



NetIQ Advanced Authentication Framework - Administrative Tools

Administrator's Guide

Version 5.1.0

Table of Contents

Table of Contents	1
Table of Contents	2
Introduction	5
About This Document	5
NetIQ Advanced Authentication Framework™ Overview	6
About NetIQ Advanced Authentication Framework™	6
NetIQ Advanced Authentication Framework™ Technology	8
NetIQ Advanced Authentication Framework™ Administrative Tools	9
Terms and Abbreviations	10
Authenticator	10
Active Directory Domain Controller	10
Delegating Control	11
Enroll Authenticator	11
Enterprise Key	11
Re-enroll Authenticator	11
Scheme Master	11
System Administrator's Workstation	12
Security Officer's Workstation	12
User Authentication	12
NetIQ Advanced Authentication Framework Components Description	13
Service Accounts and Groups	15
Administrative Tools	16
Active Directory Users and Computers	17
Working with User Accounts	17
Creating New User	18
Enrolling Authenticator	22
Editing NetIQ Advanced Authentication Framework User Properties	24
Linked Accounts	27
Managing Authenticators	30
Adding Authenticator	32
Re-enrolling Authenticator	34
Testing Authenticator	35
Removing Authenticator	36
Editing Properties of Multiple NetIQ Advanced Authentication Framework Users	37
Resetting Active Directory Password	38
Removing User	40
Delegating Control	41
Allowing to Cache Authenticators	45
Allowing to Cache Authenticators on Multiple Computers	47
Automatic logon in NetIQ Advanced Authentication Framework	48
NetIQ Advanced Authentication Framework User Viewer	49
Adding User Viewer to Console	49
Visual Appearance	52

Viewing Users	54
Managing User Properties	55
Managing Authenticators	55
Adding Authenticator	57
Re-enrolling Authenticator	57
Testing Authenticator	57
Removing Authenticator	57
Data Exporting	58
Logon Methods Report	58
Audit Tools	59
Log Server Setting	59
Event Viewer	60
NetIQ Events List	61
Group Policies	64
Adding Group Policies	66
Configuring Group Policies	72
Security Policies	73
Authenticator Life Period	73
Credential Providers Filter Settings	75
Disable Random Password Generation by Default	76
Enable PIN Caching	77
Hide password mode from logon UI	78
Lock account on failed logon	78
Password Length	79
PIN Restrictions	81
Use domain password as PIN	82
Disabled PIN Host List	83
Event Log Policies	85
Freeze Communication if Log Server is Unavailable	85
Log Servers	88
Register All Password Management Events	89
Register All User Authentication Events	90
Workstation Policies	91
Alternative Logo for Credential Provider	91
Alternative Logo for GINA and Wizard	94
Deny to Specify Authenticator Comment at Enrollment	96
Deny to Start Client Tray When User Logs on to Windows	97
Disable "Use Dial-up Connection" Option	98
Do Not Allow to Skip Welcome Window	99
Enable Device Detection for All	100
Enhanced Reaction on Device Events	101
Force Logoff Once Authenticator is Successfully Enrolled	103
Lifetime of Notification about Password Reset	104
Tap and Go	105
"Use Current Settings as Defaults" Option Management for PC Unlocking	106
"Use Current Settings as Defaults" Option Management	108

BSP Policies	110
Number of Fingers to Enroll	111
Play Sounds	112
Repository Policies	116
Repository	116
ADAM Settings	119
Enable Novell Support	120
UI Look & Feel Policies	121
Show OSD Num Pad	121
Radius BSP	122
Pin Required	123
Troubleshooting	124
Error Initializing User Viewer Snap-In	125
User Authentication Error	125
NetIQ Users Settings in ADUC are not Active	127
Time Drift	128
Index	129

Introduction

About This Document

Purpose of the Document

This Administration Tools Administrator's Guide is intended for system administrators and describes how to work with NetIQ Advanced Authentication Framework administrative tools.

Document Conventions

This document uses the following conventions:



Warning. This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.



Important notes. This sign indicates important information you need to know to use the product successfully.



Notes. This sign indicates supplementary information you may need in some cases.



Tips. This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

NetIQ Advanced Authentication Framework™ Overview

About NetIQ Advanced Authentication Framework™

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

Why choose NetIQ Advanced Authentication Framework™?

NetIQ Advanced Authentication Framework™...

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

What is NetIQ Advanced Authentication Framework™?

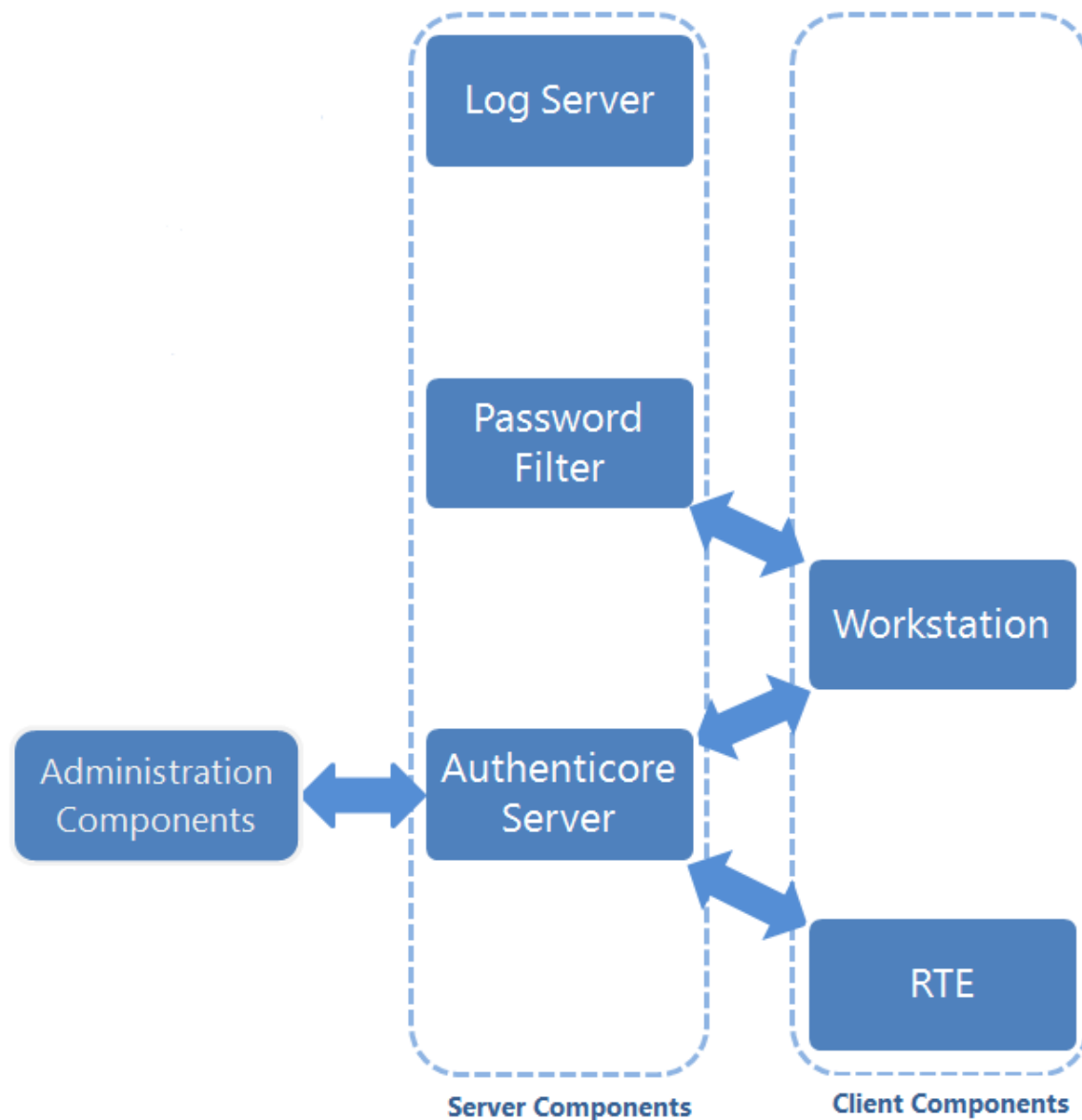
NetIQ Advanced Authentication Framework™ is a system made up of 3 sets of components (Server components, Administrator components and Client components).

Administrative components are used to create, edit and remove NetIQ Users. They are also used to create, edit and remove users' authenticators and to enable or disable caching. Administrator components allow using User Viewer.

Server components are used for working with data storage. They check user authentication requests and modify data storage.

Administrator components and **Server components** may be installed both, on the same or separate servers.

Client components perform user authentication. They are also used to create, edit and delete authenticators on behalf of the user.



- NetIQ Advanced Authentication Framework™ is intended for the use within corporate environment.
- Users data stored in Active Directory database are protected by **Enterprise Key** (see [Enterprise Key](#)).

NetIQ Advanced Authentication Framework™ system includes the following additional module:

- **RTE** (Runtime Environment), which allows to use SDK with no need to install “NetIQ Advanced Authentication Framework – Client” component. It is helpful when you would like to use NetIQ Advanced Authentication Framework™ to secure access to certain applications only, without changing the regular Windows logon procedure.

NetIQ Advanced Authentication Framework™ Technology

NetIQ Advanced Authentication Framework™ technology relies on [authenticator](#).

Although password authentication is simple and the most common, it has a number of disadvantages:

- a simple password is both easy to remember and to obtain. They can easily be guessed or hacked;
- a complex password is both hard to obtain and to remember. However, users tend to write their long complex passwords down and keep them on their workplaces where anyone else can see them.
- a password can be communicated to anyone else.

Authenticators are better, because they do not complicate logon procedure, but allow users to give up passwords and thus keep access to their information secure. NetIQ Advanced Authentication Framework™ gives users an opportunity to use hardware authentication devices and retains an opportunity to log on by password (on permission from NetIQ administrator).

Authentication devices supported by NetIQ Advanced Authentication Framework™ include biometric scanners, smart cards, tokens, memory cards, etc.

- An authenticator can be enrolled (created) at first logon or at any time later.
- The number of authenticators you can have is defined by NetIQ administrator.
- NetIQ Advanced Authentication Framework™ allows you to manage your authenticators: enroll, re-enroll (edit), test, delete. All these actions require permission from NetIQ administrator.

NetIQ Advanced Authentication Framework™ Administrative Tools

- Due to **Enhanced User Creation Wizard**, you may create an NetIQ Advanced Authentication user when creating an Active Directory user account. When creating a new user, you can enroll and manage user's authenticators.
- When managing user properties, you have an opportunity to manage user authenticators (if you were delegated control over the corresponding rights from NetIQ Advanced Authentication User/Computer settings management).

 Delegating control option doesn't work for ADLDS/ADAM configurations. In that case, you will need Authenticore Admins group rights to edit NetIQ Advanced Authentication user settings.

You have an opportunity to edit properties of multiple users and allow authenticators caching on multiple computers at a time via **Properties** of selected users or **Organization Unit Properties and Group Properties**.

- **NetIQ Advanced AuthenticationFramework User Viewer MMC snap-in** allows you to view the list of users, check authentication methods used by the users, modify user properties and manage their authenticators.
- A number of group policies allow you to manage NetIQ Advanced Authentication Framework™ system. The policies are divided into sections depending on their scope (Security policies, Event Log policies, Workstation policies, Repository policies, UI Look & Feel policies).
- Enabling **Allow caching of user authenticators on this computer** box for particular computer allows you also to cache authenticators for RTE, even if NetIQ Advanced Authentication Framework Client component is not installed.

Terms and Abbreviations

In this chapter:

- [Authenticator](#);
- [Active Directory Domain Controller](#);
- [Delegating Control](#);
- [Enroll Authenticator](#);
- [Enterprise Key](#);
- [Re-enroll Authenticator](#);
- [Scheme Master](#);
- [System Administrator's Workstation](#);
- [Security Officer's Workstation](#);
- [User Authentication](#).

Authenticator

Authenticator is data submitted by a user for the purpose of his/her personality validation. Both common character strings (e.g. symbolic password) and data received from a hardware authentication device (e.g. digital fingerprint model, memory card ID) can appear as an authenticator. Two authenticator types are usually distinguished: **reference authenticator** and **current authenticator**.

Reference authenticator is data submitted by a user to the system as a part of user registration procedure. Particular characteristics of these data depend on the authentication method selected by the user, such as password, or digital fingerprint model, or memory card ID, etc. Once a reference authenticator has been created and encrypted, it is saved in Active Directory database. Authentication server uses reference authenticators to carry out user authentication procedure.

Current authenticator is data submitted by a user to the system as a part of authentication procedure. Particular characteristics of these data depend on the authentication method selected by the user, such as password, or digital fingerprint model, or memory card ID, etc.

A successful logon is performed only when the reference and the current authenticators match.

Active Directory Domain Controller

Domain Controller in Microsoft Windows family environment is the computer that is responsible for users' authentication and containing the part of the catalogue. Domain controller allows you to access data stored in the catalogue and to manage and modify this information. All modifications done on one domain controller are automatically copied onto the rest of the controllers. Thus, almost all operations concerning network administering can be performed on any of the domain controllers. However, a number of operations are performed only on one controller – [Scheme Master](#).

Delegating Control

Delegating control means giving control over NetIQ Advanced Authentication Framework settings to a user or a group of users within a container/Organizational Unit.

Enroll Authenticator

Enroll authenticator means to create an authenticator, "train" the system to recognize it and save the result to the database. (See also: [Authenticator](#)).

Enterprise Key

Enterprise key is an encryption key set, which is used by Authenticore Server to encrypt/decrypt users' data. Enterprise key configuration is the final step you take when installing the first Authenticore Server in the domain. In case you install additional Authenticore Servers, Enterprise Key is transferred from the first server and obtained on additional ones automatically.

Re-enroll Authenticator

Re-enroll authenticator means to change the authenticator and save the changes to the database. (See also: [Authenticator](#)).

Scheme Master

A Domain Controller is intended to authenticate users and contains the catalogue part. The network can be administered on any of the domain controllers. However, only the first Active Directory Domain Controller – **Scheme Master** – can modify catalogue Scheme. If more than one domain controller modifies the Scheme, it may lead to conflicts and, as a result, to a failure in

normal network functioning. Therefore, only one current server responsible for catalogue Scheme is allowed at a time.

System Administrator's Workstation

A system administrator can use control both standard and specific administrative tools to manage NetIQ Advanced Authentication Framework system. The standard administrative tools are "Active Directory Users and Computers" MMC snap-in, Event Viewer MMC snap-in. The specific administrative tools are installed in "NetIQ Advanced Authentication Framework – Administrator Components" package on the **system administrator's workstation**.

Security Officer's Workstation

A **security officer's workstation** must contain the installed "NetIQ Advanced Authentication Framework – Administrator Components" package. The main tool for a security officer is the "NetIQ Advanced Authentication Framework – User Viewer" MMC snap-in. The use of other administrative tools depends on tasks assigned to the officer in each specific case.

User Authentication

With NetIQ Advanced Authentication Framework, user authentication process includes the following steps:

1. When authentication is required, the logon window is displayed and the user is prompted to submit an [authenticator](#).
2. Authenticore Server receives information about the current authenticator, retrieves the reference authenticator from the Active Directory database and compares both.
3. When the authenticators match, the user's identity is successfully proven.

NetIQ Advanced Authentication Framework Components Description

Server Components:

- **Authenticore server** is intended for processing NetIQ Advanced Authentication Framework users authentication requests.
- **EAP Server** is an Internet Engineering Task Force (IETF) standard that provides an infrastructure for network access clients and authentication servers to host plug-in modules for current and future authentication methods.
- **Log Server** is a separate computer/server which is intended for storing data on events occurred on Authenticore servers.
- **Network Policy Server (NPS) Plugin** adds Authentication to the Microsoft Network Policy Server. It allows authenticating with any RADIUS compliant client using OATH OTP authenticator to NetIQ.
- **Password Filter** installation is an obligatory step of NetIQ Advanced Authentication Framework system installation. Password filter guarantees passwords synchronization independently of the methods and means used for their change.
- **Web Service** is a component that allows people to be authenticated in domain from outside the domain using their own authenticators.

Administrator Components:

- Extension of standard Active Directory Users and Computers (ADUC) MMC console.
- MMC snap-in for viewing NetIQ Advanced Authentication Framework users properties (NetIQ Advanced Authentication Framework User Viewer).
- Administrative templates of security policies.
- Wizard of rights delegation for working with NetIQ Advanced Authentication Framework tab.
- Administrator's Manual.

Client Components:

- **Client.** The installation runs on the user workstation and replaces the standard Windows login with an NetIQ Advanced Authentication Framework.
- **RTE (Runtime Environment)** – a set of components used by NetIQ Advanced Authentication Framework SDK and NetIQ Advanced Authentication Framework Client modules. In case of NetIQ Advanced Authentication Framework, Runtime Environment does not require separate installation.

Add- ons (authentication providers modules installation is intended to install different NetIQ Advanced Authentication Framework system authentication provider modules within the given package:

- BIO-key authentication provider.
- Flash+PIN authentication provider.
- Universal Card authentication provider.
- Lumidigm authentication provider.
- OATH authentication provider.
- RADIUS authentication provider.

Service Accounts and Groups

When you install Authenticore Server for the first time, the following groups and accounts are created:

- **AuthenticoreService** – a mandatory domain account used by Authenticore Server. AuthenticoreService is a member of the Domain Users, Domain Admins and Enterprise Admins groups and is given a batch logon privilege on each Authenticore Server.
- **Authenticore Admins** – a domain group of users able to install and configure Authenticore Servers on any of the Windows Server family domain computers. By default, the group includes the following predefined system groups of the users: Domain Admins and Enterprise Admins. If the administrator is not a member of the Authenticore Admins group, he/she will not be able to install and set up Authenticore Server.
- **Authenticore Servers** – a domain group, which lists all Authenticore Servers installed in the domain. A new computer is automatically added to Authenticore Servers group when “NetIQ Advanced Authentication Framework - Authenticore Server” package is installed.
- **NetIQ Advanced Authentication Framework Admins** – a domain group of users, which can be given control over NetIQ Advanced Authentication Framework user and computer settings. In this case all you need to do to delegate control to a new user is add them to NetIQ Advanced Authentication Framework Admins group. By default, NetIQ Advanced Authentication Framework Admins group contains Domain Admins group, members of which have pre-given control over NetIQ Advanced Authentication Framework setting. For other users, which are not members of NetIQ Advanced Authentication Framework Admins or Domain Admins group, control over NetIQ Advanced Authentication Framework settings is given manually (see [Delegating Control](#)).
- **NetIQ Advanced Authentication Framework ADAM Servers** – a domain group that contains servers with installed Active Directory Lightweight Directory Services (AD LDS) or Active Directory Application Mode (ADAM) Servers. This group is only exists in configurations with extended ADAM/AD LDS schema.

Administrative Tools

The system administrator can use both standard and specific administrative tools to manage NetIQ Advanced Authentication Framework system. The standard administrative tools are "Active Directory Users and Computers" MMC snap-in, Event Viewer MMC snap-in. The specific administrative tools are installed in "NetIQ Advanced Authentication Framework – Administrative Tools" package on the system administrator's workstation.

The "NetIQ Advanced Authentication Framework – Administrative Tools" package contains:

- **Active Directory Users and Computers MMC Snap-in**

Active Directory Users and Computers MMC snap-in (ADUC) allows a system administrator to:

- work with users' accounts (create, edit, remove users, reset user account passwords). For details see chapter [Working with User Accounts](#);
- enable and disable the caching of NetIQ Advanced Authentication Framework credentials on a local computer. For details see chapter [Allowing to Cache Authenticators](#);
- add group policy templates and configure the policies. For details see chapter [Group Policies](#);
- delegate control. For details see chapter [Delegating Control](#).

- **NetIQ Advanced Authentication Framework User Viewer MMC Snap-in**

NetIQ Advanced Authentication Framework User Viewer is a standalone MMC snap-in allowing you to view the list of all domain users, check which logon methods they use, track their logon/-logoff time, view and edit their account properties.

Active Directory Users and Computers

Working with User Accounts

The ADUC MMC snap-in allows you to perform the following operations with user accounts:

- **Create a new user** with the help of the enhanced User Creation Wizard. The Wizard allows you to create a NetIQ Advanced Authentication Framework user and enroll authenticators for him/her while creating an Active Directory user account.
- **Edit NetIQ Advanced Authentication Framework users' properties.** A number of NetIQ Advanced Authentication Framework settings are available on the same-name tab in the user properties dialog. You can allow or forbid the use of authenticators, set up random password generation, and more.
- **Remove user account.** You can delete a NetIQ Advanced Authentication Framework user (that is, forbid an Active Directory user to use authenticators) or delete an Active Directory user account. When you withdraw the permission to use authenticators from a user, his/her authenticators are lost. When you remove an Active Directory account, all NetIQ Advanced Authentication Framework user attributes are cleared.



It is highly recommended that before deleting an Active Directory user, you should first disable NetIQ user settings.

- **Reset Active Directory passwords.** Resetting password is required in case a NetIQ Advanced Authentication Framework user has removed the only authenticator and cannot log on with password because it was changed for a random one. Resetting Active Directory password allows the user to log on again and enroll a new authenticator. When the password is reset for the user with existing authenticators, the authenticators are lost. Other user settings on the NetIQ Advanced Authentication Framework tab retain their current state.

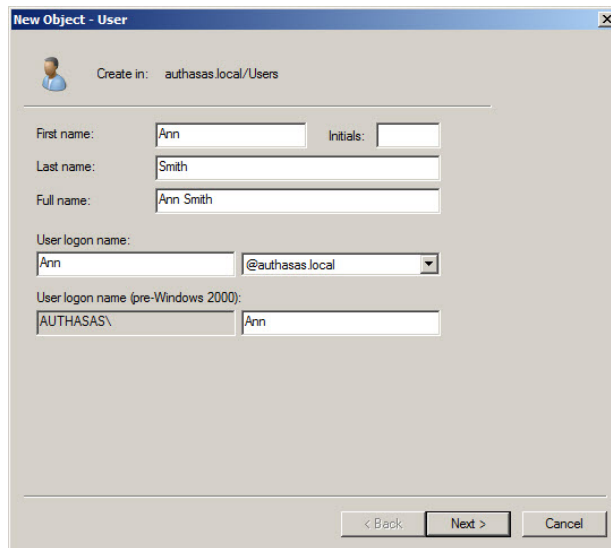
Creating New User

The enhanced User Creation Wizard allows you to create an NetIQ Advanced Authentication Framework user and enroll authenticators for them while creating an Active Directory user account.

 The maximum number of NetIQ Advanced Authentication Framework users in a domain is limited by the user license.

To create a new user

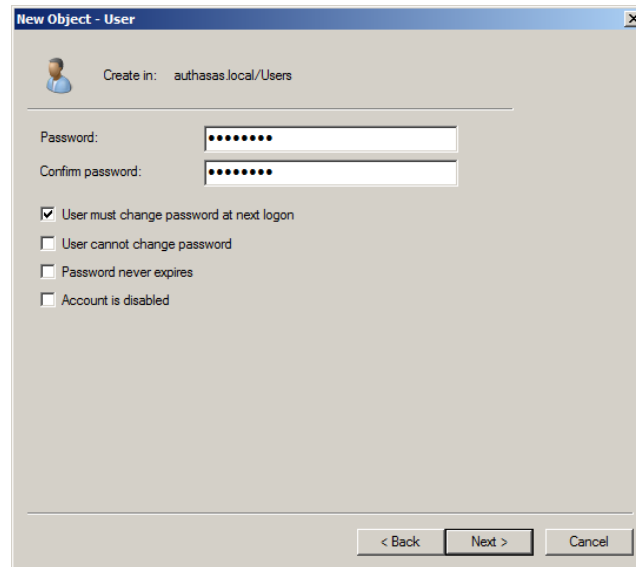
1. In **Active Directory Users and Computers**, select an Organizational Unit/container.
2. Click  toolbar button or right-click the container and select **New > User** or click **Action** and select **New > User**.
3. The User Creation Wizard opens.



The image shows a screenshot of the 'New Object - User' dialog box in Active Directory Users and Computers. The dialog box has a title bar with 'New Object - User' and a close button. Inside, there is a 'Create in:' field showing 'authasas.local/Users'. Below this are several input fields: 'First name:' with 'Ann', 'Initials:' (empty), 'Last name:' with 'Smith', 'Full name:' with 'Ann Smith', 'User login name:' with 'Ann' and a dropdown menu showing '@authasas.local', and 'User login name (pre-Windows 2000):' with 'AUTHASAS\Ann'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter user name and click **Next >**.

4. Enter password for the user and click **Next**.



New Object - User

Create in: authasas.local/Users

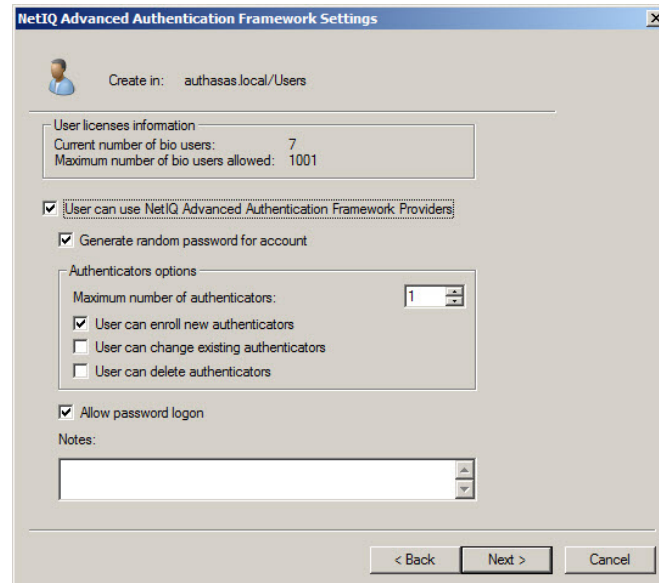
Password: [masked]
 Confirm password: [masked]

☒ User must change password at next logon
☐ User cannot change password
☐ Password never expires
☐ Account is disabled

< Back Next > Cancel

✖ The following steps (5-6) do not appear in the situation when you use AD attributes, because we should modify schema to have these features.

5. The following page contains NetIQ Advanced Authentication Framework settings. If you would like to create a plain Active Directory user, skip this step.



NetIQ Advanced Authentication Framework Settings

Create in: authasas.local/Users

User licenses information
 Current number of bio users: 7
 Maximum number of bio users allowed: 1001

☒ User can use NetIQ Advanced Authentication Framework Providers
☒ Generate random password for account

Authenticators options
 Maximum number of authenticators: 1
☒ User can enroll new authenticators
☐ User can change existing authenticators
☐ User can delete authenticators

☒ Allow password logon

Notes:
 [text area]

< Back Next > Cancel

- **User licenses information** field displays the current number of NetIQ Advanced Authentication Framework users and the limit stated in the user license.

- **The User can use hardware authentication devices** box, if checked, enables the user to use authenticators (in other words, an NetIQ Advanced Authentication Framework user is created).

- The **Generate random password for account** box, if checked, enables random password generation.
- The **Authenticators options** allow you to set the maximum number of authenticators for the user and define how user can manage his/her authenticators.
 - The Maximum number of authenticators setting allows you to set the limit to the number of authenticators the user can have (by default equals to 1).
 - The **User can enroll new authenticators** box, if checked, enables the user to add authenticators.
 - The **User can change existing authenticators** box, if checked, enables the user to re-enroll authenticators.
 - The **User can delete authenticators** box, if checked, enables the user to remove authenticators.
- In the **Notes** box, you can enter a comment to the user's account. When the settings are done, click **Next** to continue.

6. From **User authenticators** page, you can enroll authenticators for the user. This page also allows you to manage enrolled authenticators if any is available (see [Managing Authenticators](#)).

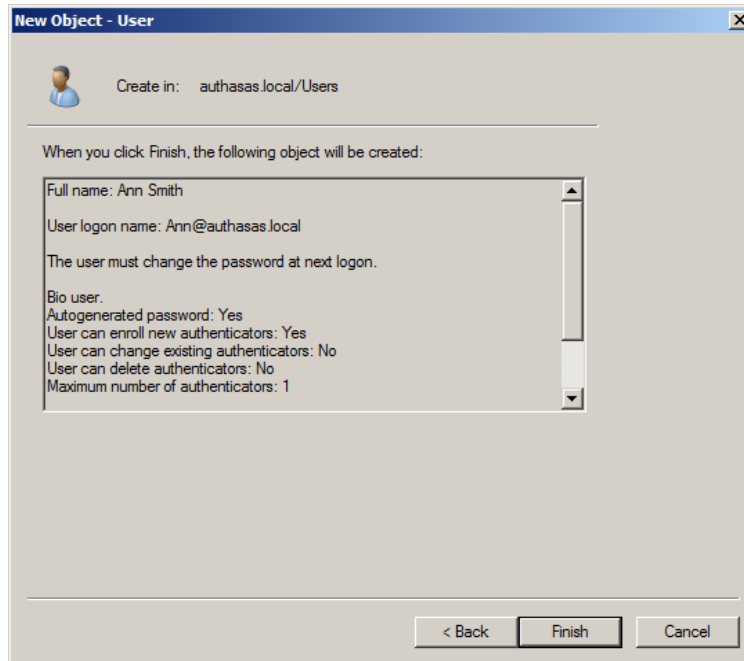
Comment	Type

Do one of the following:

- To start enrolling an authenticator, click **Enroll...** (see [Enrolling Authenticator](#)).

b) To continue without authenticator enrollment, click **Next**.

7. Check the summary of changes you have made. Click **Finish**.



Enrolling Authenticator

To enroll authenticator from **User Creation Wizard**:

1. On **User authenticators** page, click **Enroll....**
2. The Enroll Authenticator window is displayed.



- From the **Type** list, select the required type.
 - Click **Enroll....**
3. You are shown the authentication device screen with instructions to follow, which depend on selected authentication type. Follow the instructions to enroll authenticator.
-  For the selected component to function, the authentication provider must have been preliminary installed.
4. After successful enrollment you can add a comment to authenticator (if allowed by the system administrator).

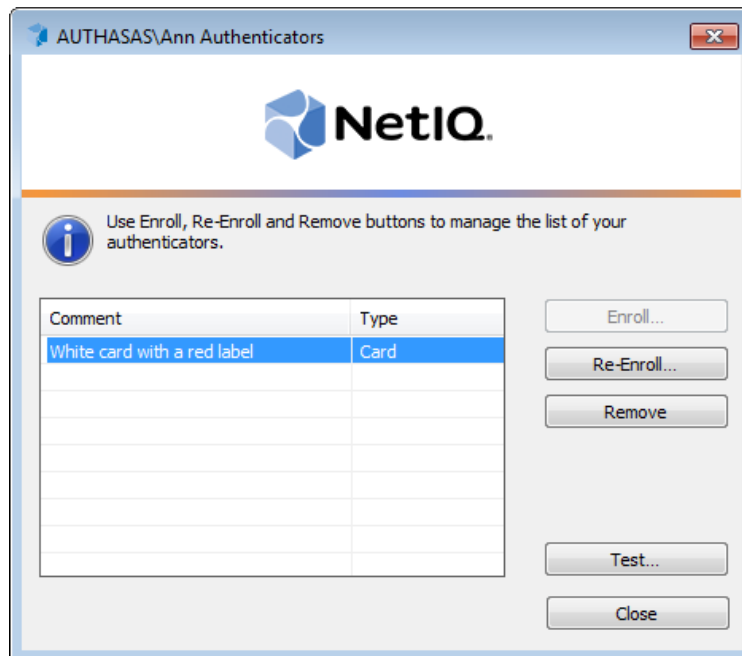


The 'Enroll Authenticator' dialog box features the NetIQ logo at the top. Below the logo, there is a 'Type:' label followed by a dropdown menu currently set to 'Card'. To the right of the dropdown is an 'Enroll...' button. Below the 'Type:' section is a 'Comment:' label followed by a text input field containing the text 'White card with a red label'. To the right of the text field are 'Save' and 'Cancel' buttons.

After that you can test authenticator by clicking **Test** (see [Testing Authenticator](#)).

5. Save authenticator by clicking **Save**.

When authenticator is enrolled, a '*Comment – Authenticator type*' record appears on **User authenticators** page (comment is editable if allowed by the system administrator).



The 'AUTHASAS\Ann Authenticators' window displays the NetIQ logo and an information icon with the text: 'Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.' Below this is a table with two columns: 'Comment' and 'Type'. The first row is highlighted in blue and contains the text 'White card with a red label' and 'Card'. To the right of the table are buttons for 'Enroll...', 'Re-Enroll...', 'Remove', 'Test...', and 'Close'.

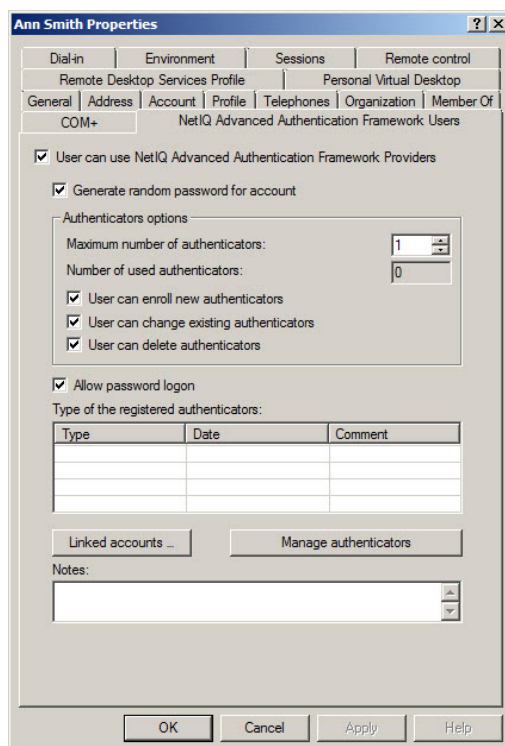
Comment	Type
White card with a red label	Card

Editing NetIQ Advanced Authentication Framework User Properties

 NetIQ Advanced Authentication Framework user properties are available for editing only for administrators with necessary privileges. These privileges can be delegated within an Organizational Unit/container (see [Delegating Control](#)).

To change NetIQ Advanced Authentication Framework user properties:

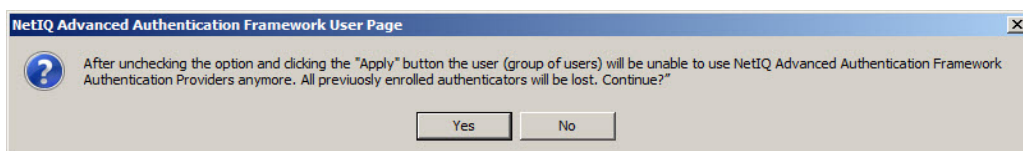
1. In **Active Directory Users and Computers**, select the user and open the properties dialog.
2. In the properties dialog, switch to the **NetIQ Users** tab.



The screenshot shows the 'Ann Smith Properties' dialog box with the 'NetIQ Advanced Authentication Framework Users' tab selected. The 'User can use NetIQ Advanced Authentication Framework Providers' checkbox is checked. Below it, the 'Generate random password for account' checkbox is also checked. The 'Authenticators options' section contains a 'Maximum number of authenticators' spinner set to 1, a 'Number of used authenticators' spinner set to 0, and three checked checkboxes: 'User can enroll new authenticators', 'User can change existing authenticators', and 'User can delete authenticators'. The 'Allow password logon' checkbox is checked. Below this is a table for 'Type of the registered authenticators' with columns 'Type', 'Date', and 'Comment'. At the bottom are buttons for 'Linked accounts ...', 'Manage authenticators', and a 'Notes' text area. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the very bottom.

The following settings are available:

- The **User can use NetIQ Authentication Providers** box, if checked, enables the user to use authenticators. When you uncheck the box, the following dialog is displayed:



The screenshot shows a warning dialog box titled 'NetIQ Advanced Authentication Framework User Page'. It contains a question mark icon and the text: 'After unchecking the option and clicking the "Apply" button the user (group of users) will be unable to use NetIQ Advanced Authentication Framework Authentication Providers anymore. All previously enrolled authenticators will be lost. Continue?'. At the bottom are 'Yes' and 'No' buttons.

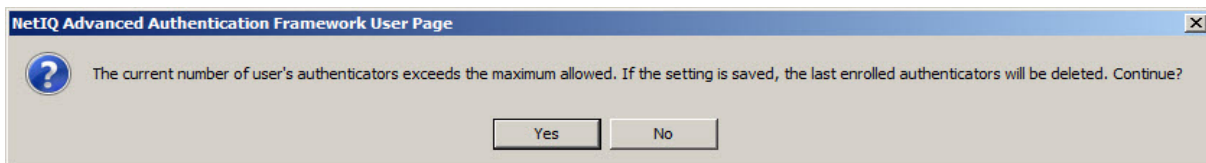
! If you uncheck the box and save the changes, the user loses his/her authenticators and will be able to log on with password only. If random password generation was set up and activated for this user, the user will be completely unable to log on after losing authenticators. In such case you have to reset Active Directory password for the user, so that he/she is able to log on and enroll a new authenticator.

- The **Generate random password for account** box, if checked, enables random password generation.

- The **Authenticators options** allow you to change the maximum number of authenticators for the user and define how user can manage his/her authenticators.

- The Maximum number of authenticators setting allows you to set the limit to the number of authenticators the user can have. The Number of used authenticators box displays the number of existing authenticators (read-only).
- The User can enroll new authenticators box, if checked, enables the user to add authenticators.
- The User can change existing authenticators box, if checked, enables the user to re-enroll authenticators.
- The User can delete authenticators box, if checked, enables the user to remove authenticators.

! If you set **Maximum number of authenticators** at lesser value than Number of used authenticators and save the changes, the following dialog opens:



Clicking Yes removes the most recent authenticators. For example, if the **Number of used authenticators** is 3 and the **Maximum number of authenticators** is set to 1, two most recent authenticators are removed.

- The **Type of registered authenticators** grid displays information about existing authenticators. The grid contains the following columns:

- Type – authenticator type;
- Date – date when the authenticator was enrolled;
- Comment – comment added to authenticator at enrollment.

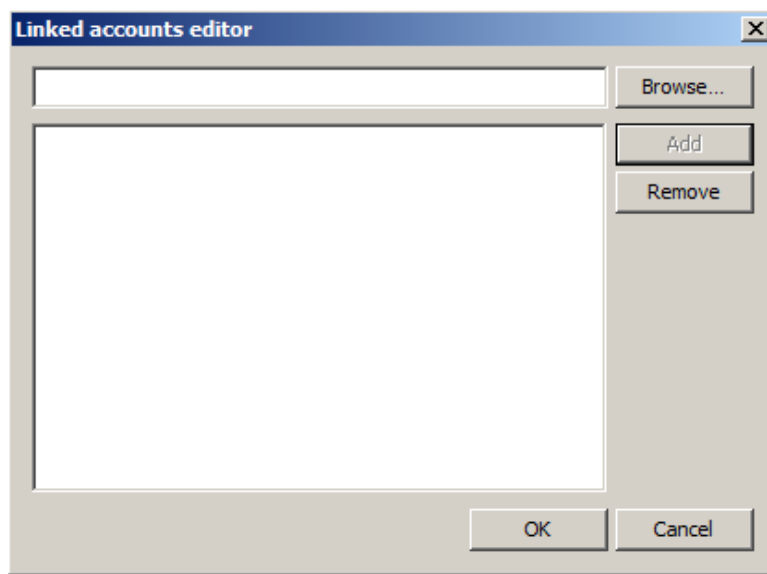
- The **Manage authenticators** button allows you to open the **Authenticators** window (see [Managing Authenticators](#)).
- The **Notes** box allows you to edit a comment to the user's account. The tab also displays the following read-only details:
 - last logon time;
 - last password change time.

Linked Accounts

When using linked accounts you are able to logon to the system as another user, who is linked to you. To logon you will use your own authenticators.

To link accounts

1. On the **NetIQ Users** tab, click **Linked Accounts....**
2. The **Linked accounts editor** window is displayed.



3. To choose a user, click **Browse....**
4. In the **Select User** window, type the name of the user you want to be linked with. Press **Check Names** to double check if you've typed the name correctly. Click **OK**.

Select User

Select this object type:
 Object Types...

From this location:
 Locations...

Enter the object name to select (examples):
 Check Names

Advanced... OK Cancel

i If you are not sure or don't know the user name, click the **Advanced** button to use a search engine:

Select User

Select this object type:
 Object Types...

From this location:
 Locations...

Common Queries

Name: Starts with Columns...

Description: Starts with Find Now

☐ Disabled accounts Stop

☐ Non expiring password

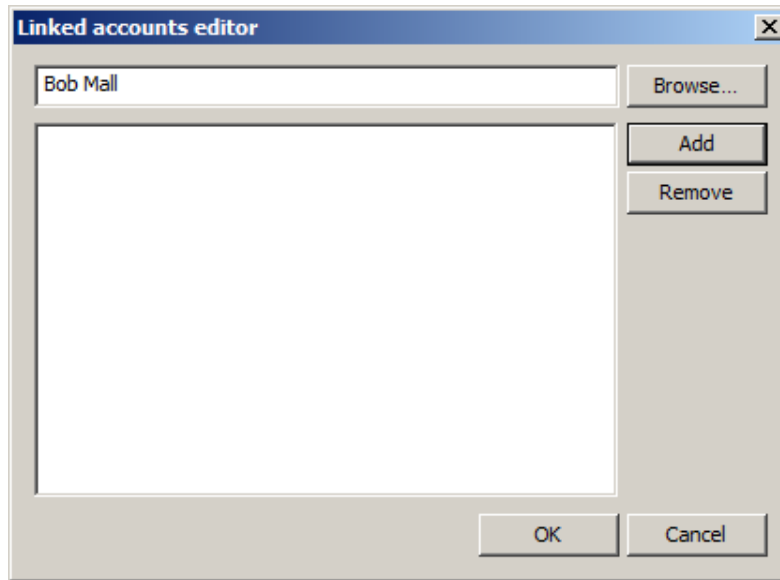
Days since last logon:

OK Cancel

Search results:

Name (RDN)	E-Mail Address	In Folder

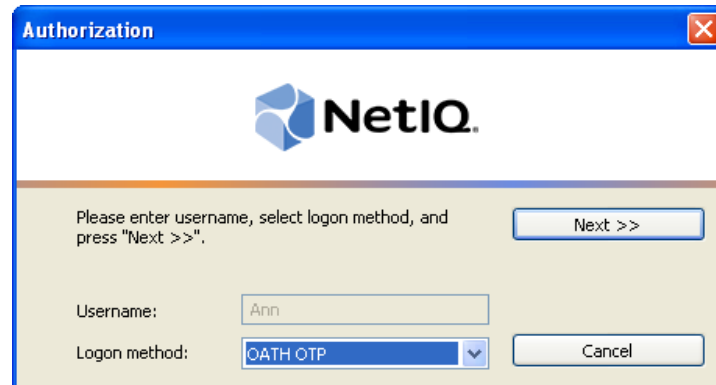
5. After the username appears in the **Linked accounts editor** window, click **Add** and **OK**.



Managing Authenticators

To manage user's authenticators

1. On the **NetIQ Users** tab, click **Manage authenticators**.
2. The **Authorization** window is displayed.



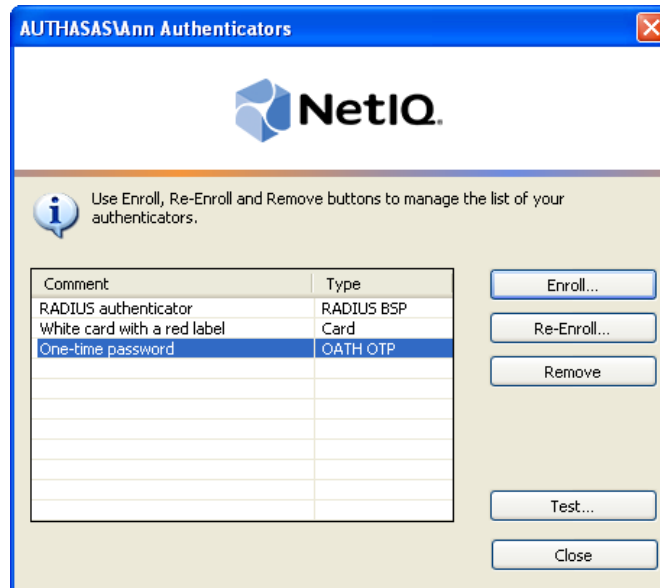
User name and domain name cannot be changed.

- Select a logon method (an authenticator type or Logon by password).
- **Click Next >>.**

 To be able to add, re-enroll or remove an authenticator, you must use an authenticator as logon method.

 To be able to test an authenticator, you may use either authenticator or password as logon method.

3. After successful authentication the **Authenticators** window is displayed.

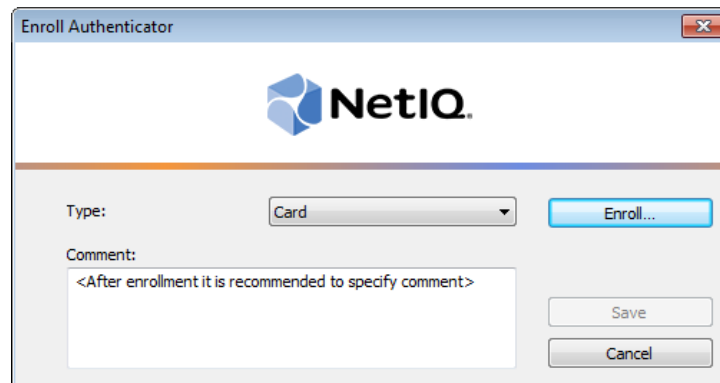


- i** If there are no enrolled authenticators yet, only the **Enroll** button will be active (no matter which way you were authorized).
- i** If some authenticators already exist and you were authenticated with a password, all the buttons except **Test** and **Close** are greyed out.

Adding Authenticator

To add an authenticator

1. In the **Authenticators** window, click **Enroll...**
2. The **Enroll Authenticator** window opens.



- From the **Type** list, select an authenticator type.
 - Click **Enroll...**
3. You are shown the authentication device screen with instructions to follow, which depend on selected authentication type. Follow the instructions to enroll authenticator.
 4. After successful enrollment you can add a comment to authenticator (if allowed by the system administrator).



After that you can test authenticator by clicking **Test** (see [Testing Authenticator](#)).

5. Save authenticator by clicking **Save**.

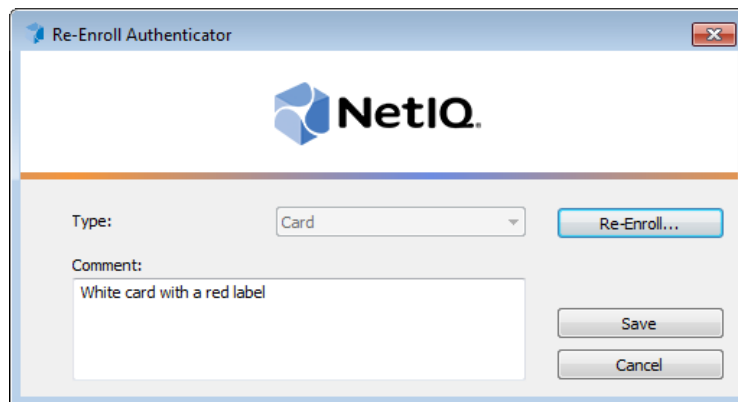
When authenticator is enrolled, a '*Comment – Authenticator type*' record appears on User authenticators page (comment is editable if allowed by the system administrator).

Re-enrolling Authenticator

 If you need to edit a comment only, you do not need to go through re-enrollment procedure. To edit a comment, select it in the **Authenticators** window and click to enter a new or comment or just press **[F2]**.

To re-enroll an authenticator

1. In the **Authenticators** window, select the record and click **Re-enroll**.
2. The **Re-enroll Authenticator** window opens.



Click **Re-Enroll....**

3. You are shown the authentication device screen with instructions to follow, which depend on selected authentication type. Follow the instructions to re-enroll authenticator.

4. After successful re-enrollment you can edit the comment (if allowed by the system administrator).

Once authenticator is successfully enrolled you can test authenticator, by clicking the **Test** button (see [Testing Authenticator](#)).

5. Click **Save**. A '*Comment – Authenticator type*' record appears in the **Authenticators** window (comment is editable if allowed by the system administrator).

Testing Authenticator

To test an authenticator

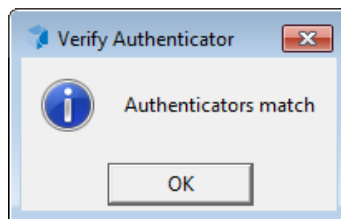
1. In the **Authenticators** window, select the record and click Test.

Testing can also be performed in the **Enroll authenticator** and **Re-enroll authenticator** windows.

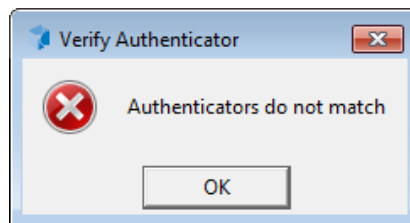
2. You are shown the authentication device screen with instructions to follow, which depend on device type. Follow the instructions to test authenticator.

3. After authentication is completed you receive one of the following messages

- a) if test passed:



- b) if test failed:



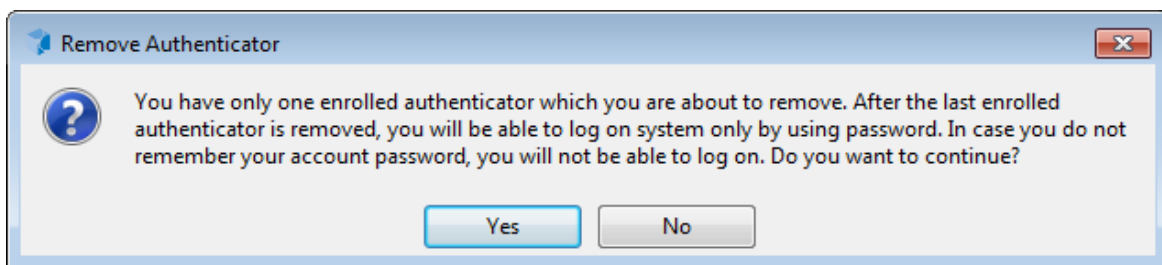
If test failed, the authentication device screen is shown again. Repeat the procedure or click Cancel and re-enroll the authenticator.

Removing Authenticator

! Be careful while removing authenticators. Do not remove all authenticators if random password generation is set up and activated for the user.

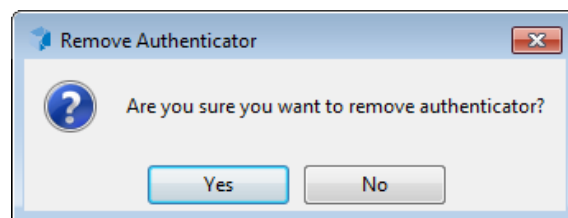
If the user has no authenticators, he/she will be completely unable to log on.

The system prevents you from accidentally removing the only authenticator by displaying the following dialog:



To remove an authenticator

1. In the **Authenticators** window, select the record and click **Remove**.
2. The following dialog is displayed:

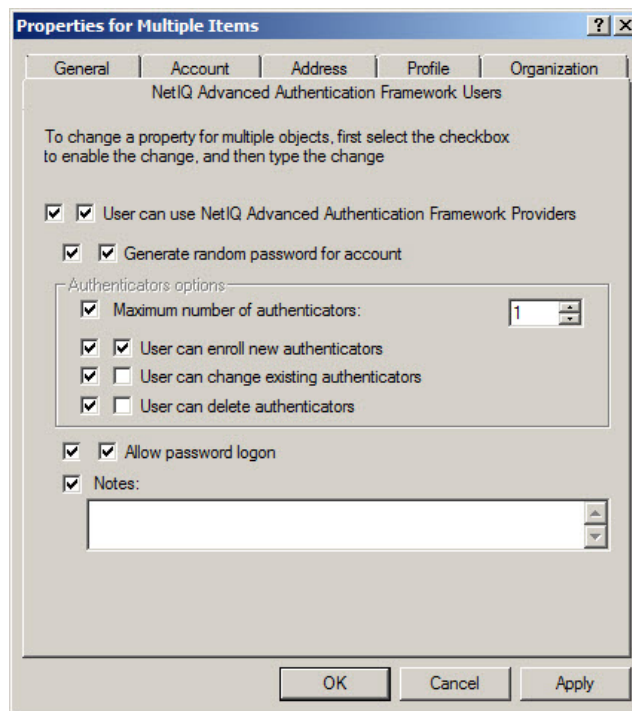


Click **Yes**.

Editing Properties of Multiple NetIQ Advanced Authentication Framework Users

To edit properties of multiple users:

1. Hold down [Ctrl] and select the users.
2. Open the properties dialog. In the Properties for Multiple Items dialog, switch to the NetIQ Users tab.
3. The NetIQ Users tab for multiple items contains all NetIQ Advanced Authentication Framework settings except the **Manage authenticators** button. The settings become available for editing when the twin check boxes are checked.



You can also edit multiple users if they belong to one organization unit or group:

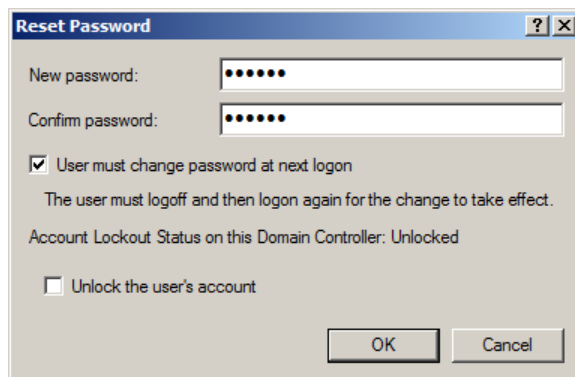
1. Right-click the required Organization Unit or group.
2. Select **Properties**, switch to the **NetIQ Users** tab.
3. Make necessary changes and save the changes by clicking **Apply**.

Resetting Active Directory Password

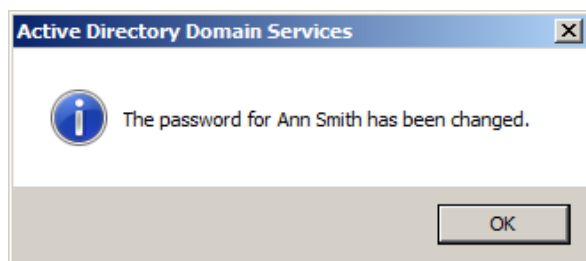
If an NetIQ Advanced Authentication Framework user is allowed to remove authenticators, it may happen that he/she removes all authenticators and will be unable log on with password because it was changed. The user may also lose his/her hardware authenticator or it may be stolen from him/her. Resetting Active Directory password allows the user to log on again and enroll a new authenticator.

i If you check the **User must change password at next logon** box, the user will be prompted to change the password manually at next logon or a random password will be generated for the user account (if random password generation has been activated).

i In Microsoft Windows Server 2008/2008 R2 the **Reset Password** dialog slightly differs. It has **Unlock user's account** checkbox. If you check this option, the user's account will be unlocked if it was previously locked:



If the password is changed successfully, you receive the following message:



The next time a user will logon using an existing Authenticator a popup message will appear explaining the user the domain password has been reset. If the user didn't request a password reset he knows his account has been compromised.



When the user selects Do not show again the message will not appear until an administrator resets the password for the user account again.

Removing User

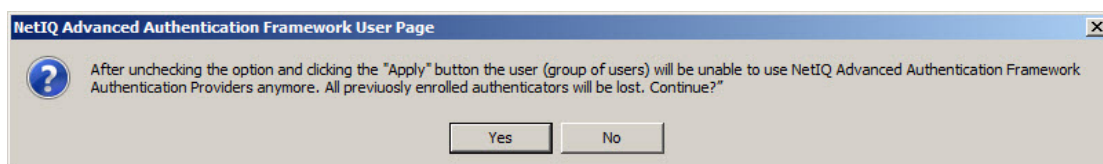
You can remove an NetIQ Advanced Authentication Framework user (that is, forbid an Active Directory user to use NetIQ Advanced Authentication Framework authenticators) or remove an Active Directory user account. When you withdraw the permission to use authenticators from a user, existing authenticators are lost. When you remove the Active Directory account, it is removed with all user attributes.

! Before removing an Active Directory user the system administrator has to uncheck the **User can use hardware authentication devices** option in order to have a free license. Otherwise, the license will be invalid.

Removing a NetIQ Advanced Authentication Framework User

To delete an NetIQ Advanced Authentication Framework user

1. In **ADUC**, double-click the user name.
2. The **Properties** dialog opens. Switch to the **NetIQ Users** tab.
3. Uncheck the **User can use NetIQ Authentication Providers** box.
4. The following dialog is displayed:



- Click **Yes**.
- Click **Apply** on the **NetIQ Users** tab.

! If you uncheck the box and save the changes, the user loses his/her authenticators and will be able to log on with password only. If random password generation was set up and activated for this user, the user will be completely unable to log on after losing authenticators. In such case you have to reset the password for the user.

✖ The number of NetIQ Advanced Authentication Framework users is re-counted every time the **User can use NetIQ Authentication Providers** option is unchecked.

Delegating Control

i Delegating control option doesn't work for AD LDS/ADAM configurations.

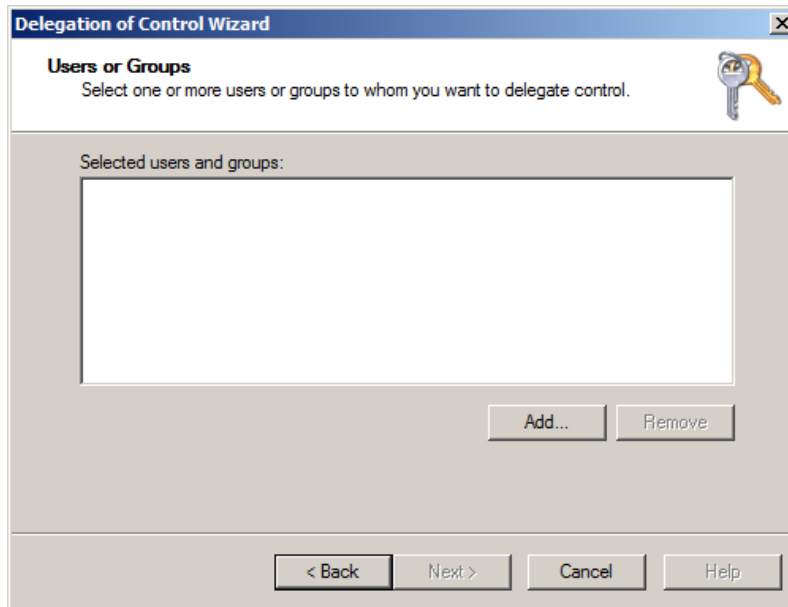
Delegating control means giving control over NetIQ Advanced Authentication Framework settings to a user or a group of users within a container/Organizational Unit.

To delegate control

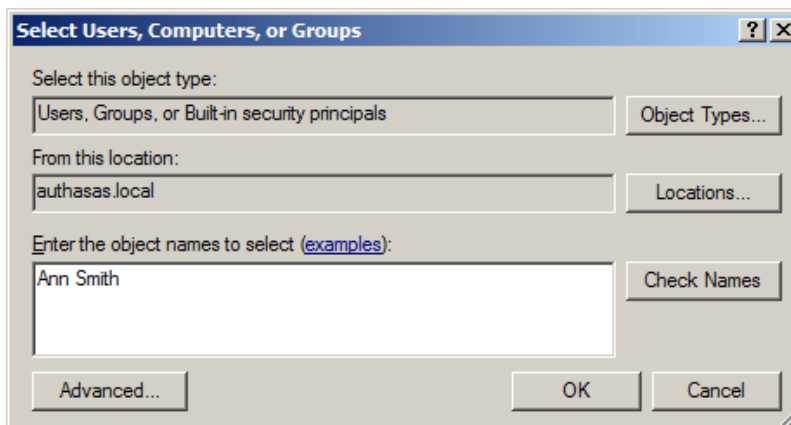
1. Right-click the container/organizational unit and select **Delegate Control**.
2. The **Delegation Wizard** is started. Click **Next >** to continue.



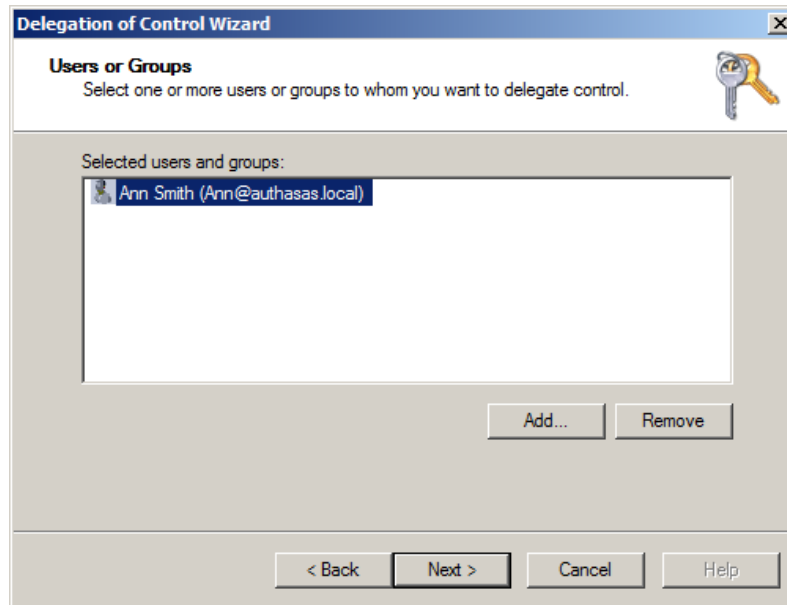
3. Click **Add**.



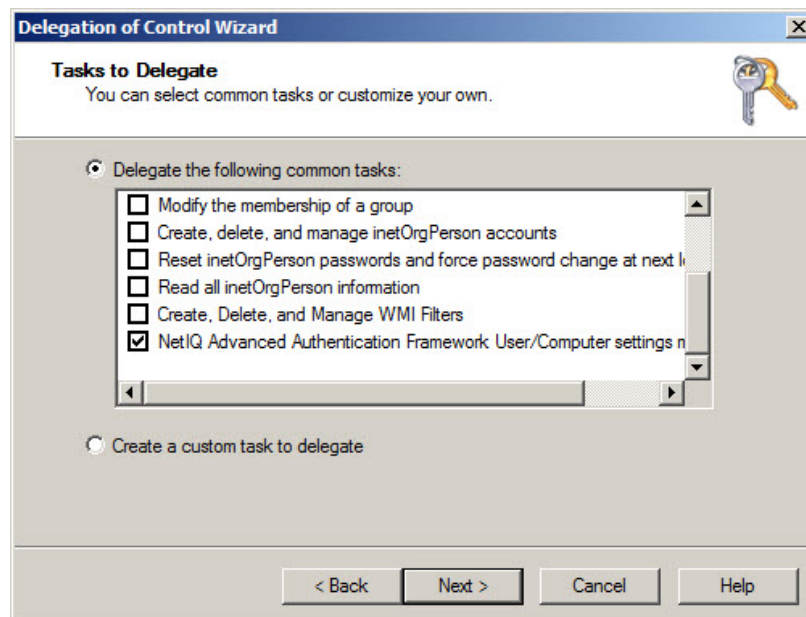
4. Enter the name of a user/group and click **OK**.



5. The name of selected user/group is displayed on the **Users or Groups** page. Click **Next>** to continue.



6. Check the **NetIQ Advanced Authentication Framework User/Computer settings management** box. Click **Next>** to continue.



7. Click **Finish** to exit the **Delegation Wizard**.



Now the user/the group of users are allowed to edit settings on **NetIQ Advanced Authentication Framework** tab within the specified container (organizational unit). To change NetIQ Advanced Authentication Framework settings, you can use either [Active Directory Users and Computers](#) or [NetIQ Advanced Authentication Framework User Viewer](#) snap-in.

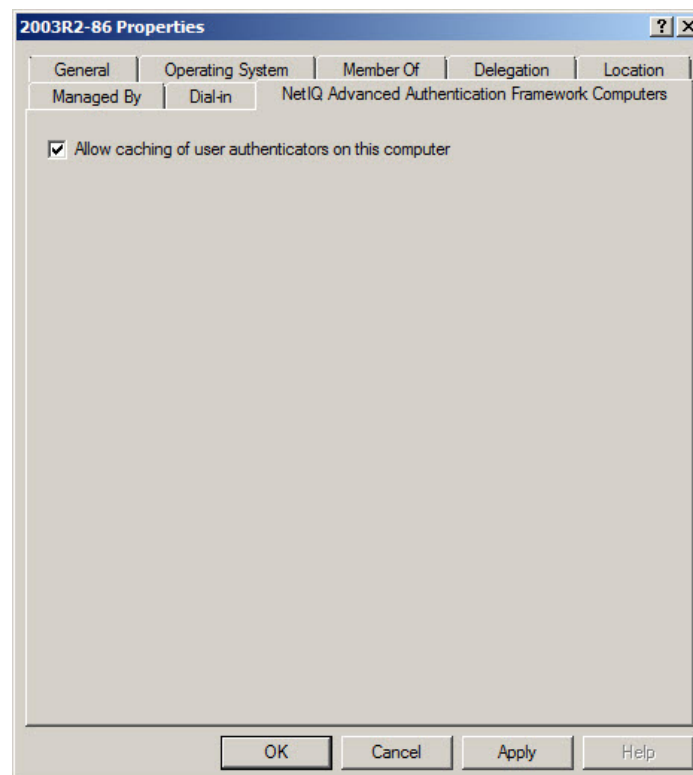
Allowing to Cache Authenticators

The **NetIQ Advanced Authentication Framework** tab is available both on user and computer properties pages. In computers, this tab contains a single setting, which allows an NetIQ Advanced Authentication Framework user to cache authenticators on the local computer.

! Caching refreshes on authentication. If a user has had an authenticator cached and then re-enrolled it, he/she must re-login using the new authenticator while connected to the network. **If connection is terminated after logoff, the user will be unable to log on with the re-enrolled authenticator.**

To allow users to cache authenticators

1. In **Active Directory Users and Computers**, select the computer and open the properties dialog.
2. In the properties dialog, switch to the **NetIQ Computers** tab.



3. Check the **Allow caching of user authenticators on this computer** box.

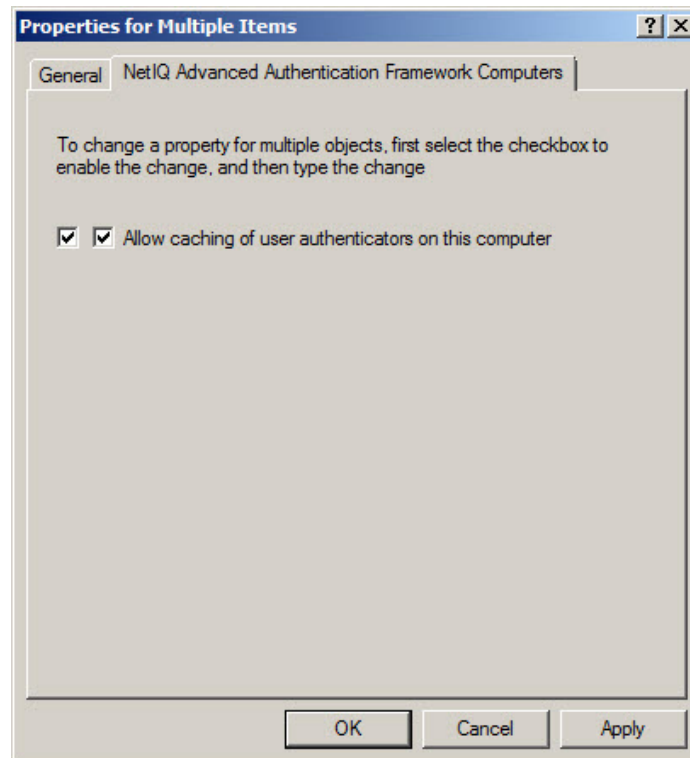
4. Click **Apply**.

 Enabling **Allow caching of user authenticators on this computer** box for particular computer allows also to cache authenticators for RTE, even if NetIQ Advanced Authentication Framework Client component is not installed.

Allowing to Cache Authenticators on Multiple Computers

To allow to cache authenticators on multiple computers

1. Hold down **[Ctrl]** and select the computers.
2. Open the properties dialog. In the **Properties On Multiple Objects** dialog, switch to the **NetIQ Computers** tab.
3. Check the twin box, then check the **Allow caching of user authenticators on this computer** box and click **Apply**.



Automatic logon in NetIQ Advanced Authentication Framework

 The Automatic logon feature is available only in operational systems based on GINA, i.e. Microsoft Windows XP and Microsoft Windows Server 2003.

The Automatic logon feature allows other users to start your computer and to use the account that you establish to automatically log on.

 If you turn on automatic logon, using Windows becomes more convenient. However, using this feature poses a security risk.

Automatic logon is a standard Microsoft feature, which is usually used for kiosks. For more detailed information about Automatic logon and the ways of turning it on/off, see [Microsoft Support page](#).

Automatic logon in joint usage with NetIQ Advanced Authentication Framework slightly differs from the original Microsoft Automatic logon.

To guarantee proper work of Automatic logon in NetIQ Advanced Authentication Framework note that:

- When enabling Automatic logon feature only password can be used as logon method. Therefore, automatic logon is unavailable for user account with random password generation;
- If you want to bypass the automatic logon to log on as a different user, hold down the **[Shift]** key after you log off, or after Windows restarts, or when you unlock PC.

 If **[Ctrl]+[Alt]+[Del]** sequence for logging on to Windows is not disabled, then the **[Shift]** key will work only at Windows restart. Otherwise, you have to disable the **[Ctrl] + [Alt] + [Del]** request at Windows logon.

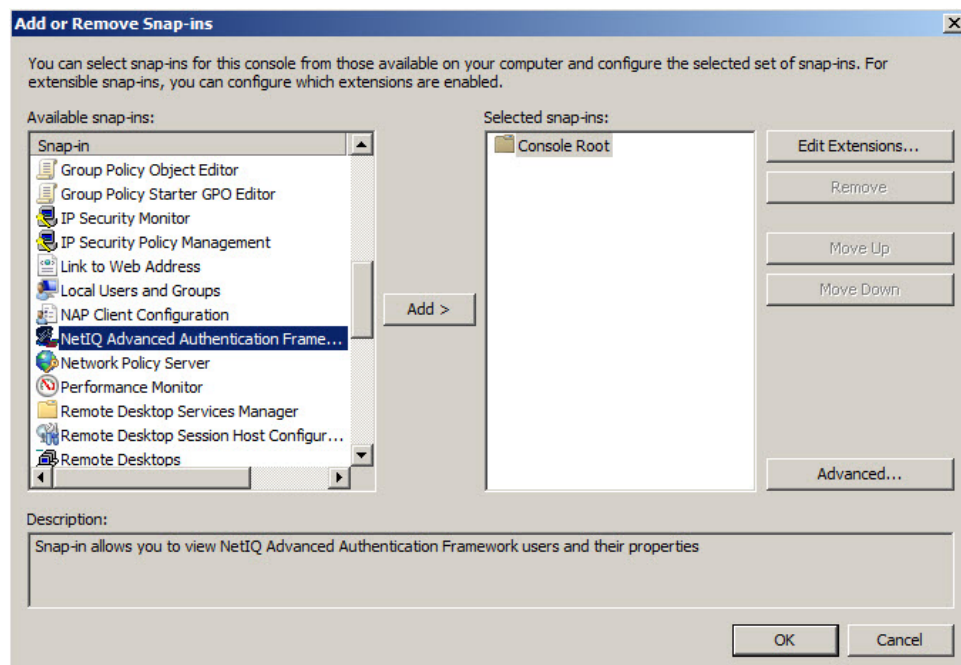
NetIQ Advanced Authentication Framework User Viewer

NetIQ Advanced Authentication Framework User Viewer is a standalone MMC snap-in intended for system administrators and security officers. This tool allows you to view the list of all domain users, check which logon methods they use, track their logon/logoff time, view and edit their account properties.

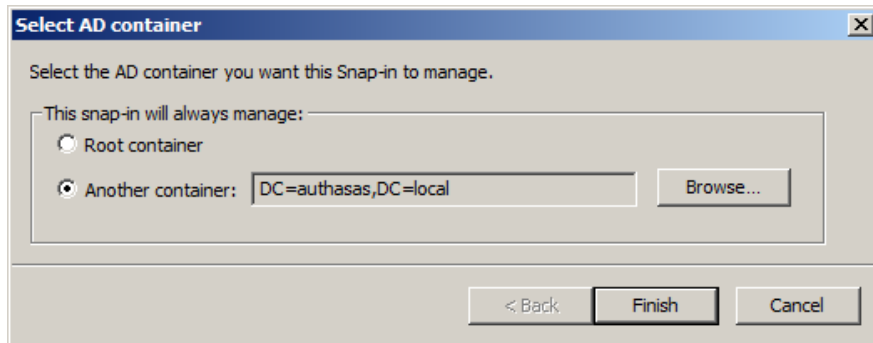
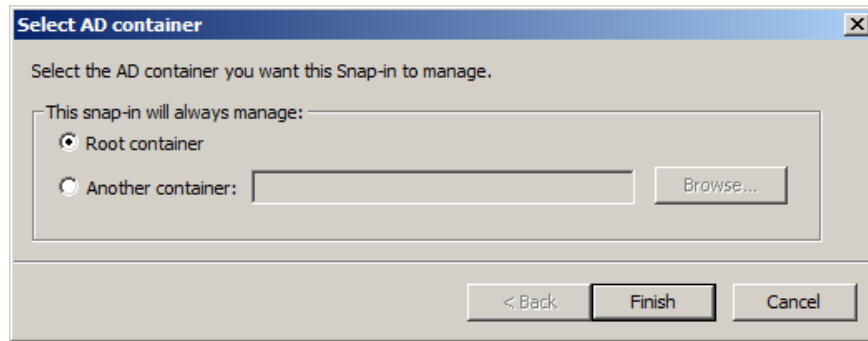
Adding User Viewer to Console

To add NetIQ Advanced Authentication Framework User Viewer to console

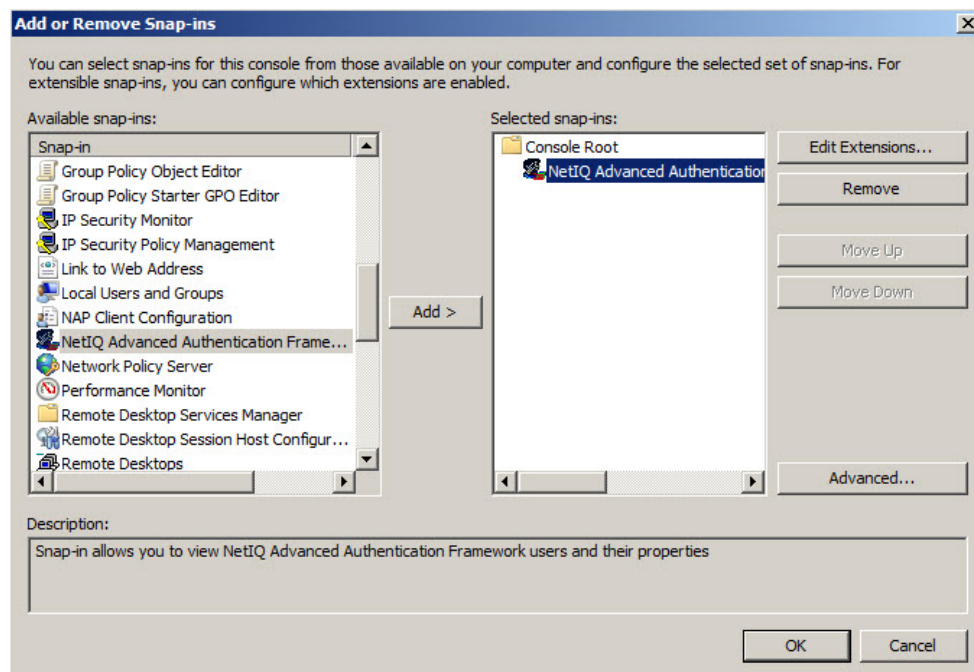
1. Open the MMC console.
2. In the console window, click **File** and select **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog, select **NetIQ Advanced Authentication Framework User Viewer** and click **Add**.



4. Select an Active Directory container to view and click **Finish**. To select a container other than the root one, use the **Browse** button.

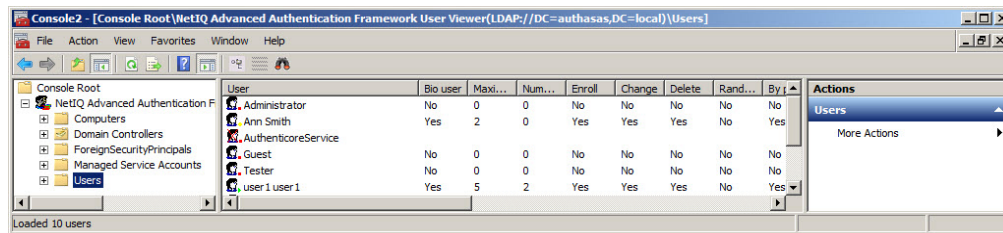


5. **NetIQ Advanced Authentication Framework User Viewer** is now displayed in the **Add or Remove Snap-ins** dialog. Click **OK**.



6. NetIQ Advanced Authentication Framework User Viewer is added to console. Save the console to file.

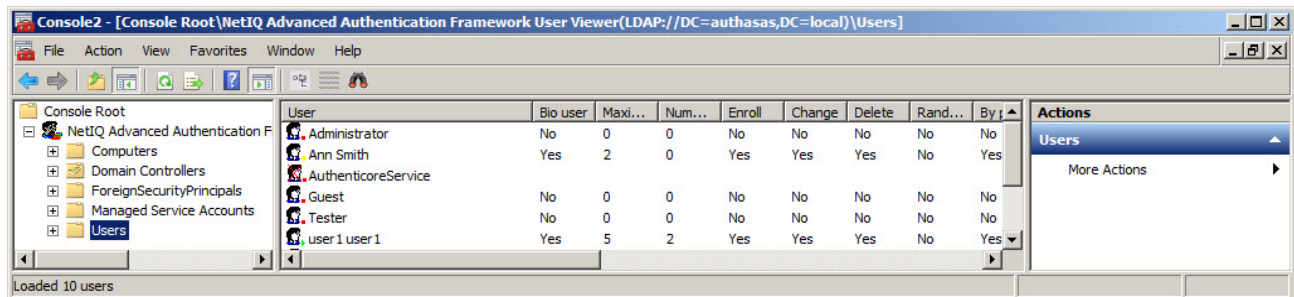
To view the list of users, click  to expand the console tree and select a container. NetIQ Advanced Authentication Framework User Viewer displays the list of users and users' properties.



 The system may have troubles initializing User Viewer saved to .msc file after NetIQ Advanced Authentication Framework™ has been re-installed. To eliminate this problem, add User Viewer to console and save it again.

Visual Appearance

NetIQ Advanced Authentication Framework User Viewer has the same user interface layout as any MMC snap-in:



- The **menu** bar is located at the top of the window. The menu bar allows you to perform standard actions such as saving console to file or customizing the interface layout.
- The **toolbar** is located at the top of the window below the menu bar. The toolbar allows you to perform standard actions such as navigating up and down the console tree, refreshing data on the information pane, or viewing object properties. There are also specific controls:

	Export List	Allows you to export data to file in case you need to analyze them with the help of other applications such as Microsoft Excel.
	Show children	Allows you to display child items (all items belonging to child containers).
	Create methods report	Allows you to view a report about logon methods in use.
	Find User	Allows you to find a certain user.

- The **console tree** is located in the left part of the window. Console tree displays containers.
- The **information panel** is located in the right part of the window. Information pane displays the list of objects (in our case - users) belonging to the selected container and information about them.

The information is divided into the following categories:

- The **“User”** category includes the user account name and an icon. Icons point out details about users’ authenticators:



- user is allowed to use authenticators, has already enrolled at least one authenticator and has used it to log on.



- user is allowed to use authenticators, but has no enrolled authenticators so far.



- user is not allowed to use authenticators.

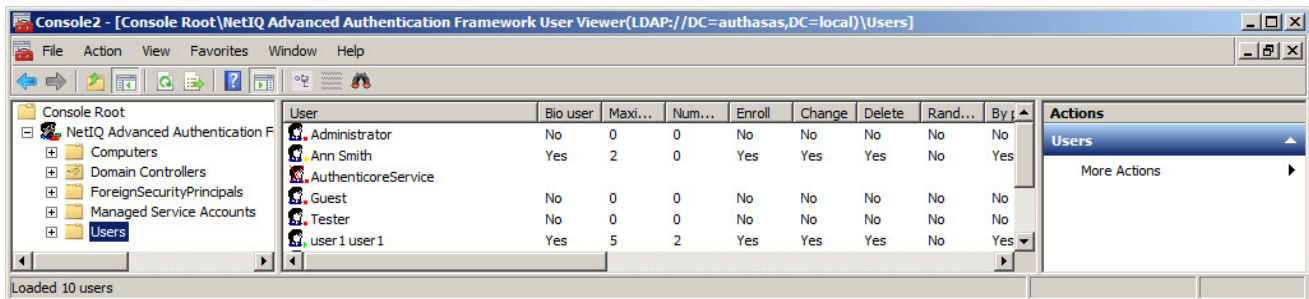


- user account is used for configuring AD, thus access to it is denied.

- The **“NetIQ User”** category shows whether the user is allowed to use NetIQ Authentication Providers or not (Yes/No).
 - The **“Maximum number of authenticators”** displays the maximum number of authenticators the user can have.
 - The **“Number of used authenticators”** category displays the number of existing authenticators.
 - The **“Enroll”** category shows whether the user is allowed to enroll authenticators (Yes/No).
 - The **“Re-enroll”** category shows whether the user is allowed to re-enroll authenticators (Yes/ No).
 - The **“Delete”** category shows whether the user is allowed to remove authenticators (Yes/ No).
 - The **“Random password”** category shows whether random password is set up and activated for the user (Yes/No).
 - The **“Description”** category shows a comment added to the user’s account by a system administrator.
- The **status bar** is located at the bottom of the window. The status bar shows results of actions (for example, the number of users loaded).

Viewing Users

To view users, select a container in the console tree. The list of users belonging to the selected container and information about them are displayed on the information pane. For more information see [Visual Appearance](#) section.



 NetIQ Advanced Authentication Framework User Viewer does not update data automatically.

To update the data, do one of the following:

- click the **Refresh**  toolbar button;
- click **Action** and select **Refresh**.

 You can sort the objects by any category. To do this, click the category name.

Managing User Properties

NetIQ Advanced Authentication Framework User Viewer allows you to change NetIQ Advanced Authentication Framework user properties and manage authenticators.

The procedure of changing user properties in NetIQ Advanced Authentication Framework User Viewer follows the same steps as standard procedure in ADUC. For detailed instruction see Editing NetIQ Authentication Advanced User Properties.

Managing Authenticators

Before you can manage user's authenticators, the system must identify the user. Follow the steps below:

1. In the user **Properties** dialog, click **Manage authenticators**.
2. The **Authorization** window is displayed.



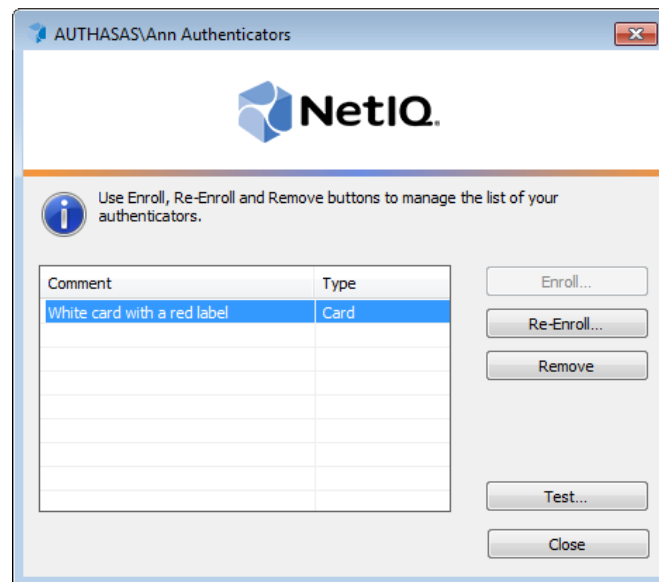
User name and domain name cannot be changed.

- Select a logon method (an authenticator type or **Logon by password**).
- Click **Next**.

 To be able to add, re-enroll or remove an authenticator, you must use an authenticator as logon method.

✖ To be able to test an authenticator, you may use either authenticator or password as logon method.

3. After successful authentication the Authenticators window is displayed.



i If there are no enrolled authenticators yet, only the **Enroll** button will be active (no matter how you were authenticated).

i If authenticators already exist and you were authenticated with a password, all the buttons except **Test** and **Close** are greyed out.

Adding Authenticator

Authenticator enrolling procedure remains the same for every administrative tool. For more details, see [Adding Authenticator](#) chapter at Active Directory Users and Computers.

Re-enrolling Authenticator

 If you need to edit a comment only, you do not need to go through re-enrollment procedure. To edit a comment, select it in the **Authenticators** window and click to enter a new or comment or just press **[F2]**.

Authenticator re-enrolling procedure remains the same for every administrative tool. For more details, see [Re-enrolling Authenticator](#) chapter at Active Directory Users and Computers.

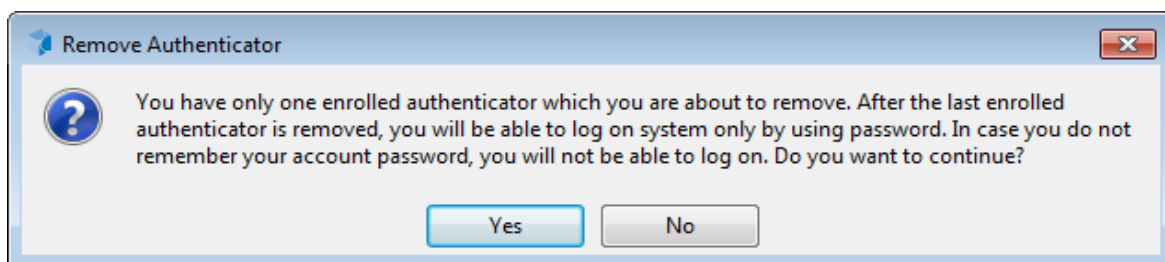
Testing Authenticator

Authenticator testing procedure remains the same for every administrative tool. For more details, see [Testing Authenticator](#) chapter at Active Directory Users and Computers.

Removing Authenticator

 Be careful while removing authenticators. Do not remove all authenticators if random password generation is set up and activated for the user. In this case the user cannot log on if they do not have authenticators.

The system prevents you from accidentally removing the only authenticator by displaying the following dialog:



Authenticator removing procedure remains the same for every administrative tool. For more details, see [Removing Authenticator](#) chapter at Active Directory Users and Computers.

Data Exporting

NetIQ Advanced Authentication Framework User Viewer allows you to export data to file for further analysis with the help of such applications as Microsoft Excel, etc.

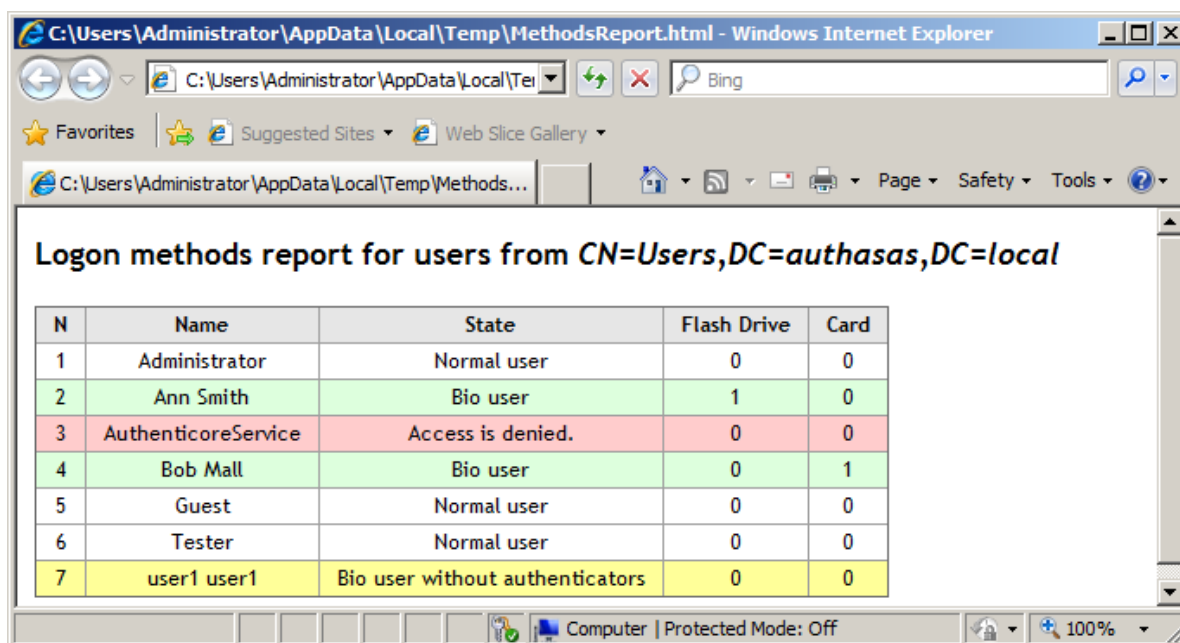
To export data to file

1. Click the **Export List**  toolbar button.
2. Specify the file name and save the file (by default the data is saved in .txt format).

Logon Methods Report

NetIQ Advanced Authentication Framework User Viewer allows you to view the report about logon methods in use.

To view the report, select the container and click the **Create methods report**  toolbar button. The report is generated in .html format and displayed in a new window:



N	Name	State	Flash Drive	Card
1	Administrator	Normal user	0	0
2	Ann Smith	Bio user	1	0
3	AuthenticoreService	Access is denied.	0	0
4	Bob Mall	Bio user	0	1
5	Guest	Normal user	0	0
6	Tester	Normal user	0	0
7	user1 user1	Bio user without authenticators	0	0

Audit Tools

Audit tools allow the administrator to view and analyze events raised in the system. NetIQ Advanced Authentication Framework solution uses the following audit tools:

- log server;

An **event log server** is a computer with installed “NetIQ Advanced Authentication Framework – Log Server” package intended to store all events raised in the NetIQ Advanced Authentication Framework system.

- standard Event Viewer MMC snap-in.

Allows you to view event messages on the local computer or remote log server.

Log Server Setting

To configure log server parameters, use the group policies listed below.

- The [Log Servers](#) policy allows you to specify the names of log servers.
- The following group policies allow you to determine the accuracy with which the log is kept, that is, whether successful events are tracked or not:
 - [Register all user authentication events](#);
 - [Register all password management events](#).
- The [Freeze communication if log server is unavailable](#) policy determines the rules for resolving conflicts in case the remote log server was unavailable at the moment of writing an event onto it.

Event Viewer

Event Viewer snap-in displays the events concerning the following actions in the system:

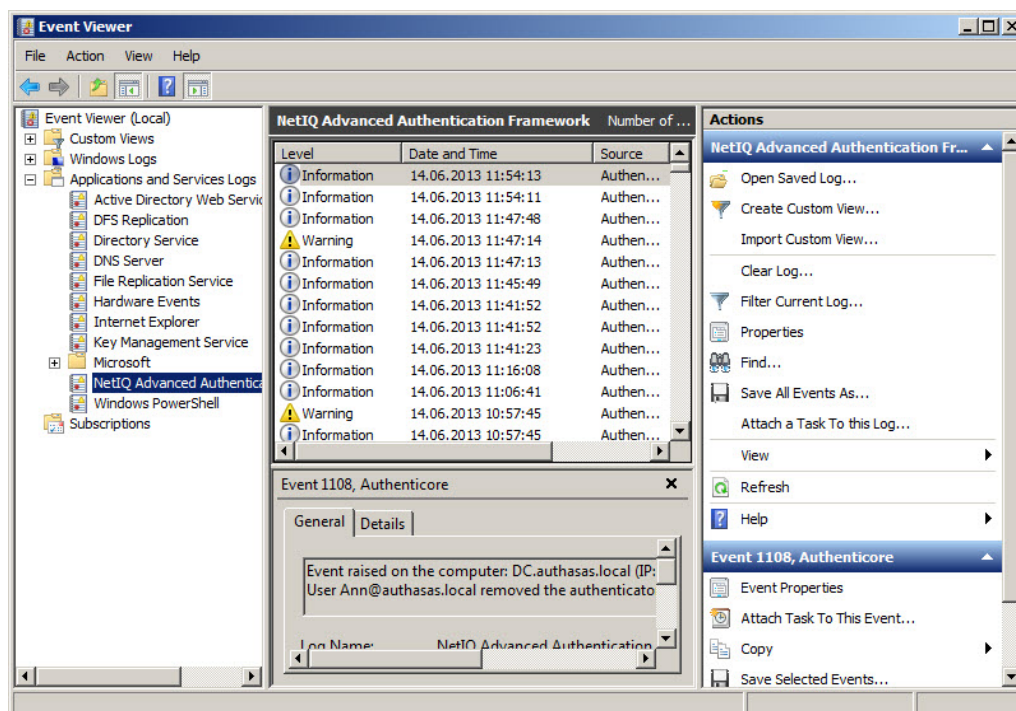
- System modules installation / removing / modifying;
- Users authentication (successful / unsuccessful);
- Enrolling/re-enrolling/removing authenticator ;
- Authenticore server work (server start/stop, server work with Enterprise Key);
- User's password change.

Viewing Events On Local Computer

To view events on the local computer

1. In the **Start** menu, select **Programs > Administrative Tools > Event Viewer**.
2. The **Event Viewer snap-in** opens.

In the console tree, select **Applications and Service Logs ->NetIQ Advanced Authentication Framework**. As a result, the list of resent events is displayed:



NetIQ Events List

The following table lists most common of the events:

Event ID	Level	Description
1103	Error	Could not authenticate the user by the entered password. The error could also occur if the entered account was invalid.
1104	Information	Certain user has re-enrolled the authenticator successfully.
1106	Information	Certain user has added new authenticator successfully.
1108	Information	Certain user has removed the authenticator successfully.
1120	Information	License was applied successfully.
1123	Error	Could not authenticate the user by provided authenticator.
1127	Warning	The user was successful authenticated by provided authenticator of linked account.
1210	Information	Certain user is allowed to use authenticators.
1212	Warning	Certain user is not allowed to use authenticators.
1217	Information	Certain user is allowed to add authenticators.
1218	Information	Certain user is not allowed to add authenticators.
1219	Information	Certain user is allowed to re-enroll his/her authenticators.
1220	Information	Certain user is not allowed to re-enroll his/her authenticators.
1221	Information	Certain user is allowed to delete his/her authenticators.
1222	Information	Certain user is not allowed to delete his/her authenticators.
1223	Information	Certain user is allowed to have certain number of authenticators.
1224	Information	Automatic password generation is allowed for certain user.
1225	Warning	Automatic password generation is not allowed for certain user.

1232	Warning	Certain users are allowed to cache authenticators.
1233	Information	Certain users are not allowed to cache authenticators.
1300	Information	Authenticore server was successfully started.
1301	Warning	Authenticore server was successfully stopped.
1310	Warning	Authenticore server exported Enterprise Key successfully.
1312	Warning	Enterprise Key was successfully imported.
1314	Warning	Enterprise Key was successfully generated.
1402	Error	Error while resetting password for a certain user.
1403	Error	Error while changing password for a certain user.
1404	Information	Password filter was successfully loaded.

Group Policies

NetIQ Advanced Authentication Framework solution has 29 group policies of its own. The policies are divided into sections depending on their application:

- The **Security** section includes security policies allowing the enhancement of data protection:
 - [Authenticator life period](#) – allows you to specify the “life time” of an authenticator.
 - [Credential providers filter settings](#) – allows you to create a list of credential providers you want to turn off.
 - [Disable random password generation by default](#) – defines the default state of the Generate random password for account setting.
 - [Enable PIN caching](#) – allows you to enable a user to only type in PIN once every 8 hours.
 - [Password length](#) – allows you to define the length of the automatically generated password.
 - [PIN restrictions](#) – allows you to define the minimum length of PIN code for PIN code devices.
- The **Event Log** section includes policies allowing you to determine logging settings:
 - [Freeze communication if log server is unavailable](#) – defines the rules for resolving conflicts should the remote log server be unavailable at the moment of writing an event onto it.
 - [Log servers](#) – allows you to define the list of log servers.
 - [Register all password management events](#) – allows you to define the accuracy with which the event log is kept concerning passwords change.
 - [Register all user authentication events](#) – allows you to define the accuracy with which the event log is kept concerning users authentication.
- The **Workstation** section includes policies allowing you to modify GINA behavior:
 - [Alternative Logo for Credential Provider](#) – allows you to define the location of an alternative logo displayed in Client (Credential Provider) windows.
 - [Alternative Logo for GINA and Wizard](#) – allows you to define the location of an alternative logo displayed in Client (GINA) windows.
 - [Deny to specify an authenticator comment at enrollment](#) – allows you to disable user comments at authenticator enrollment/re-enrollment.
 - [Deny to start Client Tray when user logs on to Windows](#) – allows you to define whether NetIQ Advanced Authentication Framework Client Tray is started automatically when a user logs on to Windows or not.

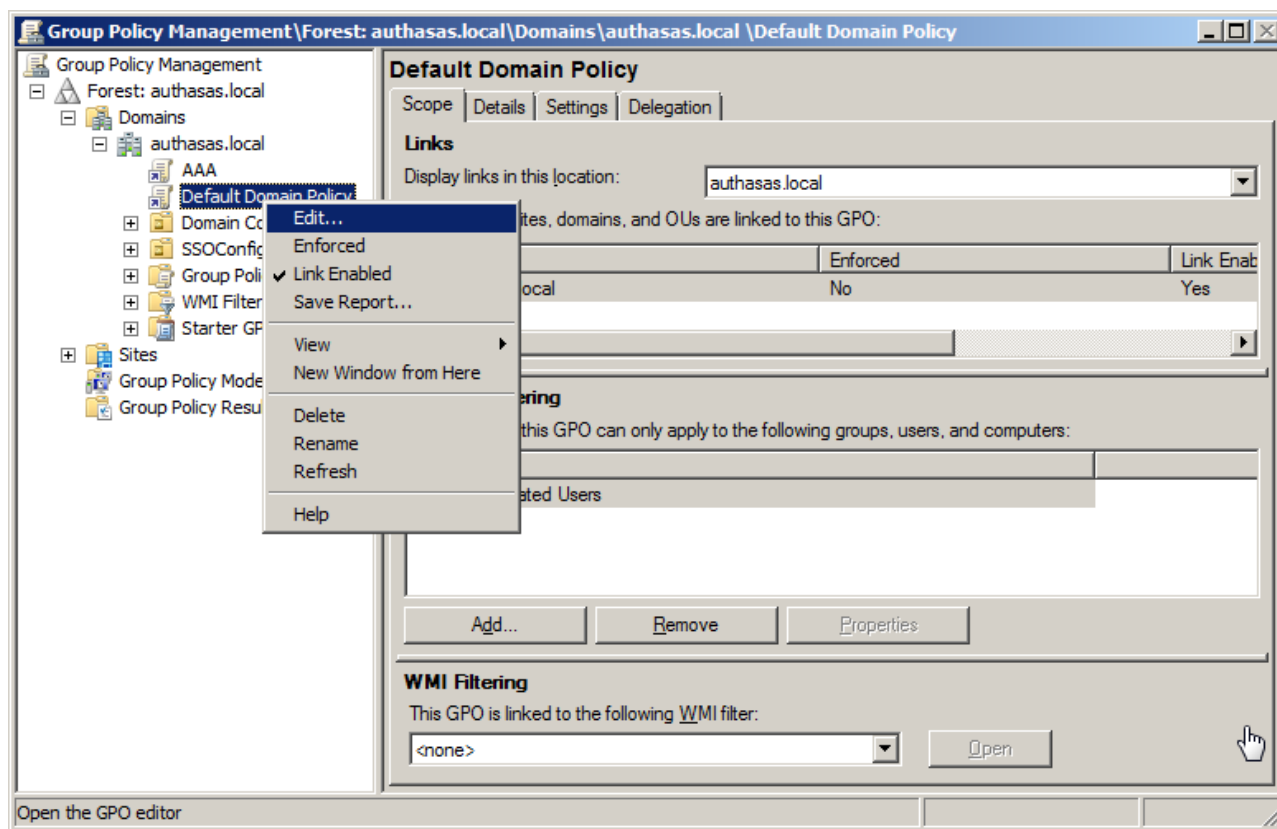
- [Disable "Use Dial-up connection" option](#) – allows you to manage the Use Dial-up connection option in the Logon window.
 - [Do not allow to skip Welcome window](#) – allows you to define whether to skip the Welcome window or not.
 - [Enhanced reaction on device events](#) – allows custom actions during device in and out events.
 - [Force logoff once authenticator is successfully enrolled](#) – allows you to enable/disable automatic logoff after successful authenticator enrollment.
 - [Lifetime of notification about password reset](#) – allows you to setup lifetime of user's notification about user's password reset by administrator.
 - [Tap and Go](#) – enables you to turn on the Tap and Go function.
 - ["Use current settings as defaults" option management for PC unlocking](#) – allows you to manage the Use current settings as defaults option in the Unlock Computer window.
 - ["Use current settings as defaults" option management](#) – allows you to manage the Use current settings as defaults option in the Logon window.
- The **BSP** section includes policies allowing you to modify enrollment parameters.
 - [Number of fingers to enroll](#) – allows you to specify the number of fingers a user can enroll.
 - [Play sounds](#) – allows you to enable sounds during enrollment process.
 - The **Repository** section includes policies allowing you to edit NetIQ repository.
 - [Repository](#) – allows you to choose whether to use native Active Directory or ADAM/AD-LDS as NetIQ repository.
 - [ADAM settings](#) – allows you to configure whether ADAM/AD-LDS is used as a repository.

Adding Group Policies

The main policy templates (Security, Event Log, and Workstation) are stored locally in **NAAF.adm** and **NetIQAdvancedAuthenticationFramework_BioKeyBSP.adm** files in **C:\Windows\inf** folder. There are also a few .adm files containing supplementary policies (**NAAF_ad_attrs.adm**, **NAAF_dbg.adm**) in the **_admttools** folder on the installation disk. To add and configure policies, use the standard Group Policy Object Editor snap-in.

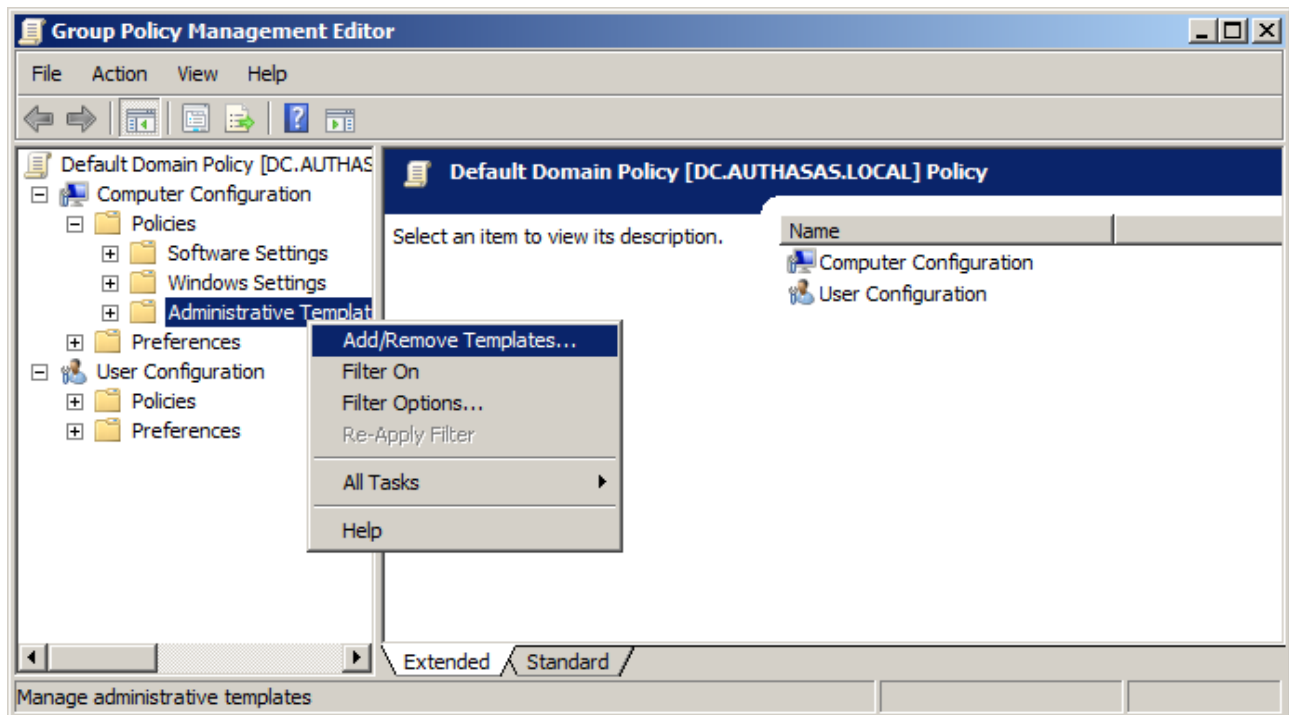
To add the group policy templates and configure the policies, use

- **Group Policy Management Console (GPMC)**, which is installed by default on a Domain Controller. To open GPMC, click **Start** and select **Administrative Tools > Group Policy Management**.
- **Group Policy Management Editor (GPME)**, which can be opened from GPMC. To open GPME, under domain right-click **Default Domain Policy** and select **Edit**.

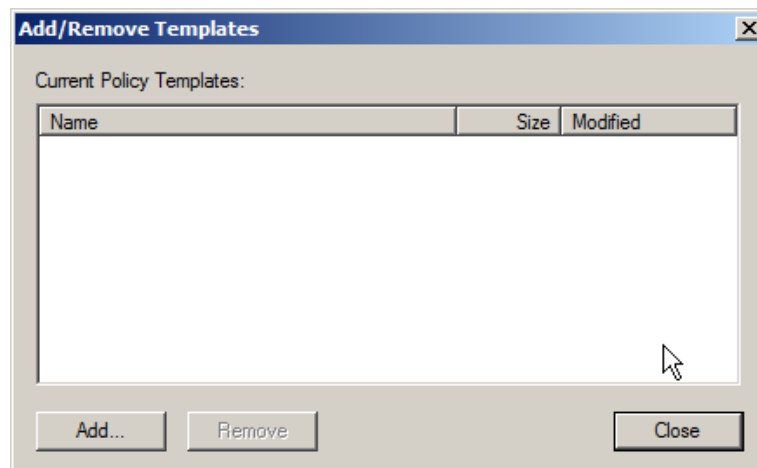


To add a group policy template

1. In **GPME**, under **Computer Configuration > Policies** right-click **Administrative Templates: Policy definitions (ADMX files)...** and select **Add/Remove Templates**.



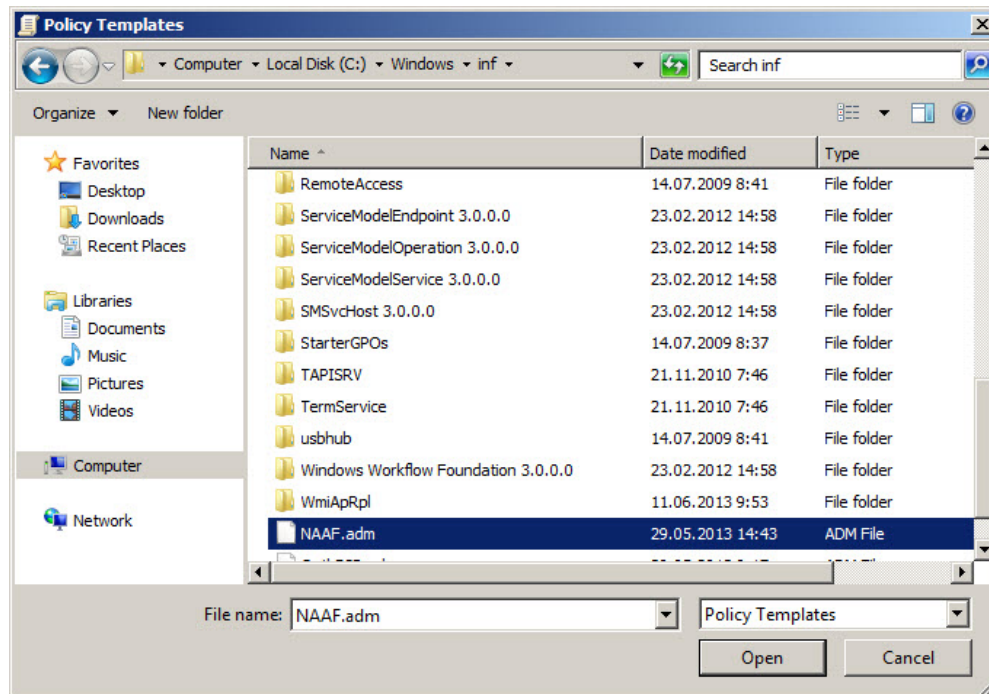
2. In the **Add/Remove Templates** dialog, click **Add**.



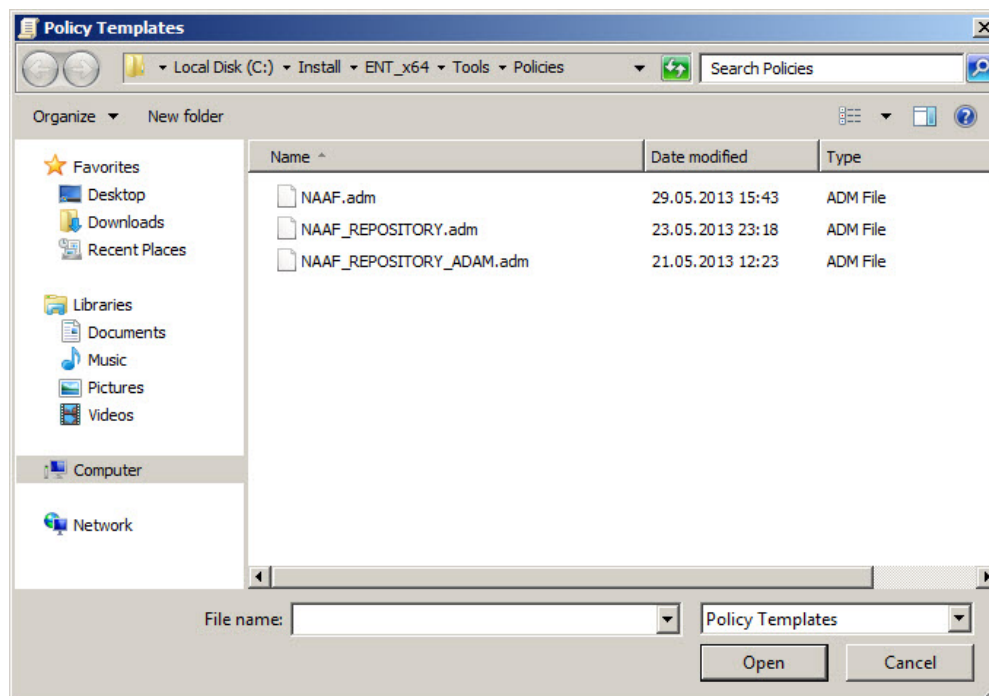
3. Select and open policy templates.

a) General templates (**NAAF.adm** and **NetIQAdvancedAuthenticationFramework_BioKeyBSP.adm** files) are located in **C:\Windows\inf** folder.

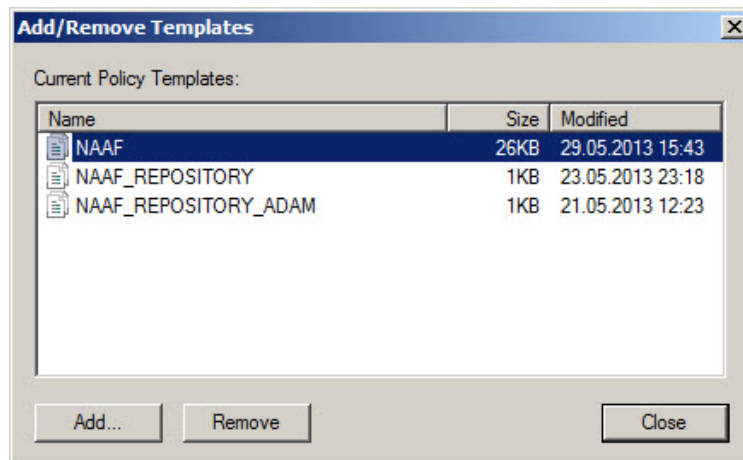
✖ NetIQAdvancedAuthenticationFramework_BioKeyBSP.adm file will be available only if BIO-Key authentication provider has been installed.



b) Supplementary templates (**NAAF_ad_attrs.adm**, **NAAF_dbg.adm**) are located in the %NETIQ installation directory%\Tools\Policies folder on the installation disk.



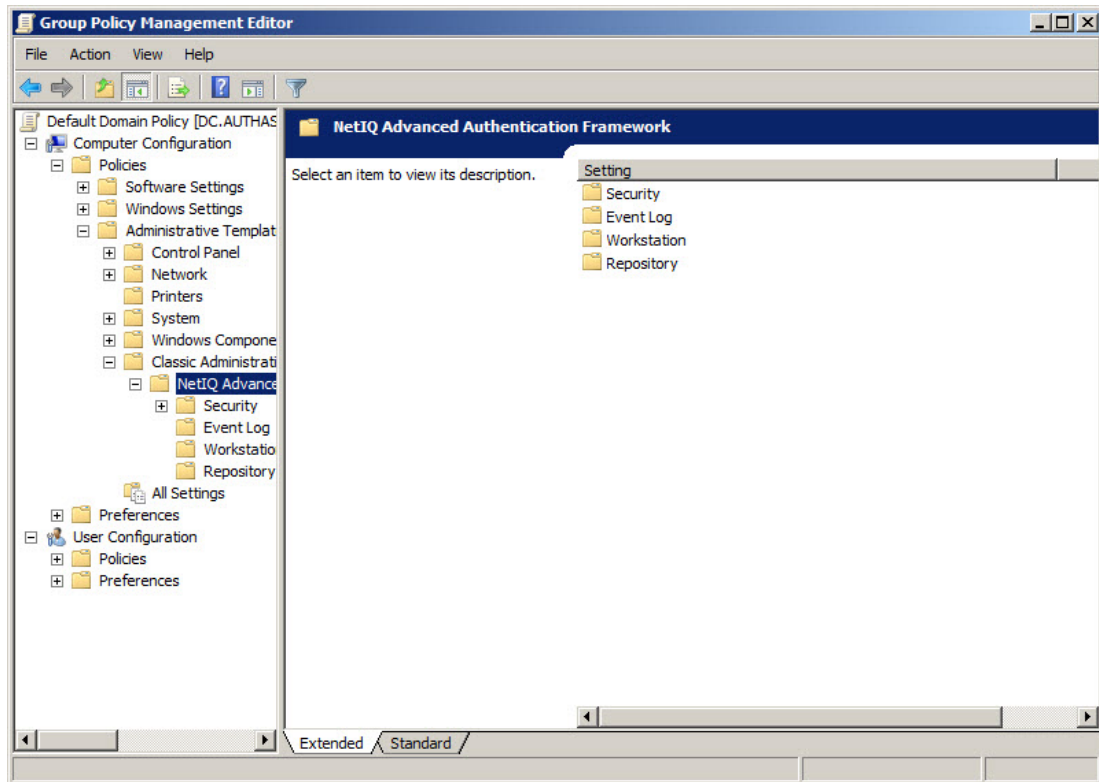
4. The names of templates appear in the **Add/Remove Templates** dialog.



Click **Close**.

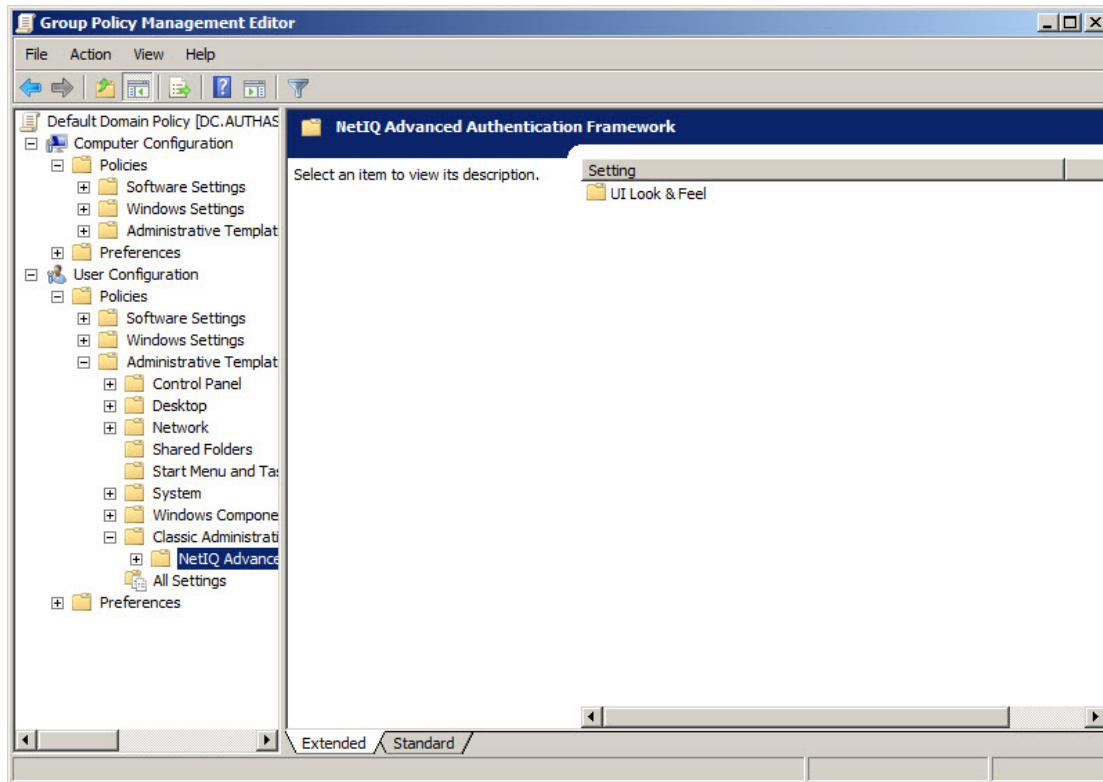
Some policies appear in GPME under **Computer Configuration > Policies > Administrative Templates: Policy definitions > Classic Administrative Templates (ADM)**:

- **NetIQ Advanced Authentication Framework > Security, Event Log, Workstation, Repository;**
- **BSP > BIO-Key.**



Others appear **under User Configuration > Policies > Administrative Templates: Policy definitions > Classic Administrative Templates (ADM):**

- **NetIQ Advanced Authentication Framework > UI Look & Feel.**



Once the templates are added, you can enable and configure the policies (see [Configuring Group Policies](#)).

Configuring Group Policies

Policy settings are available for editing only when the policy is activated. To activate a policy:

1. In Group Policy Object Editor, double-click the policy name.
2. In the properties dialog, click **Enabled**.

To switch between the policies, use the **Previous setting** and the **Next setting** buttons.

To save changes, use the **Apply** button. When switching between the policies, the changes are saved automatically.



The changes take effect after group policy refresh.



To refresh group policy immediately, in the command line enter `gpupdate /force`.

Security Policies

The **Security** section includes security policies allowing the enhancement of data protection.

It includes:

- [Authenticator Life Period](#);
- [Credential Providers Filter Settings](#);
- [Disable Random Password Generation by Default](#);
- [Enable PIN Caching](#);
- [Password Length](#);
- [PIN restrictions](#).

Authenticator Life Period

The **Authenticator life period** policy allows you to specify the 'life time' of an authenticator.

This policy is used to counteract all possible attempts to intercept IP-packages and crack the system.

Authenticator life period

Authenticator life period

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on:

Options:

Authenticator validity period (in minutes):

5

Help:

The policy determines the length of a current authenticator "life period".

The "Authenticator validity period (in minutes)" setting allows you to specify how long a current authenticator remains "valid".

In case the time period between authenticator submission and authenticator verification exceeds the specified value, the authenticator is considered "invalid".

This is a protective measure in case someone attempts to intercept IP-packages and gain unauthorized access to the system.

In case the policy is not configured or disabled, default authenticator "life time" equals to 5 minutes.

OK Cancel Apply

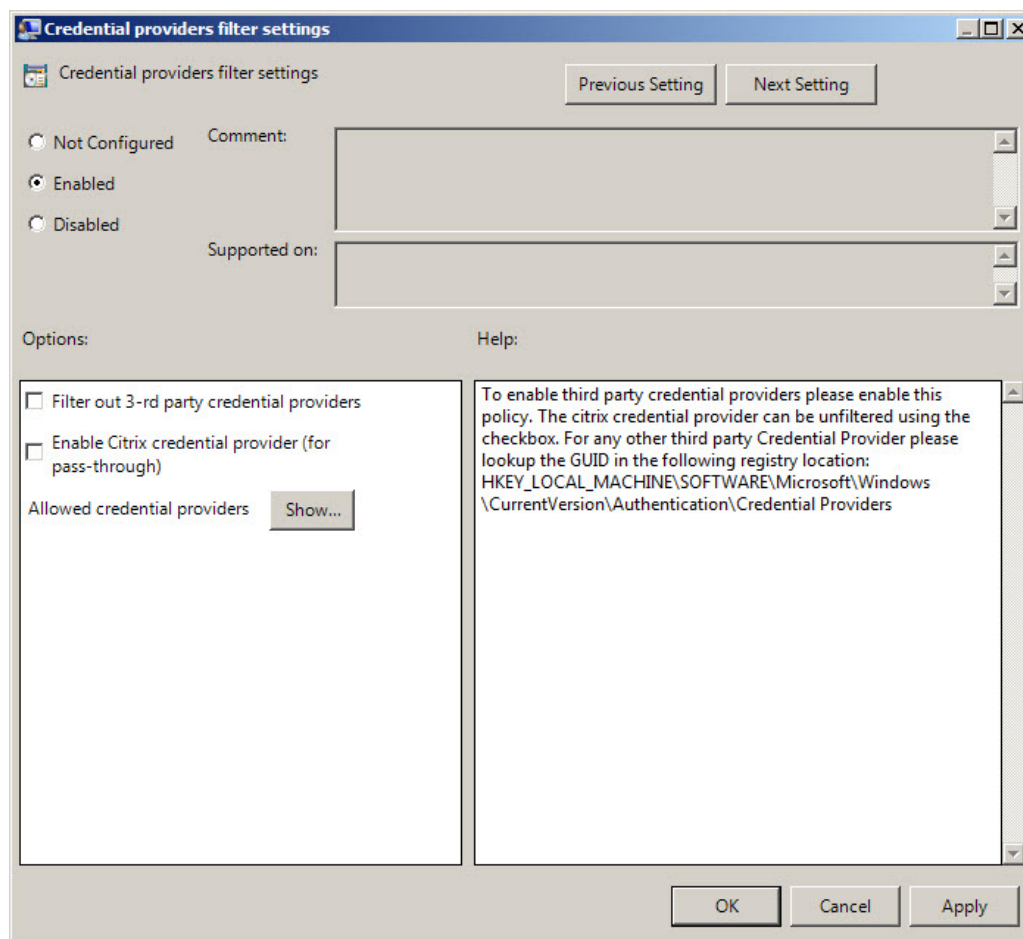
The **Authenticator validity period** setting allows you to define how long an authenticator obtained from the user remains "valid" before it is checked on Authenticore server.

If the time interval between the moment the authenticator is received and the moment it is checked on Authenticore server exceeds the specified value, the authenticator is considered invalid.

 If the policy is not defined or is disabled, the "life time" of an authenticator is 5 minutes.

Credential Providers Filter Settings

The Credential providers filter settings policy allows the system administrator to create a list of credential providers that should be turned off. Some credential providers (CP) may conflict with NetIQ CP, that is why they should be turned off.



To turn off some of the CP, **Filter out 3-rd party credential providers** option should be checked.

The list of allowed credential providers are shown in the **Show Contents** window, that appears after clicking the **Show...** button.

In order to set a policy for listing all the important CPs, uncheck the **Filter out 3-rd party credential providers** option.

* Only NetIQ CP is listed by default, however some applications may substitute it with their CPs.

Disable Random Password Generation by Default

The **Disable random password generation by default** policy defines the default state of the **Generate random password** for account setting.

The screenshot shows a Windows-style dialog box titled "Disable random password generation by default". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio button options: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these options is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a list box. At the bottom left, there is an "Options:" section with a large empty text box. At the bottom right, there is a "Help:" section containing the following text: "Defines the default state of 'Generate random password for account' setting. If you enable this setting, the 'Generate random password for account' setting will be unchecked by default while you create a new user or edit user settings. If you disable this setting or do not configure it, the 'Generate random password for account' setting will be checked by default while you create a new user or edit user settings. This setting is designed to let administrators disable random password generation by default for the new user." At the very bottom, there are "OK", "Cancel", and "Apply" buttons.

✖ If you enable this policy, the **Generate random password for account** setting will be unchecked by default when you create user or edit user's properties.

✖ If you disable this setting or do not configure it, the **Generate random password for account** setting will be checked by default when you create user or edit user's properties.

Enable PIN Caching

PIN caching is used together with authenticators using a PIN. PIN caching enables the user to only type in his/her PIN once every eight hours by default. But PIN cache expiration can be configured manually. Within the PIN cache expiration period the user can just tap their card and get access. After the PIN cache expiration period the user needs to provide PIN again.

The screenshot shows a Windows-style configuration window titled "Enable PIN caching". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. Under the "Options:" label, there is a "PIN cache expiration period (in minutes)" spinner box set to "480". To the right of this is a "Help:" text box containing the text: "PIN caching is used together with authenticators using a PIN. PIN caching enables the user to only type in their PIN once every 8 hours. Within the 8 hours the user can just tap their card and get access. After the 8 hours the user needs to provide the PIN again." At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

✖ If the policy is not defined or is disabled, the user should type in his/her PIN during every authentication process.

✖ If Enable PIN caching policy is used together with Disabled PIN Host List policy, then it will be possible to configure a list of workstations that will not require PIN code.

Hide password mode from logon UI

If you enable this setting, the **"Logon by password"** mode will not be shown in authentication methods menu on workstations with NetIQ Client installed. If you disable this setting or do not configure it, the **"Logon by password"** mode will be shown in authentication methods menu.



Please ensure that all users of workstation on which you want to enable this policy have at least one enrolled authenticator. Otherwise, you will have problems with user logon.

Lock account on failed logon

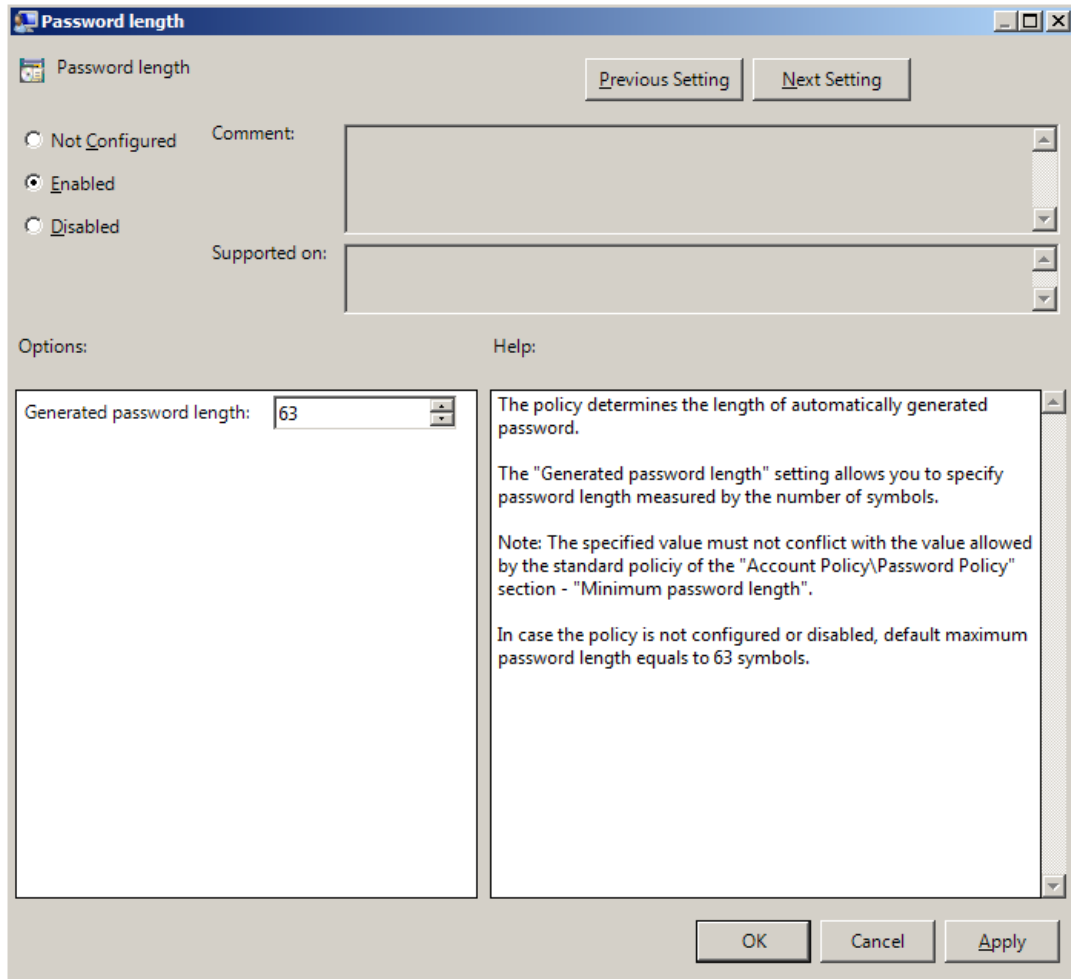
If this policy is enabled the **user account will be locked after invalid logon attempts** (depending on number configured in [Account lockout threshold](#) policy) regardless of authentication mode. In this case, the user will get an Authorization Error "The referenced account is currently locked out and may not be logged on to."

If this policy is disabled or do not configured, the user account will be locked after invalid logon attempts by password only (depending on number configured in [Account lockout threshold](#) policy).

You also can configure [Account lockout duration](#).

Password Length

The Password Length policy allows you to define the length of the automatically generated password.



The screenshot shows the 'Password length' configuration window. At the top, there are 'Previous Setting' and 'Next Setting' buttons. Below them, three radio buttons are present: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' section with a list box. The 'Options:' section contains a 'Generated password length:' label followed by a spinner box set to '63'. The 'Help:' section contains a text area with the following text: 'The policy determines the length of automatically generated password. The "Generated password length" setting allows you to specify password length measured by the number of symbols. Note: The specified value must not conflict with the value allowed by the standard policy of the "Account Policy\Password Policy" section - "Minimum password length". In case the policy is not configured or disabled, default maximum password length equals to 63 symbols.' At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

The **Generated password length** setting allows you to specify the length of automatically generated random passwords (in symbols).

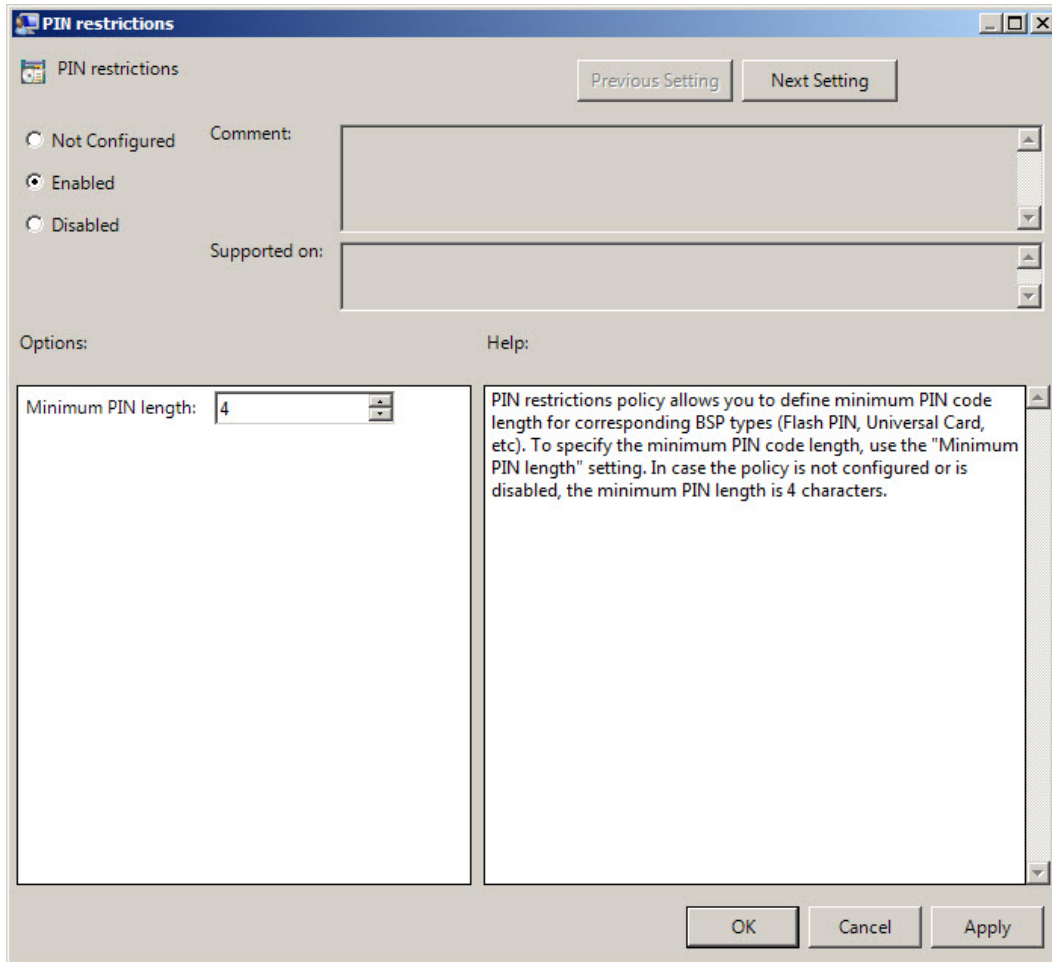
 The specified value and the frequency of passwords change must not conflict with the values defined by the standard policies of the Account Policy\Password Policy section:

- Password must meet complexity requirements;
- Minimum password length;
- Enforce password history.

 If the policy is not defined or is disabled, the password length equals to the maximum of 63 symbols.

PIN Restrictions

The **PIN restrictions** policy allows you to define the minimum length of the PIN code for PIN code devices (for Universal Card authentication provider, Flash+PIN authentication provider).



The screenshot shows a window titled "PIN restrictions". At the top, there are "Previous Setting" and "Next Setting" buttons. Below them, on the left, are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. In the "Options:" section, there is a "Minimum PIN length:" label followed by a spinner box containing the number "4". To the right of the options is a "Help:" section containing a text box with the following text: "PIN restrictions policy allows you to define minimum PIN code length for corresponding BSP types (Flash PIN, Universal Card, etc). To specify the minimum PIN code length, use the 'Minimum PIN length' setting. In case the policy is not configured or is disabled, the minimum PIN length is 4 characters." At the bottom right of the window are "OK", "Cancel", and "Apply" buttons.

The **Minimum PIN length** setting allows you to specify the minimum length of PIN code (in symbols).

 If the policy is not defined or is disabled, the minimum length of PIN code is 4 symbols.

Use domain password as PIN

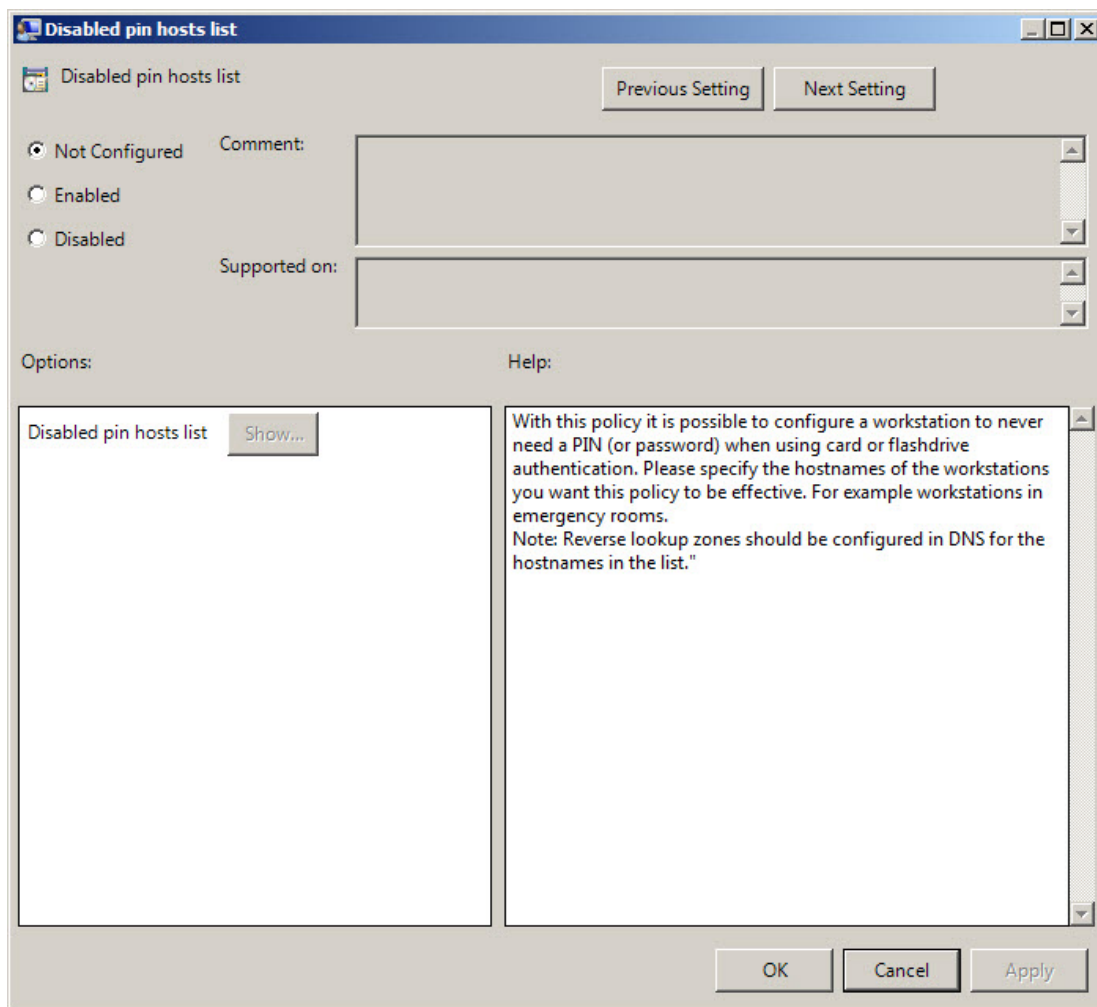
When this policy is enabled, a user should use the domain password together with a card. This will replace the use of a PIN code.

 It is not allowed to change this policy after cards have been enrolled. You need to re-enroll the authenticators or enable the policy.

Disabled PIN Host List

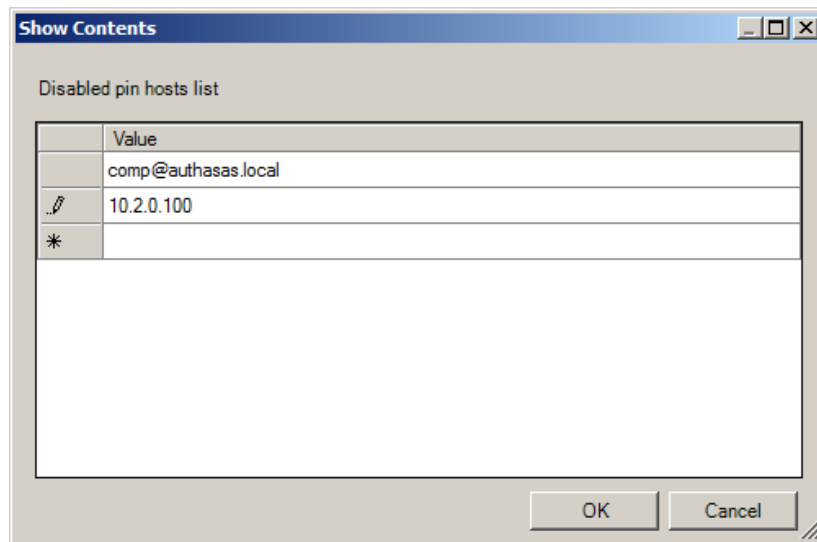
The **Disabled PIN Host List** policy allows you to logon just by a device. This policy guarantees fast access to the system as PIN is not needed for logon.

To enable the Disabled PIN Host List policy, open **Classic Administrative Templates (ADM) > NetIQ Advanced Authentication Framework > Security**. From the list of the policies, choose the **Disabled PIN Host** policy. The following window will be displayed:



-  The **Disabled PIN Host List** policy can be enabled only if the **Enable PIN Caching** policy is enabled.
-  If the policy is enabled, adding comments at authenticator enrollment is not allowed.
-  If the policy is not defined or is disabled, adding comments at authenticator enrollment is allowed.

Click the **Enabled** radio button and the **Show** button. The window with the opportunity of adding computers and IP addresses will appear.



After all computers and IP addresses that will not need to enter PIN to logon are added, click the **OK** button to save changes. Then click the **Apply** button to save all the changes.

When the changes are saved, PIN will not be required for the specified list of computers during the authentication.

Event Log Policies

The **Event Log** section includes policies allowing you to determine logging settings.

It includes:

- [Freeze communication if log server is unavailable](#);
- [Log Servers](#);
- [Register all password management events](#);
- [Register all user authentication events](#).

Freeze Communication if Log Server is Unavailable

The **Freeze communication if log server is unavailable** policy defines the rules for resolving conflicts in case the remote log server was unavailable at the moment of writing an event onto it. The "freezing" of the communication with the faulty log server minimizes attempts to connect to the remote log server while it is unavailable and increases log service fault tolerance.

Freeze communication if log server is unavailable

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on:

Options:

Max time-out period (in minutes): 120

Normal time-out period (in minutes): 30

Time interval to restore communication (in minutes): 5

Increasing time interval for the next time-out period (in minutes): 5

Help:

The policy determines logic according to which communication with unavailable remote event log server is suspended/restored.

If a remote event log server proves unavailable and an event cannot be received and recorded, communication with this server is "frozen" (suspended).

This measure is intended to minimize the number of connection setup attempts when remote event log server is unavailable and to increase fault tolerance of the log server.

Duration of the suspense period is modified by means of the "Time interval to restore communication" setting.

When the suspense period is over and a new event occurs, the event log Client attempts to restore communication with the event log server.

Duration of communication recovery period is modified by means of the "Normal time-out period" setting.

OK Cancel Apply

If the remote event log server becomes unavailable in the moment of recording an event, the communication with this remote log server is "frozen" for the time period specified by the **Time interval to restore communication (in minutes)** setting. After the period elapses, and a new event occurs, a new attempt will be made to establish connection with the remote log server. The attempts continue during the time period specified by the **Normal time out period (in minutes)** setting. In case the connection to the faulty log server is not restored within this time period, the connection "freezes" for a longer period. The increase in "freeze" duration is specified by the **Increasing time interval for the next time-out period (in minutes)** setting. The "freeze" duration increases until it reaches the value specified by the **Max time-out period (in minutes)** setting. After that, the "freezing" time is reset to its initial state specified by the setting.



If the policy is not defined or disabled, then its parameters have the following default values:

Time interval to restore communication (in minutes): 5;

Normal time-out period (in minutes): 30;

Increasing time interval for the next time-out period (in minutes): 5;

Max time-out period (in minutes): 120.

Log Servers

The **Log servers** policy allows you to define the list of the Log Servers.

The screenshot shows the 'Log servers' policy configuration window. It includes a title bar, window controls, and a 'Log servers' icon. The main area has radio buttons for 'Not Configured', 'Enabled' (selected), and 'Disabled'. There are text boxes for 'Comment:' and 'Supported on:'. Below these are 'Options:' and 'Help:' sections. The 'Options:' section has a 'Log servers:' label and a large text box. The 'Help:' section contains explanatory text. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

This **Log servers** box should contain the list of log servers names. Put the names in one line in UPN or NetBIOS format and separate them with semicolon. Do not use spaces. *Example:* Computer1; Computer2.domainname.com; Computer3.

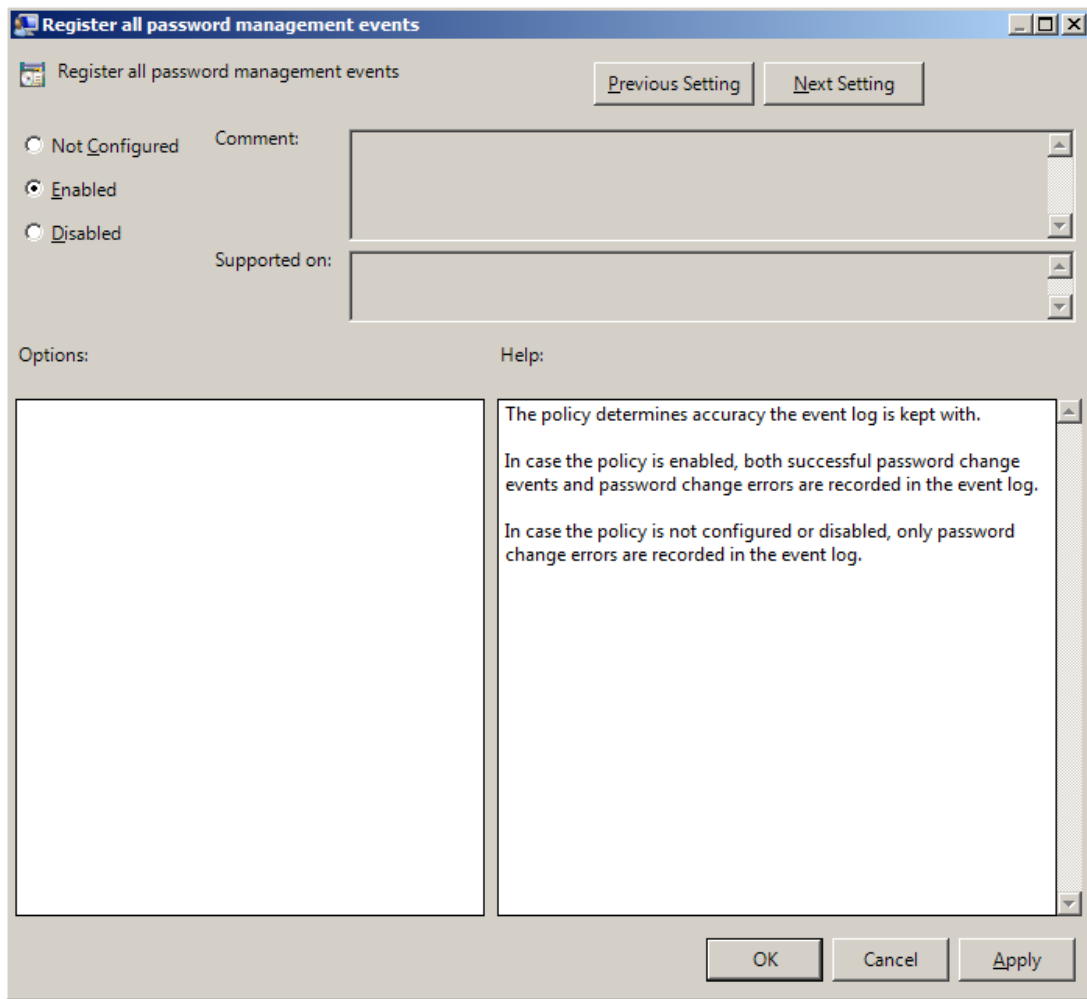
 The "NetIQ Advanced Authentication Framework – Log Server" package must be installed on the computers specified in the policy setting.

 This setting does not disable registering events in the local log of the computer.

 If the policy is not defined or is disabled, NetIQ Advanced Authentication Framework events are recorded in the local log of the computer.

Register All Password Management Events

The **Register all password management events** policy allows you to define whether successful password change events are recorded into the event log.



The screenshot shows a Windows-style dialog box titled "Register all password management events". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio button options: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these options is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a list box. At the bottom left, there is an "Options:" section with a large empty text box. At the bottom right, there is a "Help:" section containing the following text: "The policy determines accuracy the event log is kept with. In case the policy is enabled, both successful password change events and password change errors are recorded in the event log. In case the policy is not configured or disabled, only password change errors are recorded in the event log." At the very bottom of the dialog are "OK", "Cancel", and "Apply" buttons.

* If the policy is enabled, all password change events including successful ones are recorded in the event log.

* If the policy is not defined or is disabled, only unsuccessful password change events are recorded in the event log.

Register All User Authentication Events

The **Register all user authentication events** policy allows you to define whether successful user authentication events are recorded into the event log.

The screenshot shows a Windows-style dialog box titled "Register all user authentication events". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. At the bottom left is an "Options:" section with a large empty box. At the bottom right is a "Help:" section containing the following text: "The policy determines accuracy the event log is kept with. In case the policy is enabled, both successful authentication events and authentication errors are recorded in the event log. In case the setting is not configured or disabled, only authentication errors are recorded in the event log." At the very bottom are "OK", "Cancel", and "Apply" buttons.

- * If the policy is enabled, all user authentication events including successful ones are recorded in the event log.
- * If the policy is not defined or is disabled, only unsuccessful user authentication events are recorded in the event log.

Workstation Policies

The Workstation section includes policies allowing you to modify GINA behavior.

It includes:

- [Alternative Logo for Credential Provider;](#)
- [Alternative Logo for GINA and Wizard;](#)
- [Deny to specify authenticator comment at enrollment;](#)
- [Deny to start Client Tray when user logs on to Windows;](#)
- [Disable "Use Dial-up connection" option;](#)
- [Do not allow to skip welcome window;](#)
- [Enhanced reaction on device events;](#)
- [Force logoff once authenticator is successfully enrolled;](#)
- [Lifetime of notification about password reset;](#)
- [Tap and Go;](#)
- ["Use current settings as defaults" option management for PC unlocking;](#)
- ["Use current settings as defaults" option management.](#)

Alternative Logo for Credential Provider

The **Alternative logo** policy defines the location of an alternative logo displayed by Credential Provider.



Credential Provider is a component of Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows Server 2008/Microsoft Windows Server 2008 R2 operation systems; it is responsible for user authentication and credentials verification.

Alternative Logo for Credential Provider

Alternative Logo for Credential Provider Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled Supported on:

Options: Help:

Logo version

Path to (125x125 pixels) logo image (*.bmp):

The policy determines the location of an alternative logo displayed by Authasas Advanced Authentication Workstation (Credential Provider).

To make Authasas Advanced Authentication Workstation display an alternative logo correctly, you should specify the location of this logo in the network or on the local computer.

The size of the logo must be 125x125 pixels.

In case the policy is not configured or disabled, an alternative logo is not displayed.

Note: To optimize the traffic, Authasas Advanced Authentication Workstation loads an alternative logo from the specified location only once assuming the Logo version or path has been changed.

OK Cancel Apply

Alternative Logo for Credential Provider

Previous Setting Next Setting

☐ Not Configured
 ☒ Enabled
 ☐ Disabled

Comment:

Supported on:

Options:

Logo version

Path to (125x125 pixels) logo image (*.bmp):

Help:

The policy determines the location of an alternative logo displayed by NetIQ Advanced Authentication Framework Workstation (Credential Provider).

To make NetIQ Advanced Authentication Framework Workstation display an alternative logo correctly, you should specify the location of this logo in the network or on the local computer.

The size of the logo must be 125x125 pixels.

In case the policy is not configured or disabled, an alternative logo is not displayed.

Note: To optimize the traffic, NetIQ Advanced Authentication Framework Workstation loads an alternative logo from the specified location only once assuming the Logo version or path has been changed.

OK Cancel Apply

To ensure an alternative logo is displayed in an appropriate way, you need to specify where the logo is stored (this can be a network drive or a local storage).

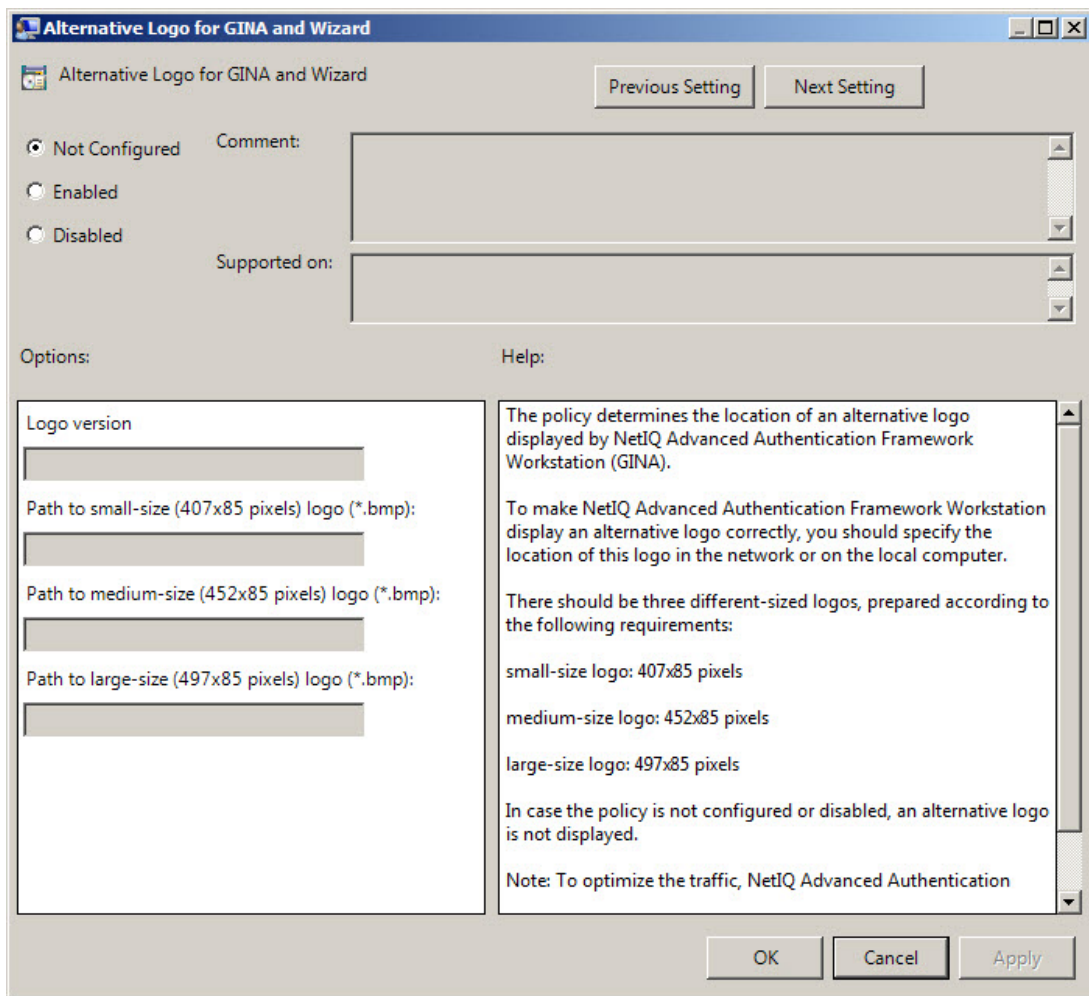
The size of the logo must be 125x125 pixels.

- ✖ To optimize the traffic, NetIQ Advanced Authentication Framework Client loads an alternative logo from the specified location only once assuming the Logo version or any of the paths have been changed.
- ✖ If the policy is not configured or is disabled, an alternative logo is not displayed.

Alternative Logo for GINA and Wizard

The **Alternative logo** policy allows you to define the location of an alternative logo displayed in NetIQ Advanced Authentication Framework Client (GINA) windows. This logo is also used in the **Enrollment wizard**.

 **GINA (Graphical Identification and Authentication)** is a component of Microsoft Windows 2000/ Microsoft Windows XP/Microsoft Windows Server 2003 operation systems; it is responsible for user authentication and credentials verification.



Alternative Logo for GINA and Wizard

Alternative Logo for GINA and Wizard

Previous Setting Next Setting

☒ Not Configured Comment:

☐ Enabled

☐ Disabled

Supported on:

Options:

Logo version

Path to small-size (407x85 pixels) logo (*.bmp):

Path to medium-size (452x85 pixels) logo (*.bmp):

Path to large-size (497x85 pixels) logo (*.bmp):

Help:

The policy determines the location of an alternative logo displayed by NetIQ Advanced Authentication Framework Workstation (GINA).

To make NetIQ Advanced Authentication Framework Workstation display an alternative logo correctly, you should specify the location of this logo in the network or on the local computer.

There should be three different-sized logos, prepared according to the following requirements:

small-size logo: 407x85 pixels

medium-size logo: 452x85 pixels

large-size logo: 497x85 pixels

In case the policy is not configured or disabled, an alternative logo is not displayed.

Note: To optimize the traffic, NetIQ Advanced Authentication

OK Cancel Apply

To display an alternative logo in NetIQ Advanced Authentication Framework Client windows correctly, it is necessary to specify the location of this logo in the network or on the local computer.

 Shared folders you use must be accessible (read-only) for **Domain Computers** group. Other access configurations are optional.

 To specify the path to the logo file, you should use the server name, NOT its IP-address.

There must be three logos of different sizes corresponding to the following parameters:

- small-size logo: 406x85 pixels;
- medium-size logo: 451x85 pixels;
- large-size logo: 495x85 pixels.

 To optimize the traffic, NetIQ Advanced Authentication Framework Client loads an alternative logo from the specified location only once assuming the Logo version or path has been changed.

 If the policy is not defined or is disabled, an alternative logo is not displayed.

Deny to Specify Authenticator Comment at Enrollment

The **Deny to specify Authenticator comment at enrollment** policy defines whether an NetIQ Advanced Authentication Framework user is allowed to add a comment at authenticator enrollment or not.

The screenshot shows a Windows-style dialog box titled "Deny to specify an authenticator comment at enrollment". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these radio buttons is a "Comment:" label followed by a large text input field. Below the radio buttons is a "Supported on:" label followed by a list box. At the bottom of the dialog, there are "Options:" and "Help:" labels. The "Options:" area is empty. The "Help:" area contains a text box with the following text: "The policy determines whether a user is allowed to add a comment at authenticator enrollment/re-enrollment. In case the policy is enabled, a user cannot add a comment both at enrollment and at re-enrollment. In case there is only one BSP module installed on the computer, the Enrol Authenticator page is skipped, so a user does not have to specify an authenticator type and click on 'Enrol' to start enrolling an authenticator. In case the policy is not configured or disabled, a user can add a comment both at enrollment and at re-enrollment, and has to specify authenticator type and click on 'Enrol' to start enrolling an authenticator." At the bottom right of the dialog are "OK", "Cancel", and "Apply" buttons.

- * If the policy is enabled, adding comments at authenticator enrollment is not allowed.
- * If the policy is not defined or is disabled, adding comments at authenticator enrollment is allowed.

Deny to Start Client Tray When User Logs on to Windows

The **Deny to start Client Tray when user logs on to Windows** policy allows you to define whether NetIQ Advanced Authentication Framework Client Tray is started automatically at Windows logon or manually.

The screenshot shows a Windows-style dialog box titled "Deny to start Client Tray when user logs on to Windows". At the top, there are two buttons: "Previous Setting" and "Next Setting". Below these, there are three radio buttons: "Not Configured" (selected), "Enabled", and "Disabled". To the right of the radio buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. At the bottom left, there is an "Options:" section with a large empty box. At the bottom right, there is a "Help:" section with a text area containing the following text:

The policy determines NetIQ Advanced Authentication Framework Settings Tray behaviour.

In case the policy is enabled, NetIQ Advanced Authentication Framework Settings Tray is not launched when NetIQ Advanced Authentication Framework users log on to Windows.

In case the policy is not configured or disabled, NetIQ Advanced Authentication Framework Settings Tray is launched when NetIQ Advanced Authentication Framework users log on to Windows (unless the "Launch at startup" option has been disabled).

At the bottom right of the dialog box are three buttons: "OK", "Cancel", and "Apply".

* If the policy is enabled, NetIQ Advanced Authentication Framework Client Tray is started manually through Start > Programs > NetIQ Advanced Authentication Framework > NetIQ Advanced Authentication Framework Settings Tray.

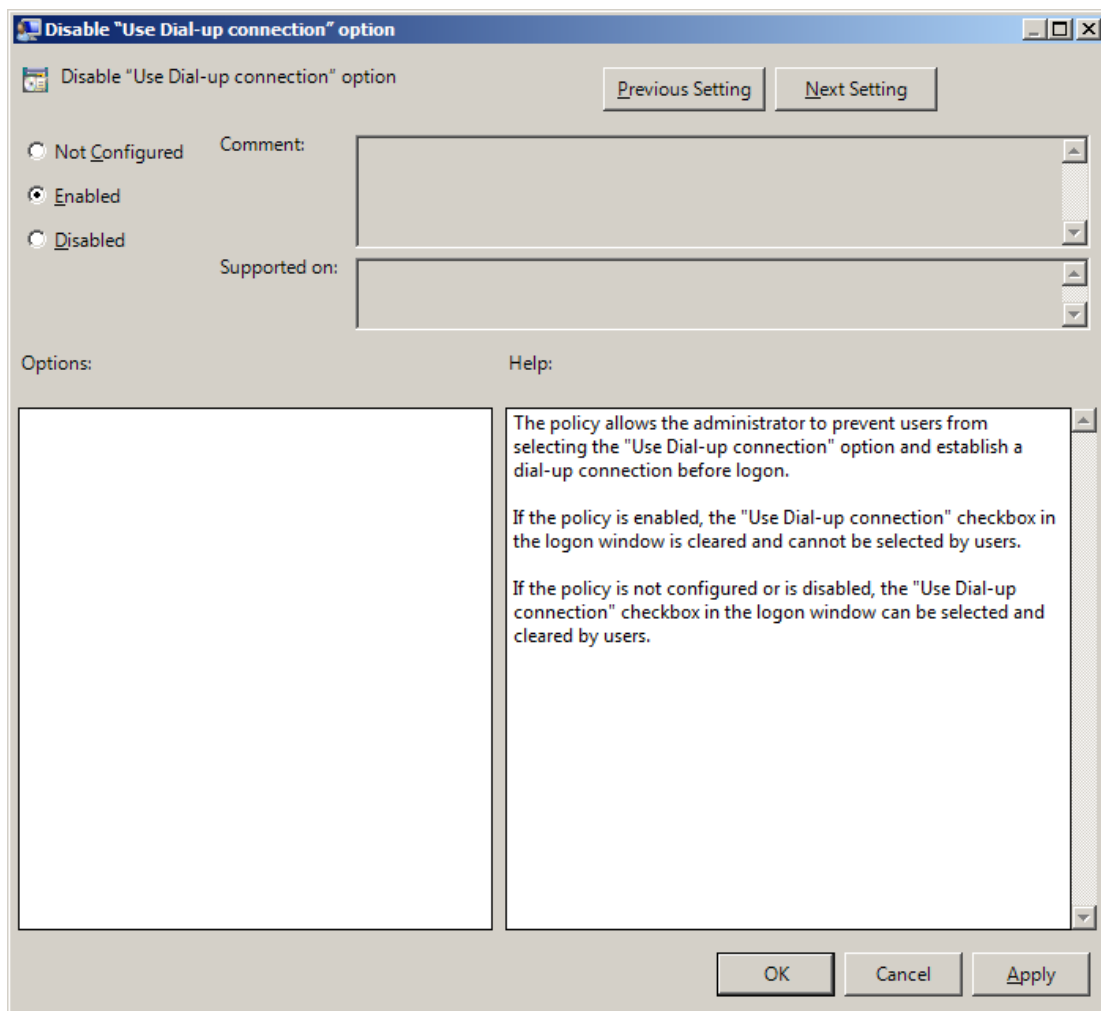
* If the policy is not defined or is disabled, NetIQ Advanced Authentication Framework Client Tray is started automatically when a user logs on to Windows.

Disable "Use Dial-up Connection" Option

The **Disable "Use Dial-up connection"** option policy allows you to manage the Use Dial-up connection option in the Logon window.

The policy provides you with the following options:

- a. disable the Use Dial-up connection option;
- b. let users select the option if they wish to.



If the policy is enabled, the Use Dial-up connection option is always disabled and cannot be selected by users.



If the policy is not configured or is disabled, the dial-up connection can be set up at logon. The **Use Dial-up connection** option in the **Logon** window can be selected by users.

Do Not Allow to Skip Welcome Window

The **Do not allow to skip Welcome window** policy, if enabled, disallows users to skip the Welcome to NetIQ Advanced Authentication Framework System at the first logon without enrolling at least one authenticator.

The screenshot shows a Windows-style configuration window titled "Do not allow to skip Welcome window". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured" (selected), "Enabled", and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a list box. At the bottom left is an "Options:" section with a large empty text box. At the bottom right is a "Help:" section with a text box containing the following text:

The policy determines the "Welcome" window behaviour.

In case the policy is enabled, a NetIQ Advanced Authentication Framework user is prompted to enrol an authenticator every time s/he logs on to Windows. The "Welcome" window stops being displayed only after the user has enrolled an authenticator.

In case the policy is not configured or disabled, a NetIQ Advanced Authentication Framework user can prevent the "Welcome" window from being displayed at next logon by selecting the "Do not display at next logon" check box.

At the bottom right of the window are "OK", "Cancel", and "Apply" buttons.

✱ If the policy is enabled, the **Welcome to NetIQ Advanced Authentication Framework System** window will be shown every time a user logs on to Windows until he/she enrolls his/her first authenticator.

✱ If the policy is not defined or is disabled, a user can skip the **Welcome to NetIQ Advanced Authentication Framework System** window at the first logon and the window will not be shown again.

Enable Device Detection for All

The Enable device detection for all policy, if enabled, allows to perform a device detection when logged in without device. *For example*, when using autologon feature and using cards to logon to applications.

The screenshot shows a Windows-style dialog box titled "Enable device detection for all". At the top, there are two buttons: "Previous Setting" and "Next Setting". Below these, there are three radio buttons for configuration status: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of the radio buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. At the bottom left, there is an "Options:" section with a large empty box. At the bottom right, there is a "Help:" section with a text box containing the text: "When this policy is enabled device detection will work when logged in without device. For example when using autologon feature and using cards to logon to applications". At the very bottom, there are three buttons: "OK", "Cancel", and "Apply".

Enhanced Reaction on Device Events

The Enhanced reaction on device events policy allows custom actions during device in and out events. For example, on a thin client the system administrator can configure the plugged out events as follows to disconnect the Citrix session "{PATH}\pnagent.exe / disconnect".

The Enhanced reaction on device events policy works when **NetIQ Client** or **NetIQ RTE** is installed. The policy works only when the user was logged on by the device.

Enhanced reaction on device events

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled Supported on:

Options: Help:

Command line for plugged in event

Command line for plugged out event

When configured this GPO allows for custom actions on device in and out events. For example: On a thin client you can configure the plugged out event as follows to disconnect the Citrix session "{PATH}\pnagent.exe / disconnect".

OK Cancel Apply

In the **Command line for plugged out event** line, you should write the command that will be performed when the device is being plugged out.

 If the policy is not configured or is disabled, no action is set for device plug in and out event.

 If the **Enable device detection for all** policy is enabled, then the **Enhanced reaction on device events** policy works also when the user was logged on by password or by other device.

Force Logoff Once Authenticator is Successfully Enrolled

The **Force logoff once authenticator is successfully enrolled** policy enables/disabled automatic logoff once an authenticator is enrolled.

The screenshot shows a Windows Group Policy configuration window titled "Force logoff once authenticator is successfully enrolled". The window has a standard Windows XP-style interface with a title bar, maximize, minimize, and close buttons. Below the title bar, there are two buttons: "Previous Setting" and "Next Setting". The main area contains three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these radio buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" section with a list box. At the bottom of the main area, there are two sections: "Options:" and "Help:". The "Options:" section contains a label "Force logoff once authenticator is successfully enrolled:" and a dropdown menu currently set to "As user wants". The "Help:" section contains a text area with the following text: "The policy determines the 'Welcome' window behaviour. The 'Force logoff once authenticator is successfully enrolled' setting allows Authasas Advanced Authentication users to log off the current Windows session once they have successfully completed the first authenticator enrollment. The setting has two possible values: 'As user wants' - the user is prompted to choose whether to log off the current Windows session or not; 'Always' - the current Windows session logoff is forced immediately after the 'Welcome' window is closed. In case the policy is not configured or disabled, the current Windows session logoff is not forced." At the bottom right of the window are three buttons: "OK", "Cancel", and "Apply".

The **Force logoff once authenticator is successfully enrolled** setting has two possible values:

- **Always** – enables automatic logoff after successful authenticator enrollment.
- **As user wants** (default) – allows a user to determine whether to log off after successful authenticator enrollment or not.

✖ If the policy is not defined or is disabled, the logoff after successful authenticator enrollment is never forced.

Lifetime of Notification about Password Reset

The **Lifetime of notification about password reset** policy allows the administrator to setup lifetime of user's notification about user's password reset by administrator.

The screenshot shows a Windows-style dialog box titled "Lifetime of notification about password reset". At the top, there are "Previous Setting" and "Next Setting" buttons. Below these, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of the radio buttons is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. In the "Options:" section, there is a label "Lifetime of notification about password reset (in days):" followed by a spin box containing the number "14". To the right of the "Options:" section is a "Help:" section with a text box containing the text: "The policy allows the administrator to setup lifetime of user's notification about user's password reset by administrator." At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

Lifetime of notification about password reset

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on:

Options:

Lifetime of notification about password reset (in days):

14

Help:

The policy allows the administrator to setup lifetime of user's notification about user's password reset by administrator.

OK Cancel Apply

Tap and Go

The **Tap and Go** policy allows the user just to tap the card on the reader and provide the PIN instead of leaving the card on the reader. When tapping the card for the second time, the action configured in the "Interactive Logon Smart card removal behavior" group policy object will be used.

Tap and Go

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on:

Options:

Help:

When enabled this GPO allows full Tap and Go functionality. Instead of leaving the card on the reader it now is possible to just tap the card on the reader and provide the PIN. When tapping the card for the second time the action configured in the "Interactive Logon" Smart card removal behaviour" GPO will be used.

OK Cancel Apply

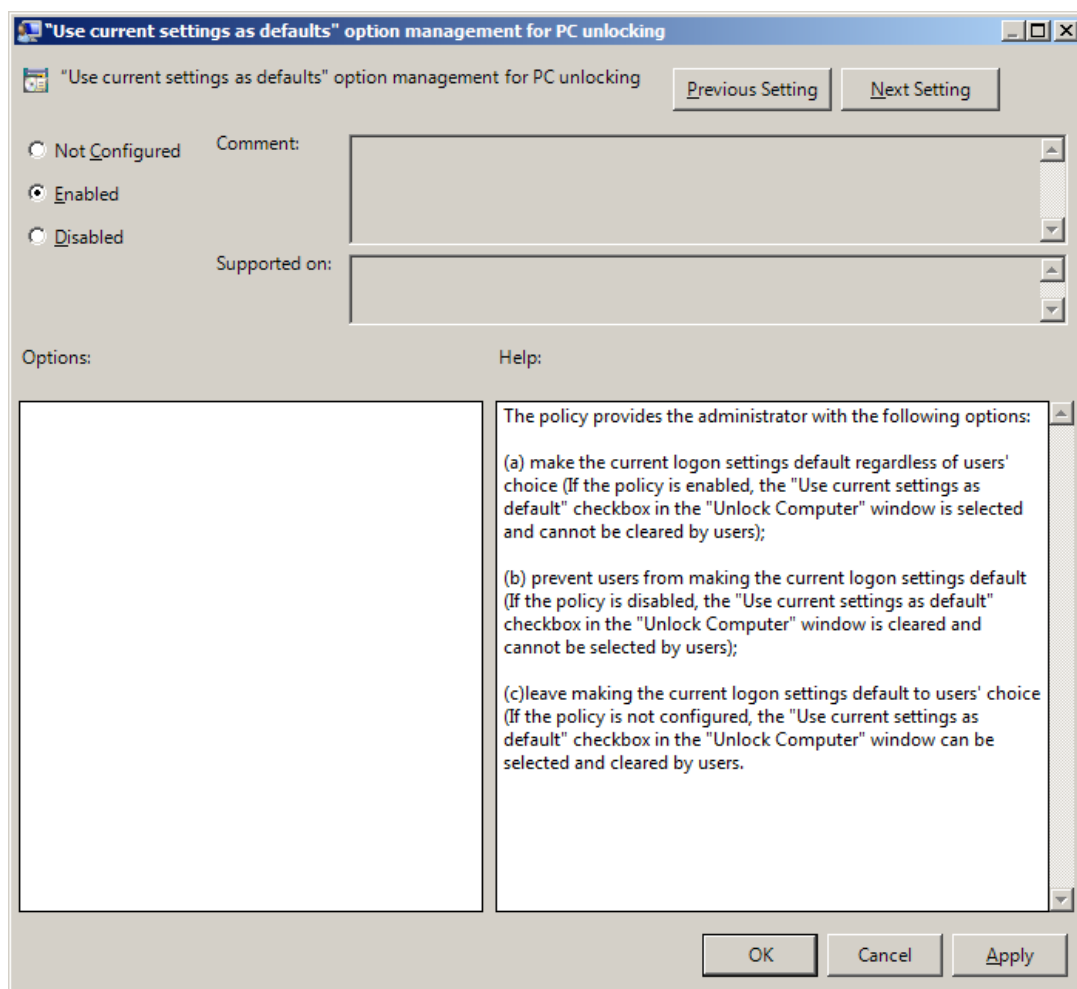
✖ If the policy is not configured or is disabled, user cannot take the card from the reader until the Logon process is finished.

"Use Current Settings as Defaults" Option Management for PC Unlocking

The "**Use current settings as defaults**" option management for unlocking PC policy allows you to manage the **Use current settings as defaults** option in the **Unlock Computer** window.

The policy provides you with the following options:

- force current logon settings as defaults regardless of users' wishes;
- disable the Use current settings as defaults option regardless of users' wishes;
- let users set the current logon settings as defaults if they wish to.



If the policy is enabled, the **Use current settings as defaults** option is always enabled and cannot be cancelled by users.

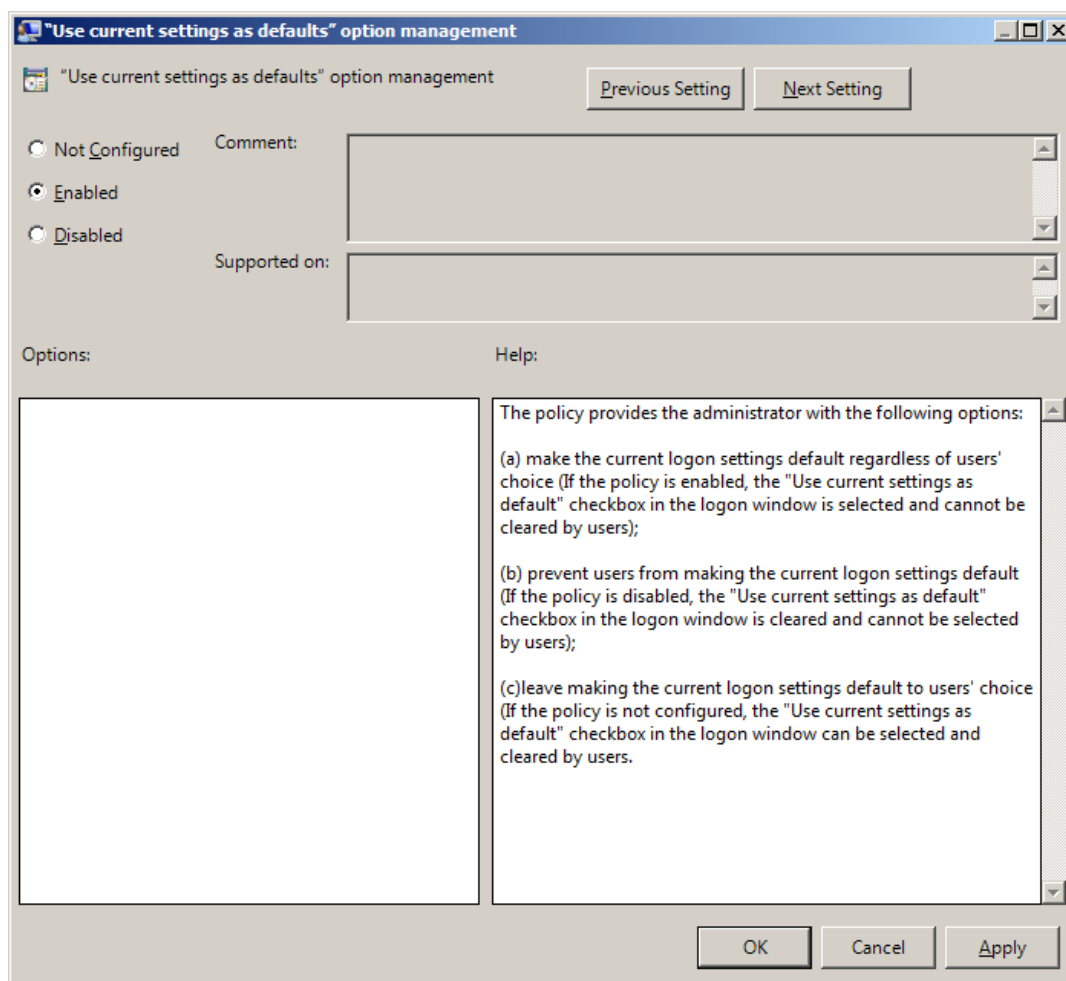
- ✖ If the policy is disabled, the **Use current settings as defaults** option is always disabled and cannot be selected by users.
- ✖ If the policy is not configured, the **Use current settings as defaults** option is enabled and can be selected or cancelled by users.

"Use Current Settings as Defaults" Option Management

The "Use current settings as defaults" option management policy allows you to manage the **Use current settings as defaults** option in the **Logon** window.

The policy provides you with the following options:

- force current logon settings as defaults regardless of users' wishes;
- disable the **Use current settings as defaults** option regardless of users' wishes;
- let users set the current logon settings as defaults if they wish to.



If the policy is enabled, the **Use current settings as defaults** option is always enabled and cannot be canceled by users.

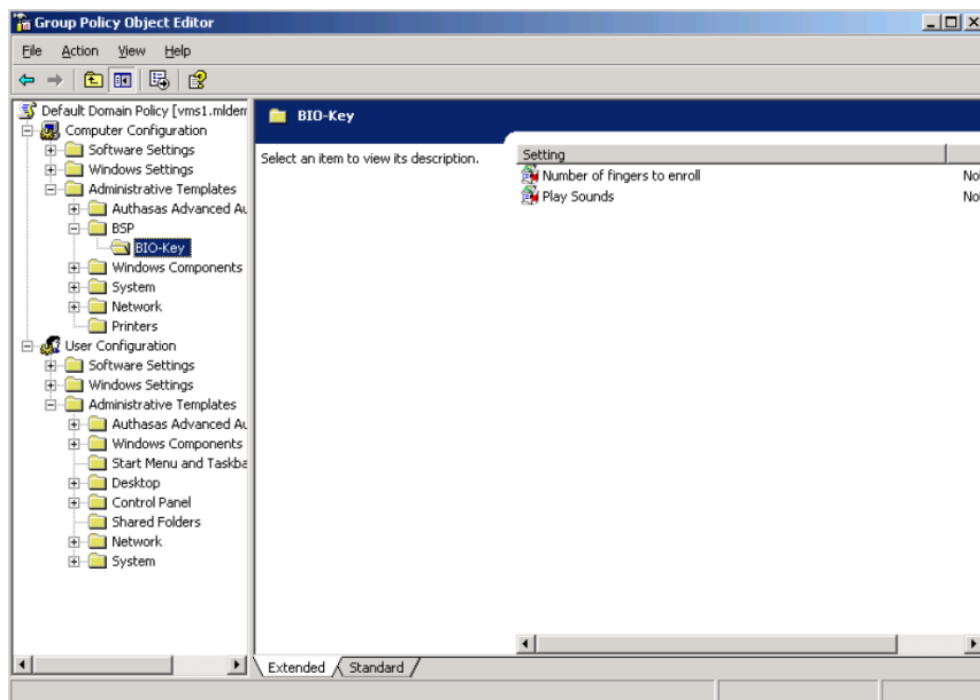
 If the policy is disabled, the **Use current settings as defaults** option is always disabled and cannot be selected by users.

 If the policy is not configured, the **Use current settings as defaults** option is enabled and can be selected or cancelled by users.

BSP Policies

The **BSP** section includes policies allowing you to modify enrollment parameters.

- i** To view authentication provider policies (for Microsoft Windows Server 2003 only)
- In the tree, select **BSP > BIO_key**.
 - Click **View** and select **Filtering**.
 - Uncheck **Only show policy settings that can be fully managed** and click **OK**.



It includes:

- [Number of fingers to enroll](#);
- [Play Sounds](#).

Number of Fingers to Enroll

The **Number of fingers to enroll** policy allows you to specify the number of fingers a user can enroll. This policy is valid only for Bio-Key authentication provider.

The screenshot shows a Windows-style configuration window titled "Number of fingers to enroll". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. In the "Options:" section, there is a label "Number of fingers to enroll" followed by a spinner box containing the value "3". To the right of this is a "Help:" section with a text box containing the text: "The number of fingers that are required to be enrolled during an enrollment. The value can range from 1 to 10. Default value is 3." At the bottom right of the window are "OK", "Cancel", and "Apply" buttons.

A user can enroll from 1 to 10 fingers. The default number of fingers to enroll is **3**.

 If the policy is not configured or is disabled, a user can enroll as many fingers they choose (from 1 to 10).

Play Sounds

The **Play sounds** policy allows you to enable sounds during enrollment process.

Play Sounds

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on:

Options:

Help:

If this policy is enabled, then the BSP user interface will play sounds during the enrollment process when a finger is placed on the reader or when a finger is lifted up from the reader.

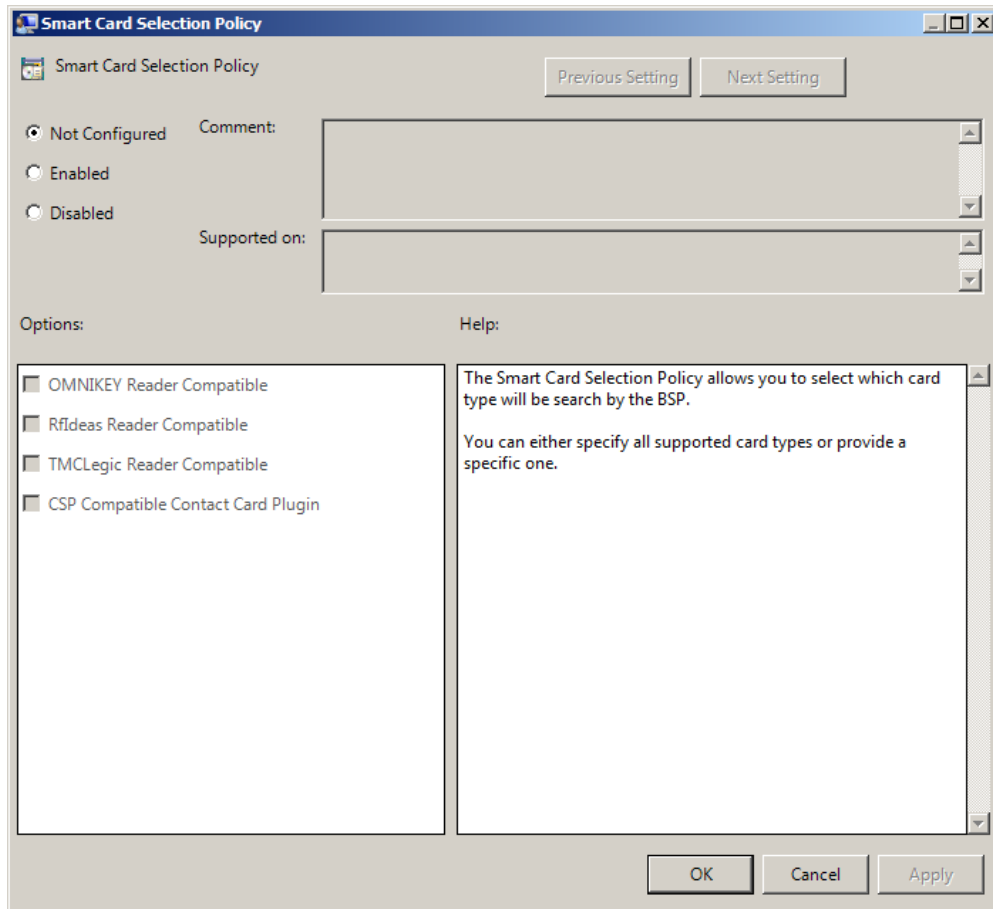
If the policy is disabled or not configured, then the sounds will be turned off.

OK Cancel Apply

 If the policy is not configured or is disabled, the sounds are turned off.

Smart Card Selection Policy

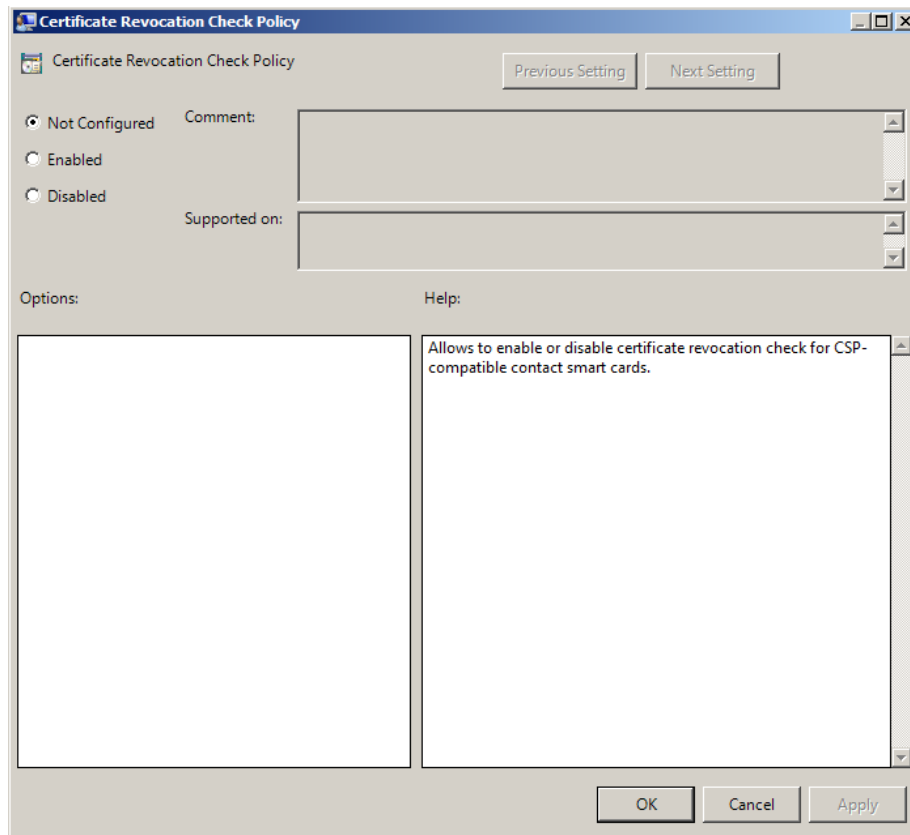
The **Smart Card Selection Policy** allows you to select which card type will be searched by BSP. You can either specify all supported card types or provide a specific one.



 After the **Smart Card Selection Policy** is applied, it is necessary to restart computer for the new values to take effect.

Certificate Revocation Check Policy

The **Certificate Revocation Check Policy** allows to enable or disable certificate revocation check for CSP-compatible contact smart cards.



 After the **Certificate Revocation Check Policy** is applied, it is necessary to restart computer for the new values to take effect.

OMNIKEY Smart Card Selection Policy

The **Omnikey Card Selection Policy** allows you to select which card type will be searched by OMNIKEY Plugin. You can either specify all supported card types or provide a specific one.

The screenshot shows a Windows-style dialog box titled "OMNIKEY Smart Card Selection Policy". At the top, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured" (selected), "Enabled", and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. Underneath, there are two sections: "Options:" and "Help:". The "Options:" section contains three checkboxes: "Proximity Card", "Contactless Card", and "I2C Card", all of which are currently unchecked. The "Help:" section contains a text box with the following text: "The Omnikey Card Selection Policy allows you to select which card type will be search by the OMNIKEY Plugin. You can either specify all supported card types or provide a specific one." At the bottom right of the dialog box are three buttons: "OK", "Cancel", and "Apply".

 After the **OMNIKEY Smart Card Selection Policy** is applied, it is necessary to restart computer for the new values to take effect.

Repository Policies

The **Repository** section includes policies that allow you not to extend Active Directory Scheme.

It includes:

- [Repository](#);
- [ADAM settings](#).

Repository

The **Repository** policy allows you to choose whether to use native Active Directory or ADAM/AD-LDS as NetIQ repository.

The screenshot shows the 'Repository' policy configuration window. At the top, there are 'Previous Setting' and 'Next Setting' buttons. Below these, there are three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of the radio buttons is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' text box. In the 'Options:' section, there is a 'Repository Type' dropdown menu with 'ADAM instance' selected. To the right of the dropdown is a 'Help:' text box containing the following text: 'Choose to use native Active Directory or ADAM / AD-LDS as the NetIQ repository. When Native Directory is used and the schema is not extended please configure the AD Settings GPO (AAA_REPOSITORY_AD.adm). If ADAM is chosen make sure the ADAM Settings GPO (AAA_REPOSITORY_ADAM.adm) is also configured.' At the bottom right, there are 'OK', 'Cancel', and 'Apply' buttons.

When **Native Directory** is used and the schema is not extended please configure the AD Settings GPO (**NAAM_REPOSITORY_AD.adm**).

If **ADAM** is chosen, make sure the ADAM Settings GPO (**NAAF_REPOSITORY_ADAM.adm**) are also configured.

ADAM Settings

The **ADAM settings** policy allows you to configure if ADAM/AD-LDS is used as repository.

The screenshot shows the 'ADAM Settings' dialog box. At the top, there are 'Previous Setting' and 'Next Setting' buttons. Below these, there are three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these is a 'Comment:' text area. Below the radio buttons is a 'Supported on:' text area. In the 'Options:' section, there is a text box for 'LDAP path to root element' containing 'CN=NAAF' and a spin box for 'ADAM servers port number' set to '50000'. In the 'Help:' section, there is a text box containing the text 'Configure if ADAM / AD-LDS is used as repository.'. At the bottom right, there are 'OK', 'Cancel', and 'Apply' buttons.

ADAM Settings

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on:

Options:

LDAP path to root element
CN=NAAF

ADAM servers port number 50000

Help:

Configure if ADAM / AD-LDS is used as repository.

OK Cancel Apply

Enable Novell Support

The **Enable Novell Support** policy allows you to activate the support mode of Novell Domain Services for Windows for the case if you are using Active Directory Lightweight Directory Services for NetIQ data storage in domain based on Novell eDirectory.

After applying the policy the domain root binds to the NetIQ settings.

If you decide not to apply this policy, the NetIQ will not work properly, - you will have a problem with 1-N authentication.

UI Look & Feel Policies

The **UI Look & Feel** section includes policies designed for terminal clients.

Show OSD Num Pad

When enabled this policy provides an **On Screen Keyboard** option during logging on. It is designed for keyboard-less terminals.

The screenshot shows a Windows-style dialog box titled "Show OSD Num pad". At the top right are "Previous Setting" and "Next Setting" buttons. Below the title bar, on the left, are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" label followed by a text area. Below the radio buttons is a "Supported on:" label followed by another text area. At the bottom left is an "Options:" label followed by a large empty text area. At the bottom right is a "Help:" label followed by a text area containing the text: "When enabled this GPO will show an On Screen Keyboard during login. Designed for terminals without keyboard." At the very bottom are "OK", "Cancel", and "Apply" buttons.

Radius BSP

- **Auto enroll** - if the policy is enabled, the enroll dialog will not be shown, the user name will be auto filled and the result authenticator will be saved.
- **Auto fill domain** - if the policy is enabled and domain is not specified (either in DOMAIN\USERNAME or USERNAME@DOMAIN), then BSP will use default domain (from policy or primary) and format template as (DEFAULT DOMAIN\USERNAME).

Pin Required

When this policy is enabled, a Pin code will be needed besides the OTP. If this policy is changed, users will need to re-enroll.

Troubleshooting

In this chapter:

- [Error Initializing User Viewer Snap-in;](#)
- [User Authentication Error;](#)
- [Users Settings in ADUC are not Active;](#)
- [Time Drift.](#)



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

When you contact support service

Please when you turn to support service for help, describe the problem as precisely as you can and attach logs from the PC, on which the problem occurred. To create logs, use LogCreator tool that is located on the installation disk in **\Tools\LogCollector** folder.

To get logs

1. Copy **LogCreator.exe** file to C:\ drive of the faulty computer. Successful tool launch from a network drive cannot be guaranteed.
2. Run the tool.
3. In the opened dialog click **Enable all**. As a result, all components in **Debugged components** section are selected.
4. Close the dialog.
5. Repeat the steps that you performed before the problem occurred.
6. Run the tool again and click **Save logs**.
7. Save the logs in archive file.

Error Initializing User Viewer Snap-In

Description:

The system cannot initialize User Viewer opened from the .msc file after NetIQ Advanced Authentication Framework system has been re-installed. The following error message is displayed: "Snap-in Initialization failed. An invalid pathname was passed".

Solution:

Add the snap-in to console and save it to file again.

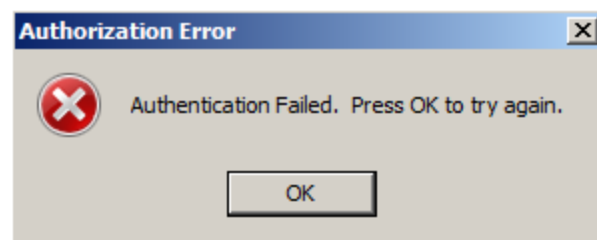
User Authentication Error

Description:

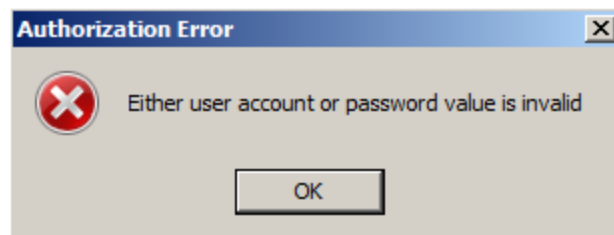
The user cannot log on and receives an error message.

Cause:

a) This error message is displayed if the user entered the wrong account name or if authenticators do not match.



b) This error message is displayed if the user entered the wrong account name or password when logging on with password.



This message may also indicate that a random password was generated for the user account.

c) The message is displayed if

- Authenticore server has not been restarted after authentication providers installation;
- Authenticore server or Domain Controller is unavailable;
- There is time drift between the Authenticore server and the user's workstation;
- Authenticore Server is installed on Microsoft Windows Server 2008™ with enabled firewall. In this case error message may also be displayed when switching to NetIQ Advanced Authentication Framework tab on Properties dialog for user/computer in Active Directory Users and Computers.

Solution:

a), b) The user should check the credentials and try to log on again. In case the error persists, the authenticator will have to be re-enrolled or Active Directory password reset. Resetting Active Directory password for the user automatically clears all enrolled authenticators and allows the user to log on again.

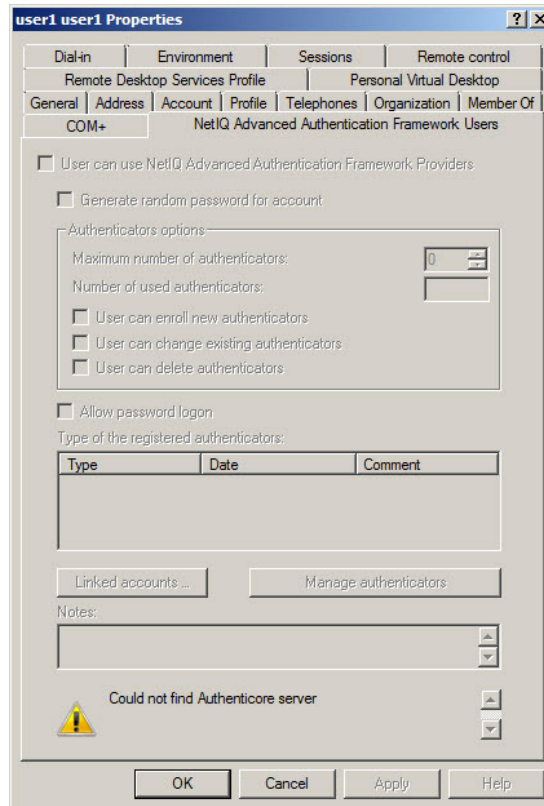
c) To solve the defined problems

- Restart all Authenticore servers where authentication providers are installed;
- Check that Authenticore server and Domain Controller are available;
- Keep Authenticore server and user workstations synchronized;
- Change firewall settings for Authenticore server: add **rpcserver.exe** and **rmevent-server.exe** services to the exception list Remote Service Management. After that the user can log on again and enroll new authenticators.

NetIQ Users Settings in ADUC are not Active

Description:

The NetIQ administrator cannot edit setting on **NetIQ Users** tab in ADUC.



Cause:

- a) NetIQ server is not available.
- b) Server hasn't been started.

Solution:

- a) Check network and Firewall settings.
- b) Start the server.

Time Drift

Description:

A time drift between an Authenticore server and user workstations causes authentication problems. Successful authentication depends a great deal on authenticator life period specified by **Authenticator life period** policy. By default, authenticator life period is 5 minutes. If time divergence exceeds 5 minutes, NetIQ Advanced Authentication Framework system treats this as potential risk. In such case the log on a Log Server and the local NetIQ Advanced Authentication Framework log on Authenticore server contains the following error message: *"EventID: 1123 Error: Time interval from the moment the user authenticator was obtained and the moment it was delivered to the Authenticore server exceeds the value of the settings, which regulates authenticator validity period (5 minutes by default). This error can occur as a result of either system time drift between user computer and Authenticore server or criminal attempt to use authenticator intercepted over network"*.

Solution:

Keep users' workstations synched with Authenticore server.

Index

A

Account 78-79
Active Directory 7, 9-10, 12-13, 15-18, 24, 38, 40, 44-45, 49, 57, 65, 116, 126
Administrator 1, 5-6, 12-13
ADUC 16-17, 40, 55, 127
Authentication 1, 5-6, 8-9, 11-13, 15-18, 24, 37-38, 40-41, 45, 48-49, 52, 54-55, 58-60, 64, 83, 88, 93-94, 96-97, 99, 125-126, 128
Authenticator 5, 10-11, 22, 32, 34-36, 38, 57, 64, 73, 96, 103, 128
Authenticore server 13, 60, 74, 126, 128
Autologon 48
Automatic logon 48

B

BIO-key 14

C

Caching 45, 77, 83
Card 14, 81, 112, 115
Client 6, 9, 13, 46, 64, 78, 93-94, 101
Client Tray 64, 91, 97
Comment 23, 25, 33-34
Connection 98
Console 49, 52, 66
Control 10-11, 15-16, 24, 41
Create 17, 58
Credential providers 64, 75
Current authenticator 10

D

Data 58
Default 66
Delete 53
Device 100-101
Dial-up 65, 91, 98
Domain 10-11, 15, 66, 94, 120, 126

E

Edit 17

Enroll 10-11, 20, 31-32, 34-35, 53, 56, 111
Enterprise Key 7, 10-11
Error 78, 124-125, 128
Event Log 64, 69, 85
Event Viewer 59-60
Export 58

F

File 49

G

Generate 20, 25, 64, 76
GINA 48, 64, 91, 94
GPMC 66
GPME 66

K

Key 111

L

Linked accounts 27
List 61, 77, 83
Local 60
Logo 64, 91, 94
Logon 5, 30, 55, 58, 65, 78, 98, 105, 108
Lumidigm 14

M

Manage 26, 30, 37, 55
Microsoft Windows Server 2003 110
Microsoft Windows Server 2008 38

N

Network 13
Notification 104

O

OATH 14
OTP 123

P

Password 13, 38, 64, 73, 76, 79, 89
PIN 14, 64, 73, 77, 81-83, 105
Policy 13, 66, 72, 112, 114-115
Properties 9, 37, 40, 47, 55, 126

R

RADIUS 14
Re-enroll 10-11, 35, 53
Reference authenticator 10
Remote 126
Remove 17, 36, 49, 67
Reset 17
RTE 7, 9, 14, 46, 101

S

Screen 121
Security 9-10, 12, 64, 66, 73, 83
Server 6, 11-13, 15, 59, 85, 126-128
Settings 73, 75, 97, 106, 108, 117, 119, 124, 127
Support 48, 120
System 10, 12, 60, 99

T

Test 23, 31-32, 34, 56

U

User 9-10, 12, 18, 22, 24, 33, 38, 40, 52, 55, 70, 90, 124-125
User Viewer 9, 12-13, 16, 44, 49, 52, 54-55, 58, 125

W

Window 99
Windows 7, 11, 14-15, 48, 64, 66, 94, 97, 99
Windows Vista 91
Workstation 12, 64, 91