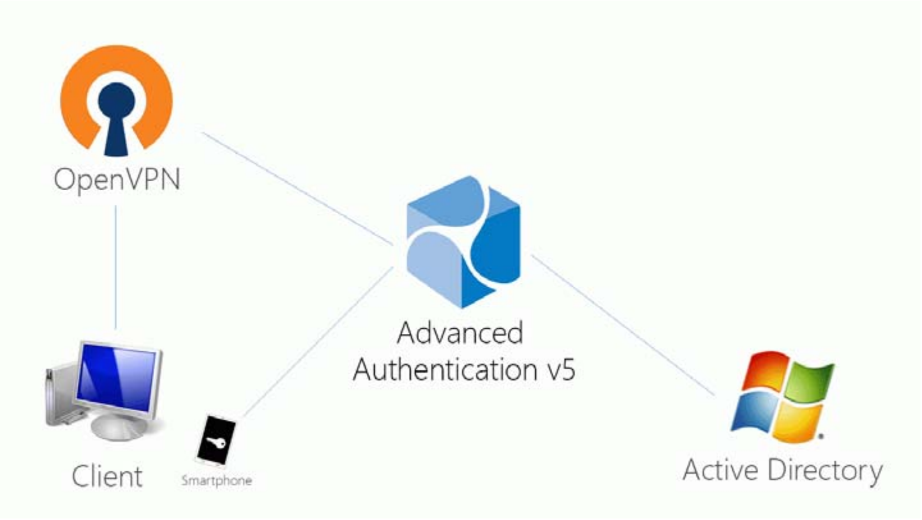
1. Enter user’s credentials and click **Login**.
2. Enter OTP and click **Login**.

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.

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
```

After 3 successful authentications with SMS AP to OpenVPN the user account was locked

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.

2.2.5 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. Windows Client (DNS name will be used as endpoint name).
6. 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 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.

2.2.6 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.
- Cache options: security settings which allows to disable local caching of authenticators.
- 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.
- Helpdesk Options: a security option which allows to disable asking for user's credential when a security officer is managing the user's authenticators.
- 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.
- Logon Filter for AD: Enable/Disable logon filter for Active Directory.
- Mail sender: SMTP server settings.
- SMS sender: settings for external SMS service provider, contains predefined settings for Twilio, MessageBird.
- Voice sender: Twilio settings for Voice Call method; an option to allow enrollment for users without telephone number.
- Sharing authenticators: setting that allows a helpdesk (security officer) to link authenticators of a user to help authenticate to another user’s account.
- Geo fencing options: setting that helps to create authentication zones by drawing boundaries for a geographical location.

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

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.

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.

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

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.

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. 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.

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.

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.

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`.

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.

To configure Logon Filter, after it is enabled, perform the following steps:

1. Open the **Repositories** section.
2. Click **Edit** for the required Active Directory repository.
3. Expand the **Advanced Settings** section.
4. Specify the Active Directory groups for **Legacy logon tag** and **MFA logon tag.**

NOTE: Legacy logon tag must point to a group in the Active Directory that must include all the users. It should be a custom group. The built-in groups like Domain Users are not supported. The users can be members of the group directly or you can add another custom group with users to the group. MFA logon tag should point to an empty group in Active Directory. When a user logs in, Logon Filter checks the user's authentication. If the user uses the Advanced Authentication, then the user is automatically moved to the group specified in the MFA logon tag field.

When all the workstations have the NetIQ Windows Client installed and users are able to login, you can restrict access to the workstations by performing the following steps.

Perform the following steps to add the group in Group Policy Management Editor:

1. On a Domain Controller, open Group Policy Management Editor by entering `gpmc.msc` in the search box.
2. Double-click the name of the forest, double-click Domains, and then double-click the name of the domain in which you want to join a group.
3. Right-click **Default Domain Policy,** and then click **Edit**.
4. In the console tree, expand and navigate to **Computer Configuration** > **Policies** > **Windows Settings** >**Security Settings** > **Local Policies** > **User Rights Assignment.**
5. In the right pane, double-click **Allow Logon Locally.**
6. Click **Add User or Group**.
7. Specify a group which is pointed in the **MFA logon tag**.
8. Click **OK**.
9. Click **OK** in the **Allow log on locally Properties** dialog box.

NOTE: The above steps prohibits the users without NetIQ Windows Client installed (only on workstations joined to the domain) from logging on to the workstations. A user with the NetIQ Windows Client installed will be automatically moved from a group pointed to the Legacy logon tag to a group pointed to the MFA logon tag.

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.

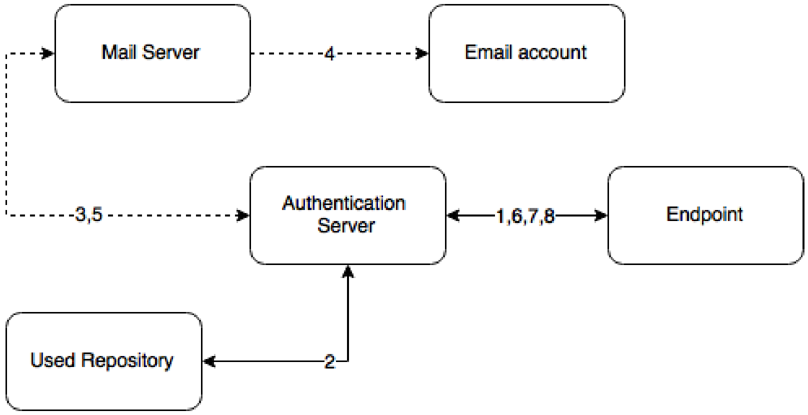
It's required to configure the following settings:

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).

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 the following fields:

1. Account sid
2. Auth token
3. Sender phone

You can find more information on the Twilio website.

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

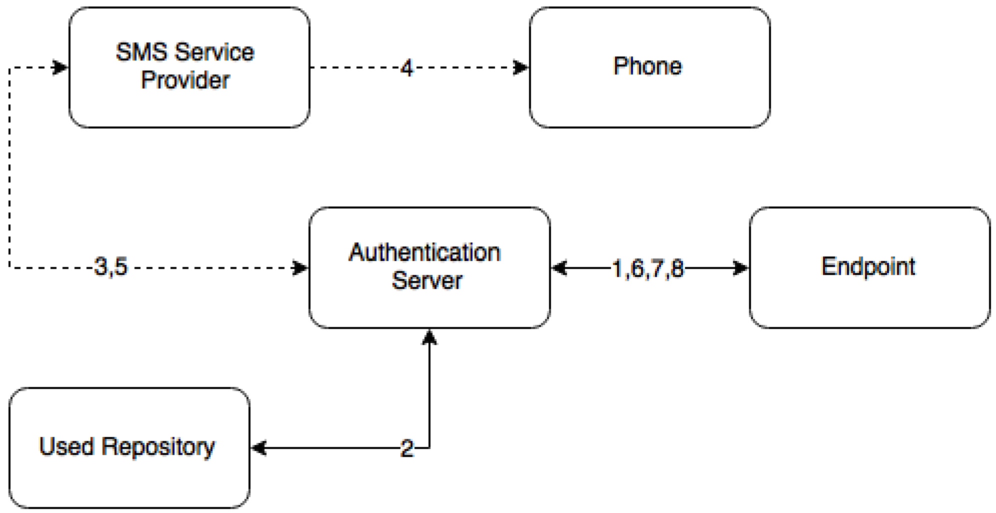
   For more information on additional parameters for Clickatell, refer to the Clickatell documentation.

   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).

Voice Sender

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

The section contains the Voice Call method settings. It's used by Voice Call. 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.

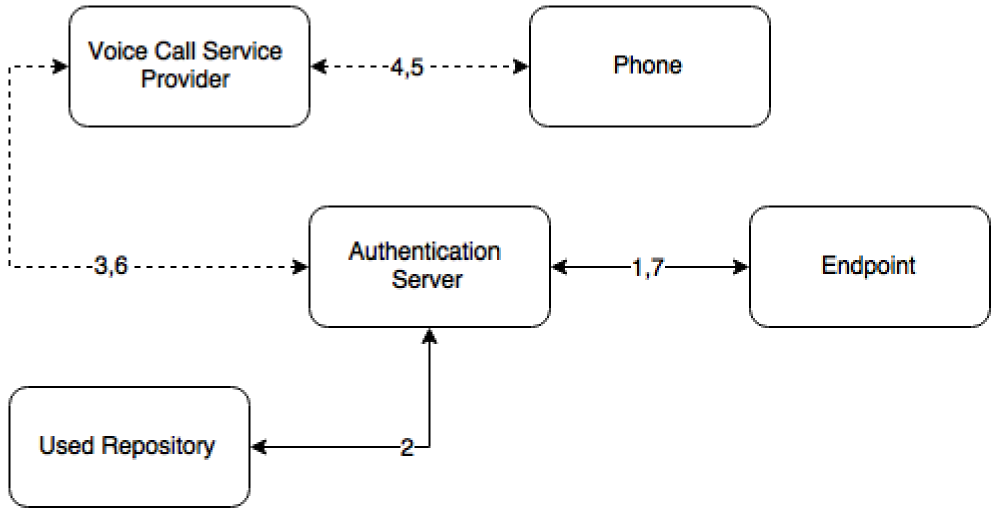
The **Enroll without phone** section allows to configure behavior when a user is trying to enroll the Voice Call authenticator, but the user's repository data doesn't contain a phone number. If **Allow enroll user w/o phone** option is set to OFF such user will not be able to enroll the Voice Call authenticator 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).

Sharing authenticators

This policy 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**.

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**.

2.2.7 Configuring Server Options

Advanced Authentication Server uses an HTTPS protocol. You should create a certificate file (PEM or CRT) 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), if they are present.
3. Click **Upload** to upload the selected SSL 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.

2.2.8 Adding 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 which was assigned to the used chains. Then perform a synchronization for the repository in the Repositories section. The existing user's authenticators will be removed.

2.3 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.

3 Advanced Authentication Server Maintenance

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.

In this chapter, the following sections are explained:

- Section 3.1, “Reporting,” on page 67
- Section 3.2, “Logging,” on page 68

3.1 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.

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.

3.2 Logging

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

- System log
- RADIUS Server log

The System log contains the following information events:

- 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

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.