



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	18
Creating New User	19
Enrolling Authenticator	23
Editing NetIQ Advanced Authentication Framework User Properties	25
Linked Accounts	28
Managing Authenticators	31
Adding Authenticator	33
Re-enrolling Authenticator	35
Testing Authenticator	36
Removing Authenticator	37
Editing Properties of Multiple NetIQ Advanced Authentication Framework Users	38
Resetting Active Directory Password	39
Removing User	41
Delegating Control	42
Automatic logon in NetIQ Advanced Authentication Framework	46
NetIQ Advanced Authentication Framework User Viewer	47
Adding User Viewer to Console	47
Visual Appearance	50
Viewing Users	52

Managing User Properties	53
Managing Authenticators	53
Adding Authenticator	55
Re-enrolling Authenticator	55
Testing Authenticator	55
Removing Authenticator	55
Data Exporting	57
Logon Methods Report	57
Audit Tools	58
Log Server Setting	58
Event Viewer	59
RPC Server Events	60
SrvWrapper Events	67
Password Filter Events	68
Password Manager Events	68
EventLog Events	69
BioAPI Events	69
Authenticore Server Events	70
Authentication Providers Events	72
Cryptography Events	73
Manager Events	73
Plugins Events	74
Licensing Events	74
Backup Provider Events	75
Administrative Tools Events	75
GINA Events	75
Data Events	76
NPS Events	78
Web Service Events	79
Group Policies	80
Adding Group Policies	83
Security Policies	84
Authenticator Life Period	85
Credential Providers Filter Settings	87
Default method for Other user	89
Disabled PIN Host List	90
Disable Random Password Generation by Default	92
Do not Allow Administrators to Remove User Credentials	93
Enable Caching	94
Enable PIN Caching	95
Hide password mode from logon UI	97
Lock account on failed logon	98
Number of Cached Users	100
Password Length	101
PIN Restrictions	103
Use domain password as PIN	104

Event Log Policies	106
Freeze Communication If Log Server Is Unavailable	107
Log Servers	109
Register All Password Management Events	111
Register All User Authentication Events	112
Network Policies	113
Always resolve client name	114
Force to use NTLM authentication during logon	115
RPC dynamic port selection allowed	116
RPC static port selection allowed	118
Runtime Environment	120
Show Enrolled Card Owner	121
Users and Groups	122
Customize Users and Group Settings	123
Workstation Policies	125
Alternative Logo for Credential Provider	126
Alternative Logo for GINA and Wizard	128
Deny to Specify Authenticator Comment at Enrollment	130
Deny to Start Client Tray When User Logs on to Windows	131
Disable First Logon Enroll Wizard	133
Disable "Use Dial-up Connection" Option	134
Do Not Allow to Skip Welcome Window	136
Enable Device Detection for All	138
Enhanced Reaction on Device Events	140
Lifetime of Notification about Password Reset	142
Linked Logon Behavior	143
Tap and Go	145
"Use Current Settings as Defaults" Option Management for PC Unlocking	146
"Use Current Settings as Defaults" Option Management	148
Web service client timeout	150
Repository Policies	151
ADAM Settings	152
Enable Novell Support	153
Repository	154
UI Look & Feel Policies	156
Show Cache Messages	157
Show OSD Num Pad	158
Configuration of Windows Firewall with Advanced Security	159
Troubleshooting	160
Error Initializing User Viewer Snap-In	161
User Authentication Error	161
NetIQ Users Settings in ADUC are not Active	163
Time Drift	164
Index	165

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

In this chapter:

- [About NetIQ Advanced Authentication Framework™](#)
- [NetIQ Advanced Authentication Framework™ Technology](#)
- [NetIQ Advanced Authentication Framework™ Administrative Tools](#)

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 unable 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 Authentication Framework 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 catalog. Domain controller allows you to access data stored in the catalog 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 administration 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.
- **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.
- **VDA (Virtual Desktop Authentication)** allows to use pre-session and in-session authentication for the following terminal server connections: Microsoft RDP, Citrix XenApp, VMware View on thin clients.

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

- Authentec authentication provider;
- BIO-key+PIN authentication provider;
- Digital Persona authentication provider;
- Flash+PIN authentication provider;
- Hitachi Fingervein+Card authentication provider;
- Live Ensure authentication provider;
- Lumidigm authentication provider;
- Lumidigm+Card authentication provider;
- OATH authentication provider;
- RADIUS authentication provider;
- Security Questions authentication provider;
- Smartphone authentication provider;
- SMS authentication provider;
- Voice Call authentication provider;
- Universal Card 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 more details, see the [Working with User Accounts](#) chapter.
- enable and disable the caching of NetIQ Advanced Authentication Framework credentials on a local computer. For more details, see the [Enable Caching](#) chapter.
- add group policy templates and configure the policies. For more details, see the [Group Policies](#) chapter.
- delegate control. For more details, see the [Delegating Control](#) chapter.

- **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

In this chapter:

- [Working with User Accounts](#)
- [Creating New User](#)
- [Enrolling Authenticator](#)
- [Editing User Properties](#)

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 an 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 an 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.

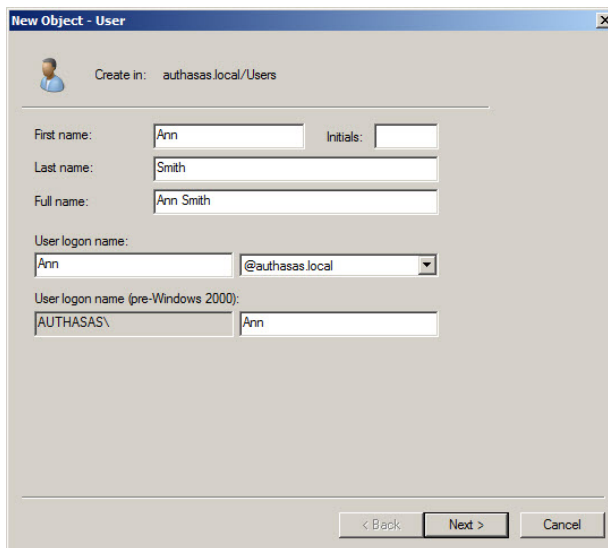
Creating New User

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:

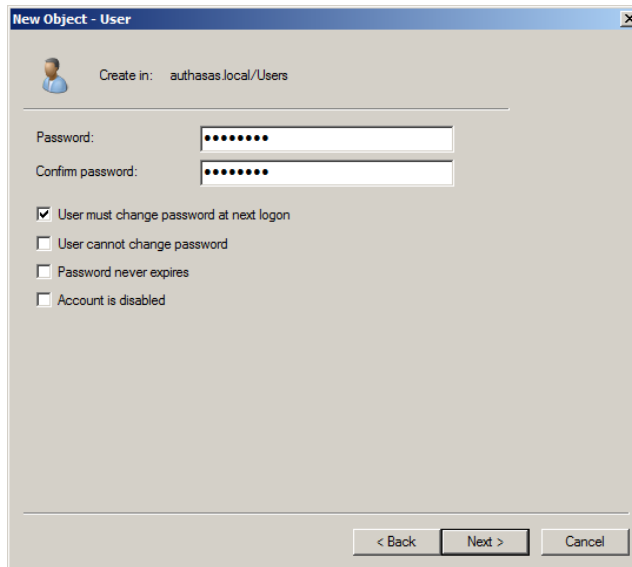
1. In **Active Directory Users and Computers**, select **Organizational Unit/container**.
2. Click toolbar button or right-click the container and select **New > User** or click **Action** and select **New > User**.
3. The **User Creation Wizard** opens.




The screenshot shows the 'New Object - User' dialog box. The 'Create in:' field is set to 'authasas.local/Users'. The 'First name' field contains 'Ann', the 'Last name' field contains 'Smith', and the 'Full name' field contains 'Ann Smith'. The 'User logon name' field is split into a text box with 'Ann' and a dropdown menu with '@authasas.local'. The 'User logon name (pre-Windows 2000):' field is split into a text box with 'AUTHASAS\' and another text box with 'Ann'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

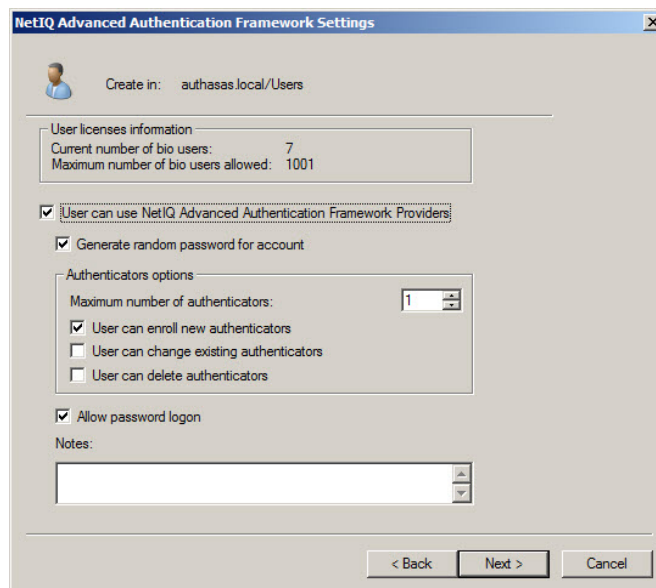
Enter the user name and click **Next >**.

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



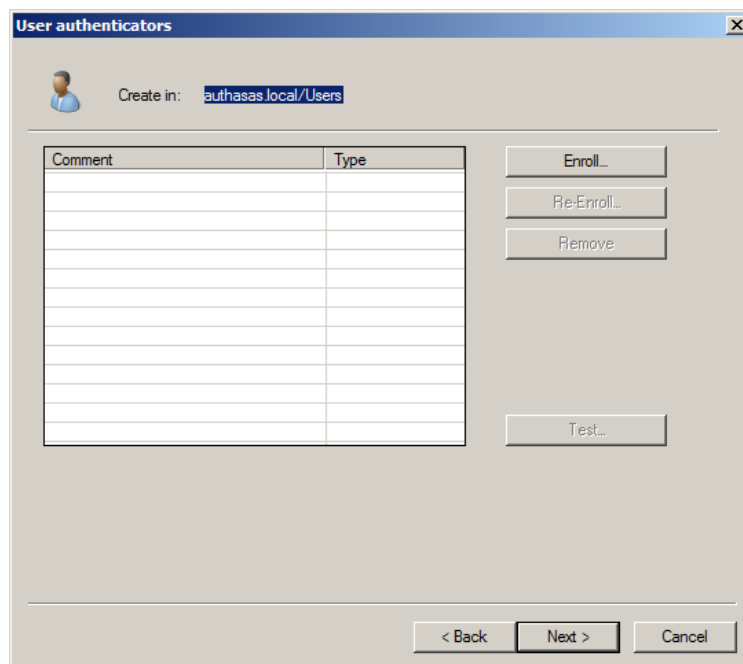
 The following steps (5-6) do not appear in the situation when you use AD attributes, because we should modify schema to have these features.

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



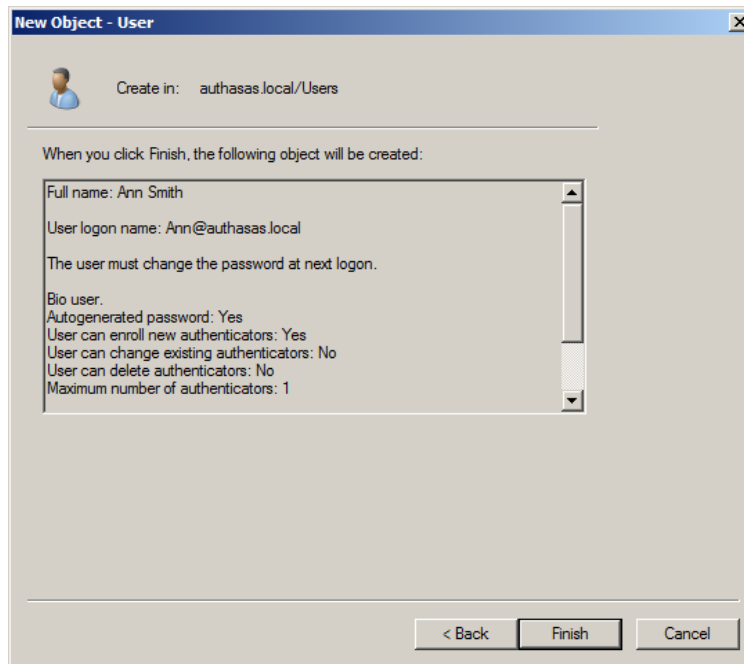
- The **User licenses information** field displays the current number of NetIQ Advanced Authentication Framework users and the limit stated in the user license.

- The **User can use hardware authentication devices** box, if checked, enables the user to use authenticators (in other words, a NetIQ Advanced Authentication Framework user is created).
 - The **Generate random password for account** box, if checked, enables random password generation.
 - The **Authenticators options** allows 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](#)).



Do one of the following:

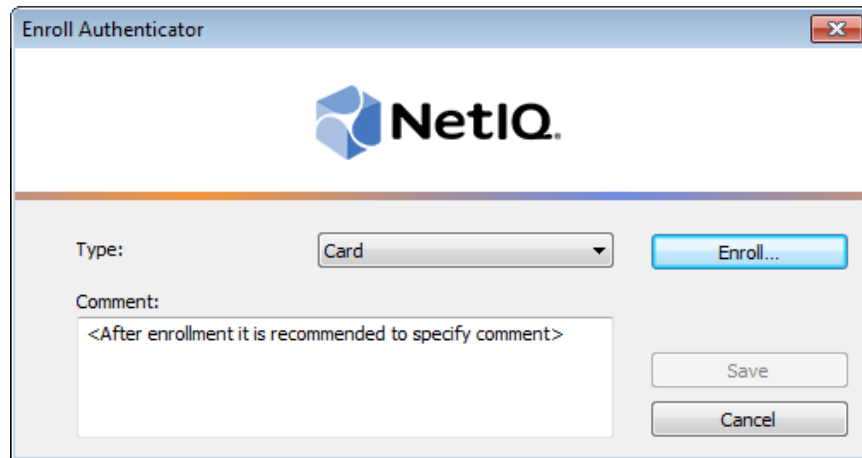
- a. To start enrolling an authenticator, click **Enroll...** (see [Enrolling Authenticator](#)).
 - b. To continue without authenticator enrollment, click **Next**.
7. Check the summary of changes you have made. Click **Finish**.




Enrolling Authenticator

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

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



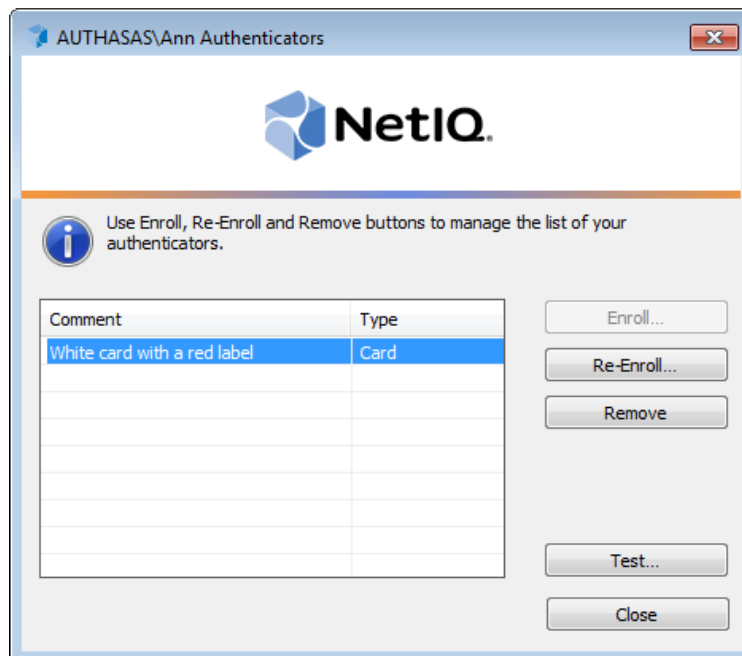
- From the **Type** list, select the required type.
 - Click **Enroll...**
3. You are shown the authentication device screen with instructions to follow, which depend on the selected authentication type. Follow the instructions to enroll authenticator.
 -  For the selected component to function, the authentication provider must have been preliminary installed.
 4. After the 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).

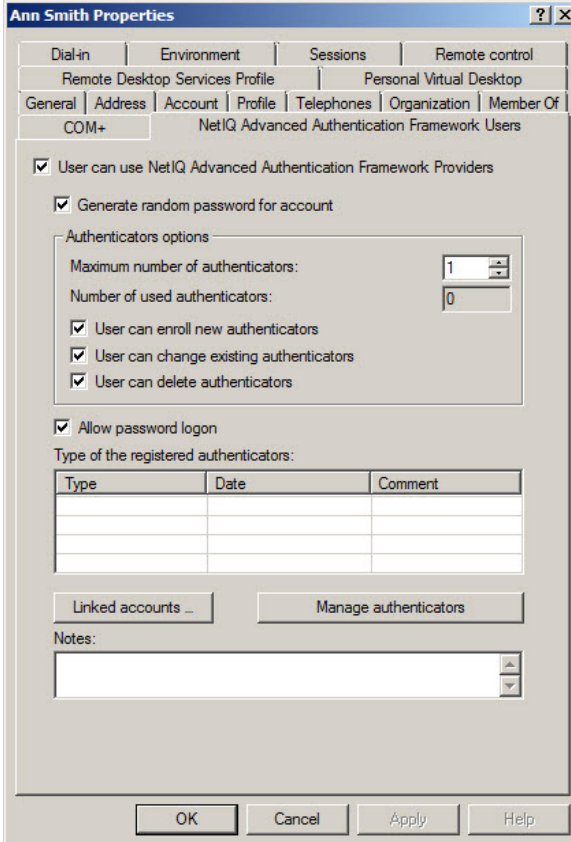


Editing NetIQ Advanced Authentication Framework User Properties

 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 Advanced Authentication Framework Users** tab.



Ann Smith Properties

Dial-in | Environment | Sessions | Remote control
Remote Desktop Services Profile | Personal Virtual Desktop
General | Address | Account | Profile | Telephones | Organization | Member Of
COM+ | **NetIQ Advanced Authentication Framework Users**

User can use NetIQ Advanced Authentication Framework Providers

Generate random password for account

Authenticators options

Maximum number of authenticators:

Number of used authenticators:

User can enroll new authenticators

User can change existing authenticators

User can delete authenticators

Allow password logon

Type of the registered authenticators:

Type	Date	Comment

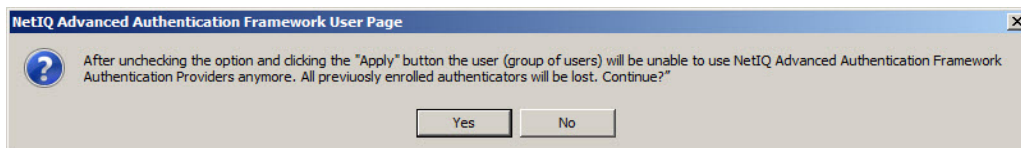
Linked accounts ... Manage authenticators

Notes:

OK Cancel Apply Help

The following settings are available:

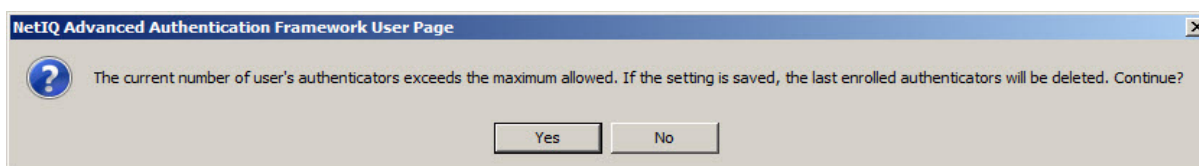
- The **User can use NetIQ Authentication Providers** check box, if selected, enables the user to use authenticators. When you clear the check box, the following dialog is displayed:



! If you clear the check box and save the changes, the user's authenticators will be deleted and he/she 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** check box, if selected, enables random password generation.
- The **Authenticators options** allows 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** check box, if selected, enables the user to add authenticators.
- The **User can change existing authenticators** check box, if selected, enables the user to re-enroll authenticators.
- The **User can delete authenticators** check box, if selected, 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:

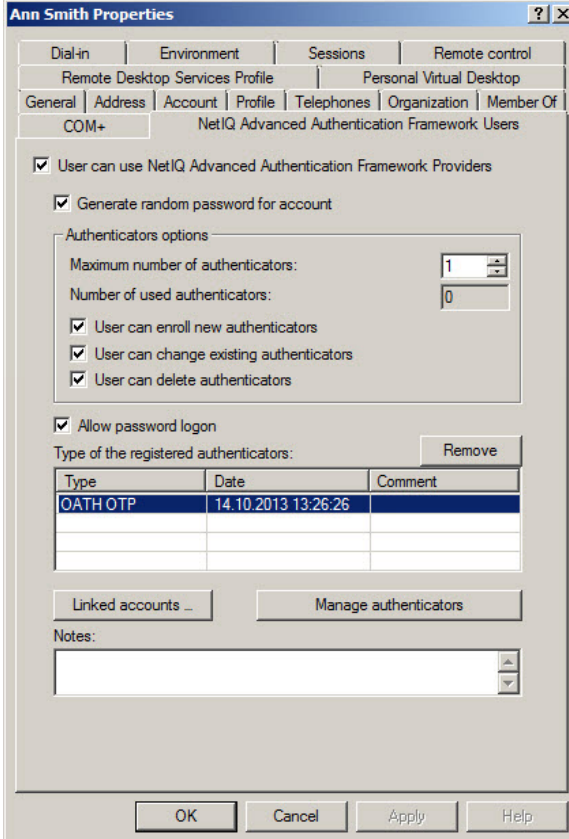


Click **Yes** to remove the most recent authenticators. For example, if the **Number of used authenticators** is 3 and the **Maximum number of authenticators** is set to 1, two most recent authenticators will be removed.

- 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.

 Administrator is provided with the opportunity to delete registered authenticators. To delete the required authenticator, select it and click the **Remove** button (it will be automatically enabled after the selection of the registered authenticator).



Ann Smith Properties

Dial-in | Environment | Sessions | Remote control

Remote Desktop Services Profile | Personal Virtual Desktop

General | Address | Account | Profile | Telephones | Organization | Member Of

COM+ | NetIQ Advanced Authentication Framework Users

User can use NetIQ Advanced Authentication Framework Providers

Generate random password for account

Authenticators options

Maximum number of authenticators: 1

Number of used authenticators: 0

User can enroll new authenticators

User can change existing authenticators

User can delete authenticators

Allow password logon

Type of the registered authenticators:

Type	Date	Comment
OATH OTP	14.10.2013 13:26:26	

Notes:

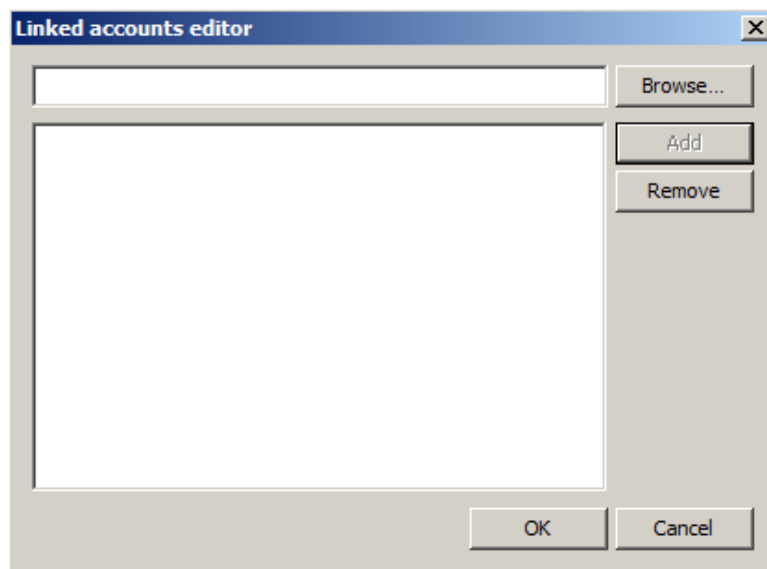
- The **Manage authenticators** button allows you to open the **Authenticators** window (see [Managing Authenticators](#)).
- The **Notes** box allows you to edit a comment to the user's account.

Linked Accounts

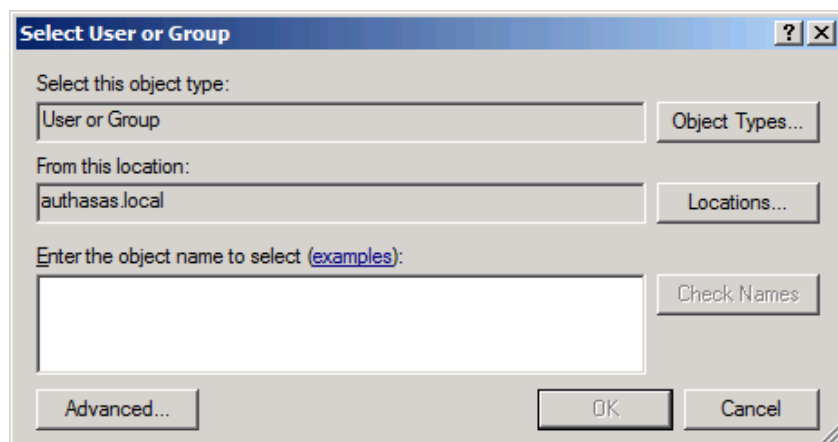
While using linked accounts, you are able to log on to the system as another user, who is linked to you or to the specified group. To log on, you will use your own authenticators.


To link accounts:


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

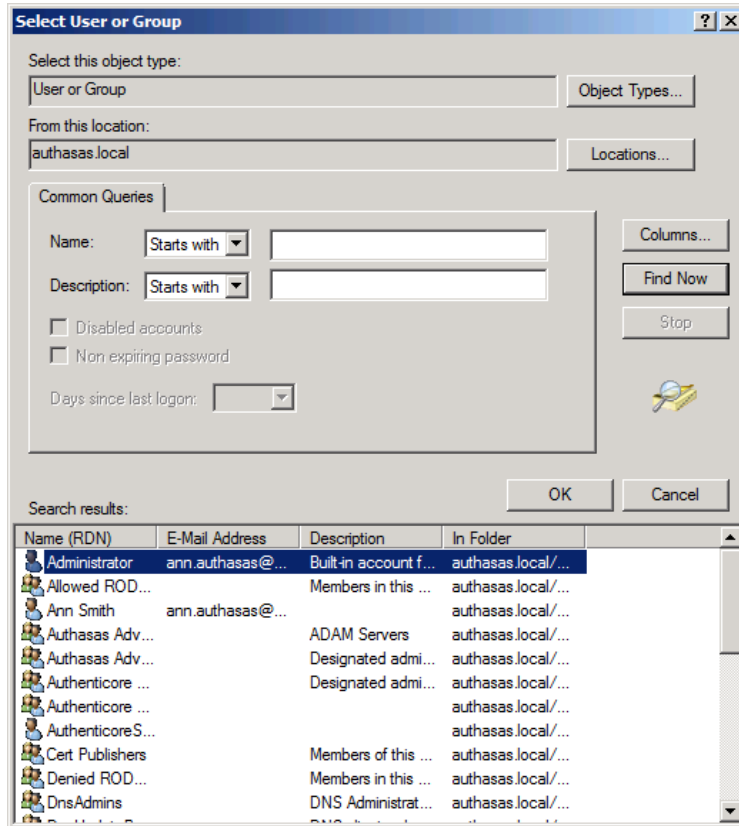


3. To choose a user or group, click **Browse...**
4. In the **Select User or Group** window, type the name of the user or group you want to be linked with. Click **Check Names** to double check, whether you have typed the name correctly. Click **OK**.

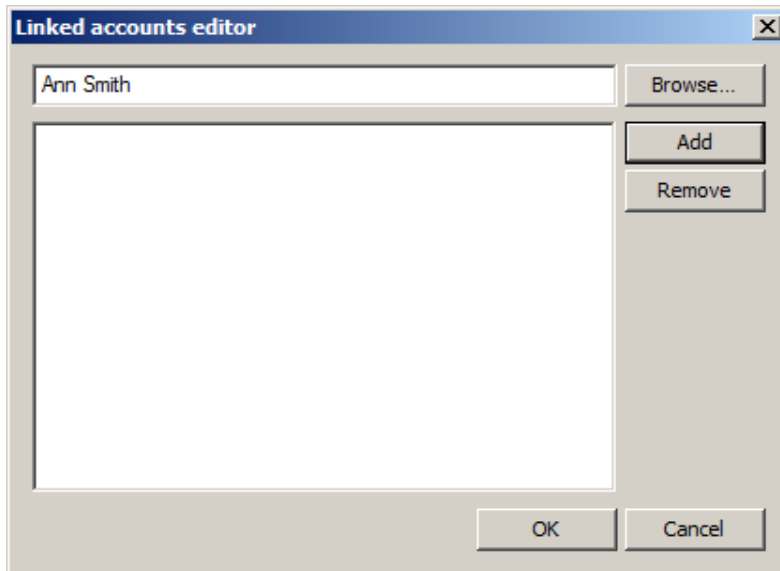


 Adding of primary groups is not supported.

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



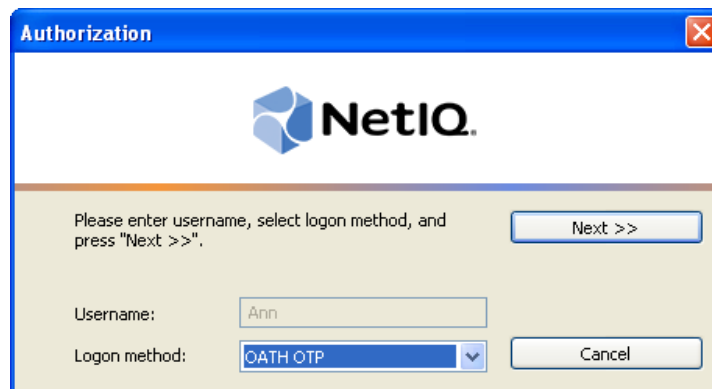
5. After the user name or group name appears in the **Linked accounts editor** window, click **Add** and **OK**.



Managing Authenticators


To manage user's authenticators:


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



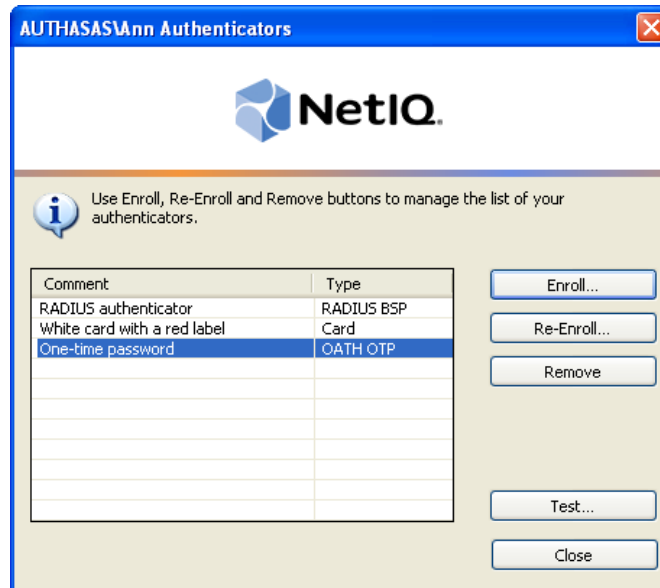
User name and domain name cannot be changed.

- 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.

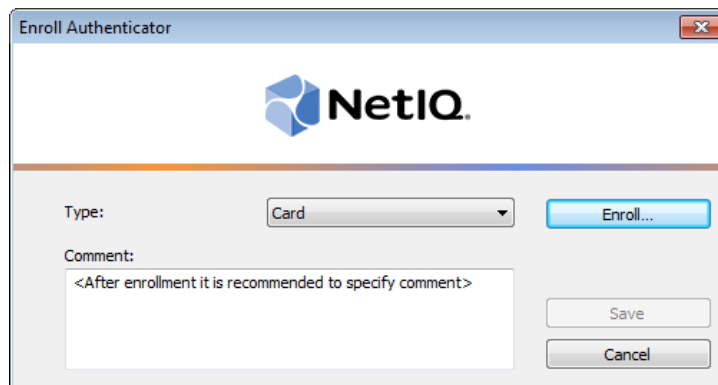


- i** If there are no enrolled authenticators yet, only the **Enroll** button will be active (no matter which way you were authorized).
- i** If some authenticators already exist and you were authenticated with a password, all the buttons except **Test** and **Close** are greyed out.

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**.

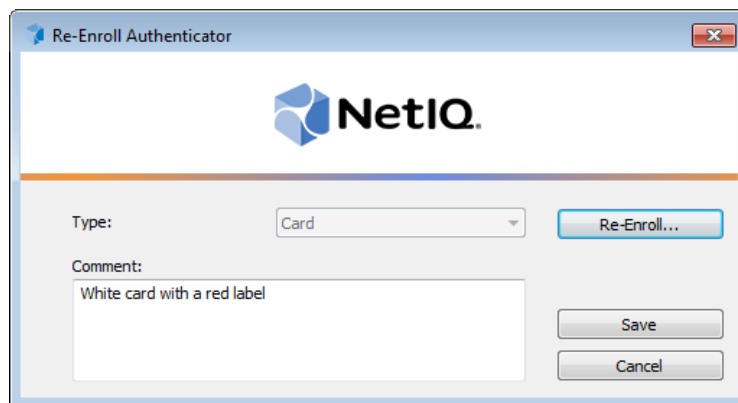
When authenticator is enrolled, a *'Comment – Authenticator type'* record appears on the **User authenticators** page (comment is editable if allowed by the system administrator).

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).

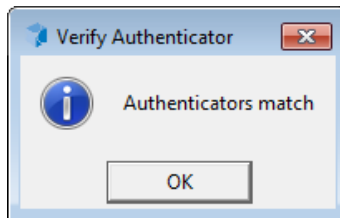
Once authenticator is successfully enrolled you can test authenticator, by clicking the **Test** button (see [Testing Authenticator](#)).

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:



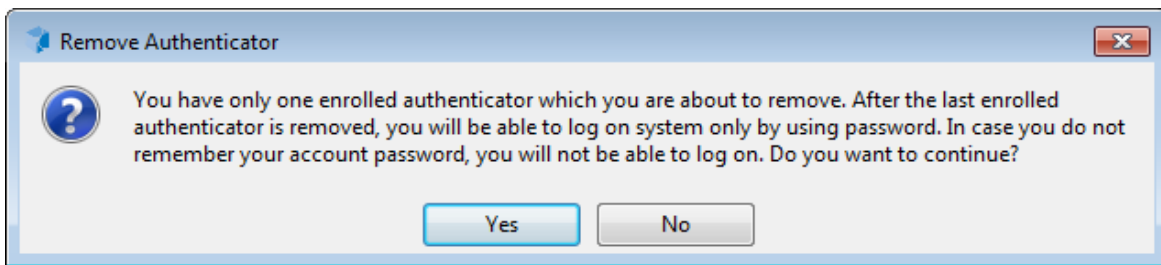
If test has failed, the authentication device screen is shown again. Repeat the procedure or click **Cancel** and re-enroll the authenticator.

Removing Authenticator

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

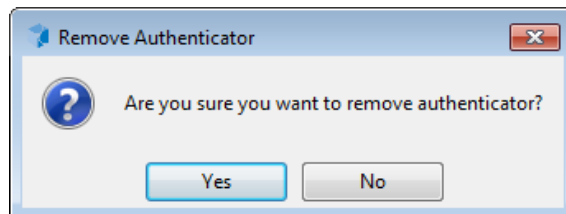
If the user has no authenticators, he/she will be completely unable to log on.

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



To remove an authenticator:

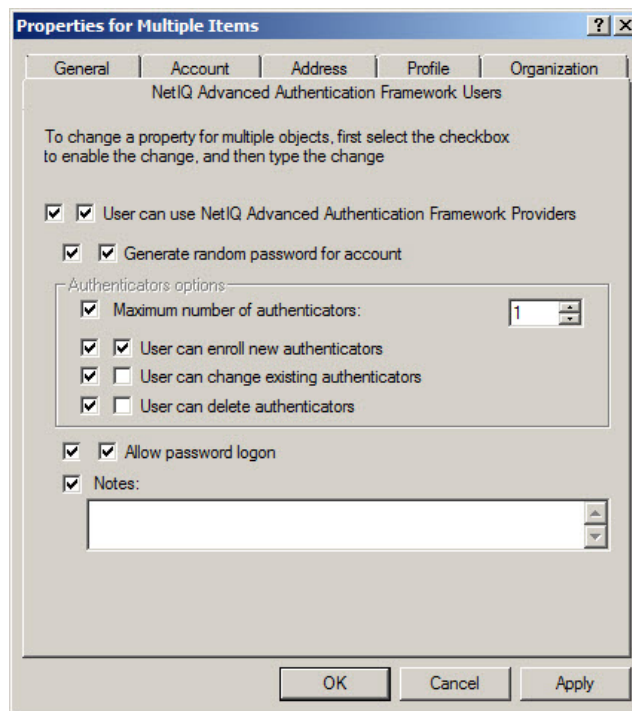
1. In the **Authenticators** window, select the record and click **Remove**.
2. The following dialog is displayed:



Click **Yes**.

Editing Properties of Multiple NetIQ Advanced Authentication Framework Users

1. Hold down **[Ctrl]** and select the users.
2. Open the properties dialog. In the **Properties for Multiple Items** dialog, switch to the **NetIQ Advanced Authentication Framework Users** tab.
3. The **NetIQ Advanced Authentication FrameworkUsers** 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 selected.



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

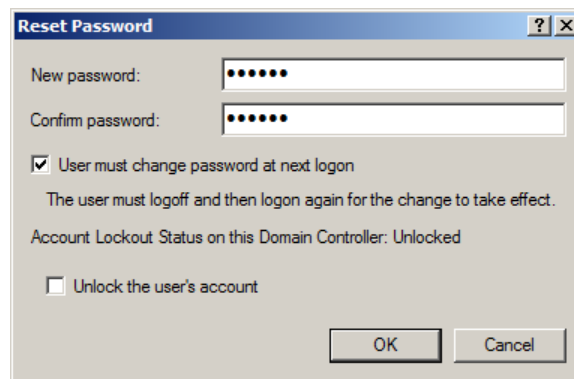
1. Right-click the required **Organization Unit** or group.
2. Select **Properties**, switch to the **NetIQ Users** tab.
3. Make necessary changes and save the changes by clicking **Apply**.

Resetting Active Directory Password

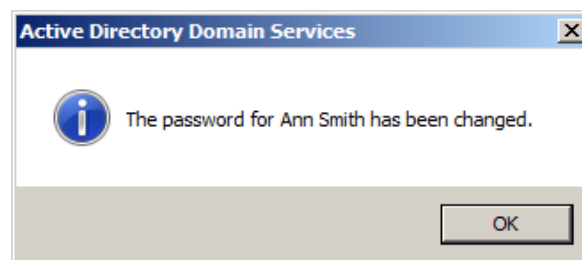
If a NetIQ Advanced Authentication Framework user is allowed to remove authenticators, it may happen that he/she removes all authenticators and will be unable log on with password because it was changed. The user may also lose his/her hardware authenticator or it may be stolen from him/her. Resetting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

i If you select the **User must change password at next logon** check 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 the **Unlock user's account** check box. If you select this check box, the user's account will be unlocked if it was previously locked:



If the password is changed successfully, you will 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 did not request a password reset, he would know 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

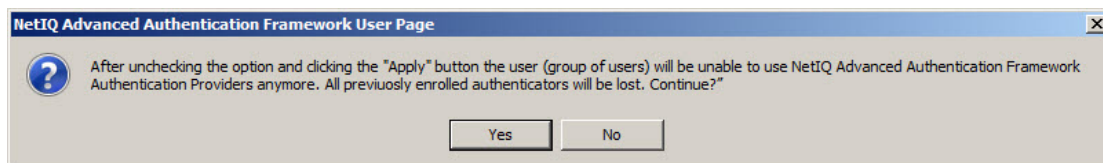
You can remove a NetIQ Advanced Authentication Framework user (that is, forbid an Active Directory user to use NetIQ Advanced Authentication Framework authenticators) or remove an Active Directory user account. When you withdraw the permission to use authenticators from a user, existing authenticators 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 clear the **User can use hardware authentication devices** check box in order to have a free license. Otherwise, the license will be invalid.

Removing a NetIQ Advanced Authentication Framework User

To delete a NetIQ Advanced Authentication Framework user:

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



- Click **Yes**.
- Click **Apply** on the **NetIQ Advanced Authentication Framework Users** tab.

! If you clear the check box and save the changes, user's authenticators will be removed and he/she 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** check box is cleared.

Delegating Control

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

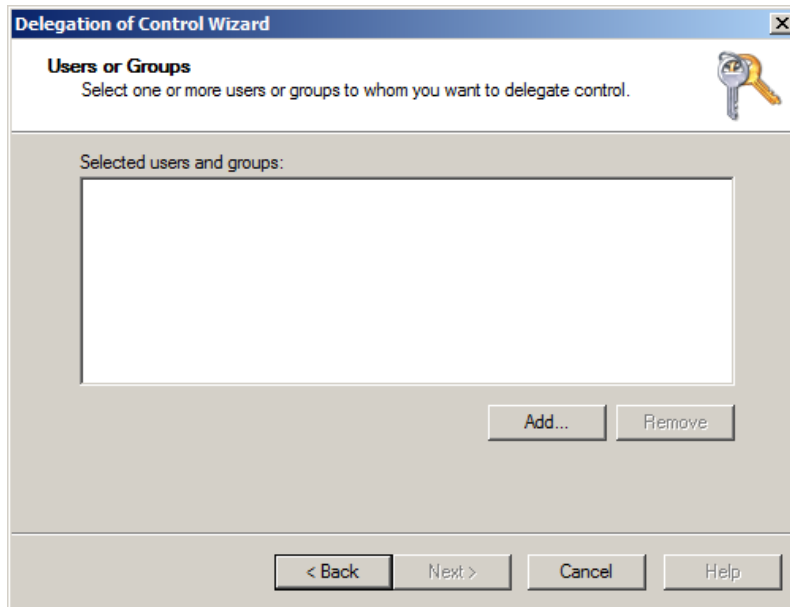
Delegating control means giving control over NetIQ Advanced Authentication Framework settings to a user or a group of users within a container/organizational Unit.

To delegate control:

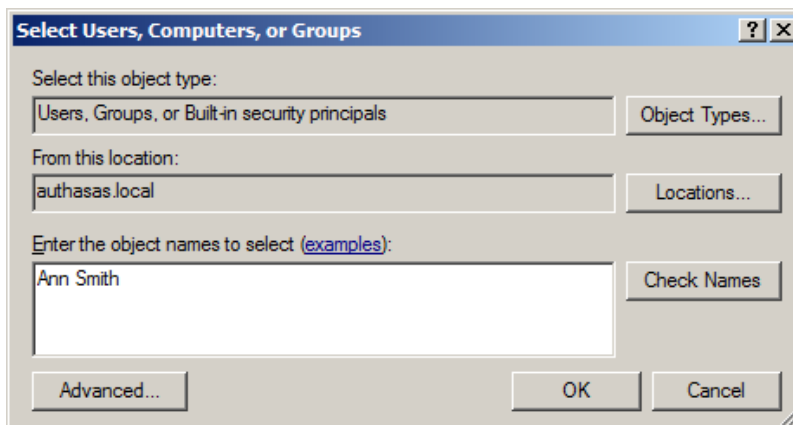
1. Right-click the container/organizational unit and select **Delegate Control**.
2. The **Delegation of Control Wizard** is started. Click **Next >** to continue.



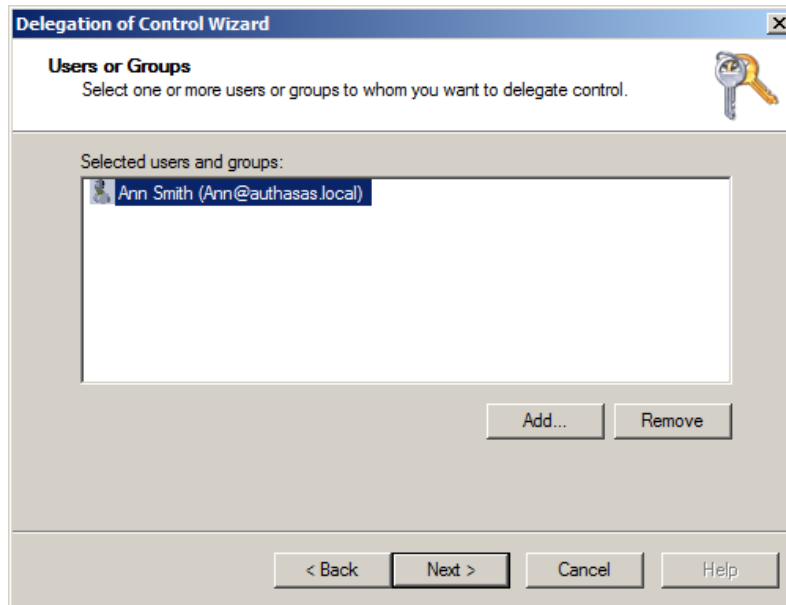
3. Click **Add...**



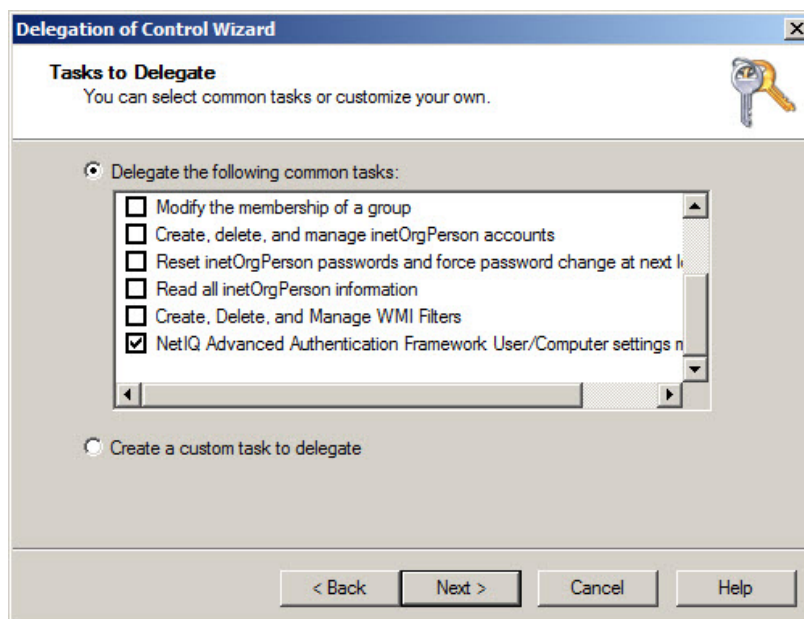
4. Enter the name of a user/group and click **OK**.



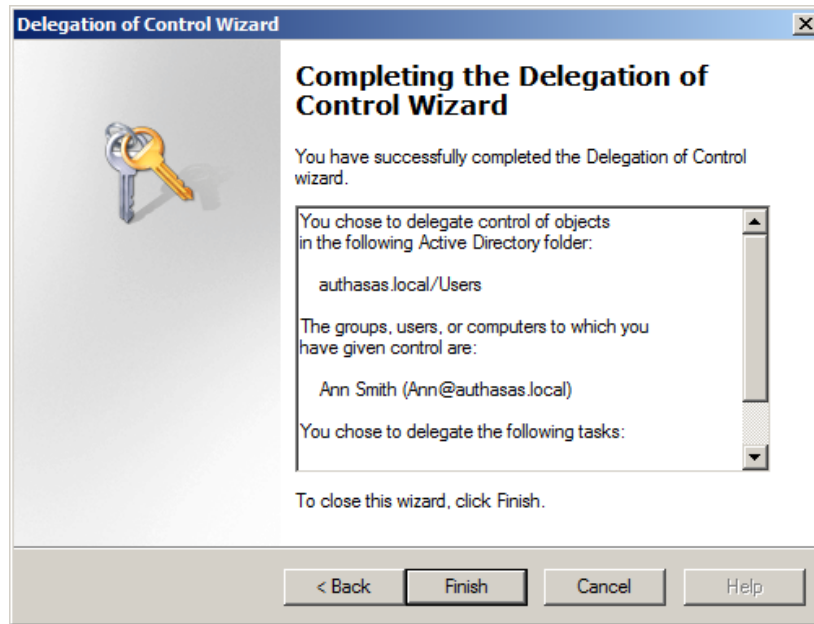
5. The name of selected user/group is displayed on the **Users or Groups** page. Click **Next>** to continue.



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




7. Click **Finish** to exit the **Delegation of Control 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.

Automatic logon in NetIQ Advanced Authentication Framework

 The Automatic logon feature is available only in operational systems based on GINA (e.g., 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 the [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.

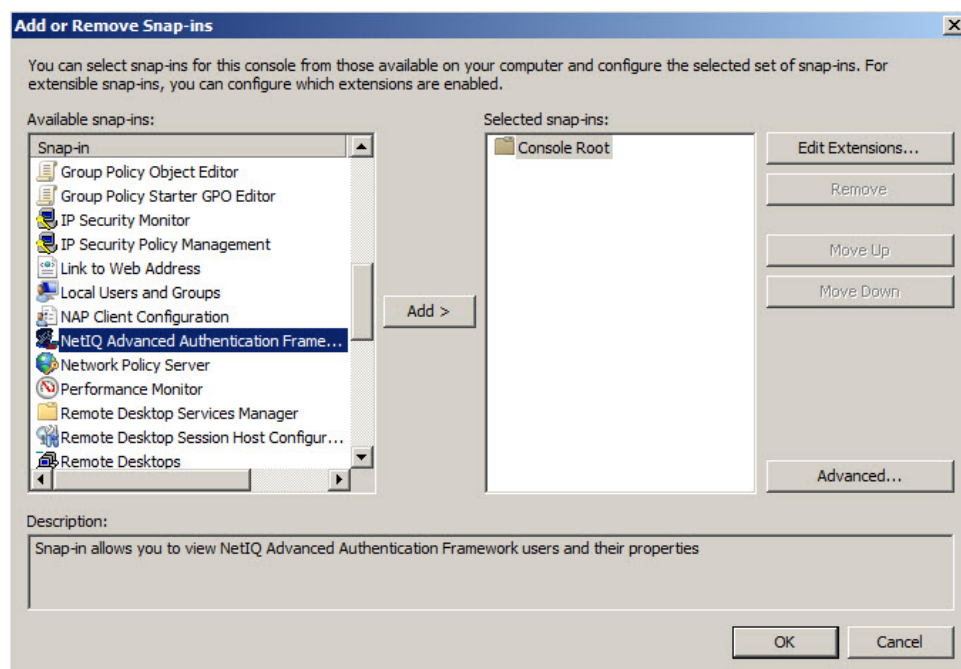
NetIQ Advanced Authentication Framework User Viewer

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.

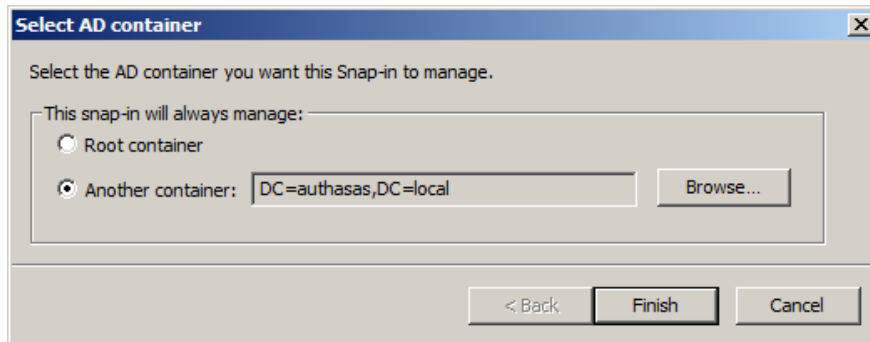
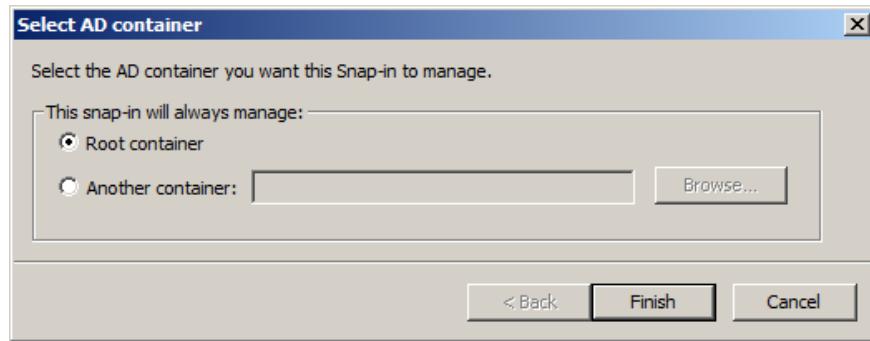
Adding User Viewer to Console

To add NetIQ Advanced Authentication Framework User Viewer to console:

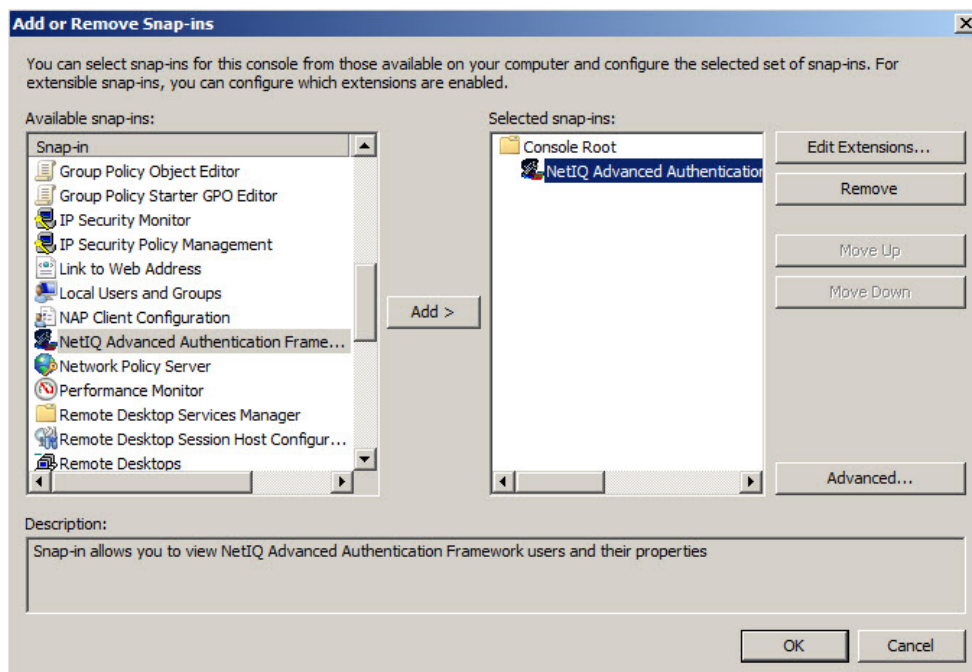
1. Open the MMC console.
2. In the console window, click **File** and select **Add/Remove Snap-in**.
3. In the **Add or Remove Snap-ins** dialog, select **NetIQ Advanced Authentication Framework User Viewer** and click **Add**.



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

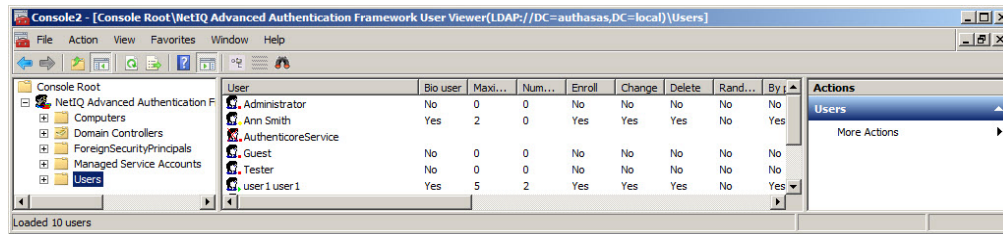


5. **NetIQ Advanced Authentication Framework User Viewer** is now displayed in the **Add or Remove Snap-ins** dialog. Click **OK**.



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

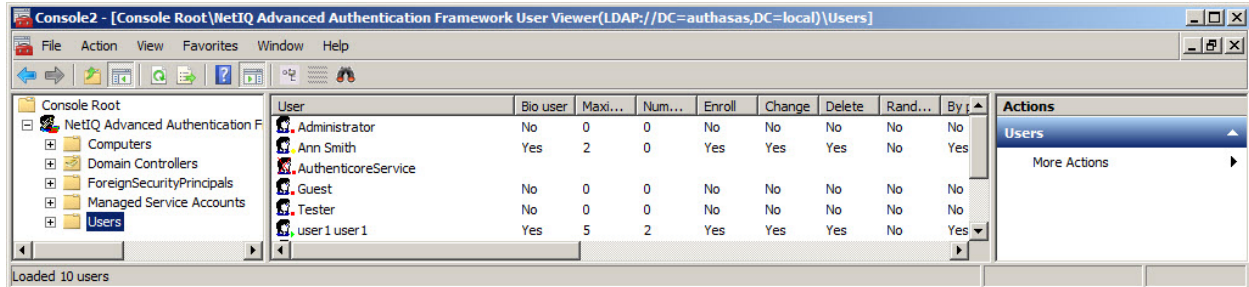
To view the list of users, click to expand the console tree and select a container. **NetIQ Advanced Authentication Framework User Viewer** displays the list of users and users' properties.







! 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).

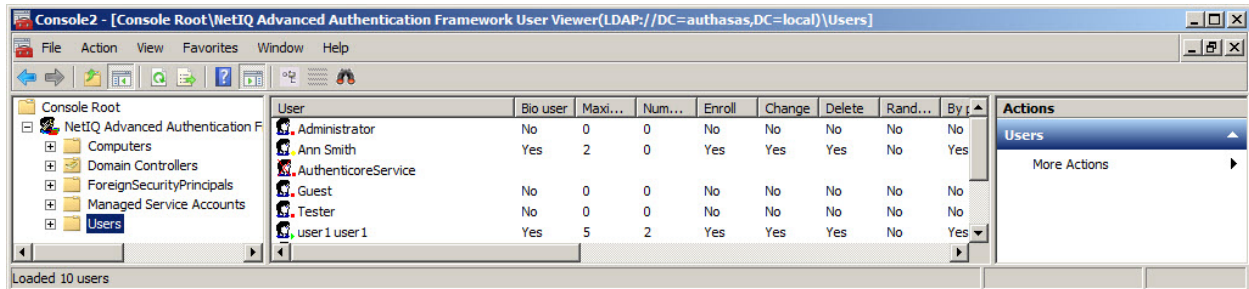


In order to optimize the entry output speed of large containers (in case when there are many users in the container), it is required to disable the display of users' settings. To disable the display of users' settings:

1. Open the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\NetIQ Advanced Authentication Framework
2. Specify the following parameter in the registry:
MmcShowUserInfo: type: REG_DWORD; value: 0x00000000 (0).

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 the [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

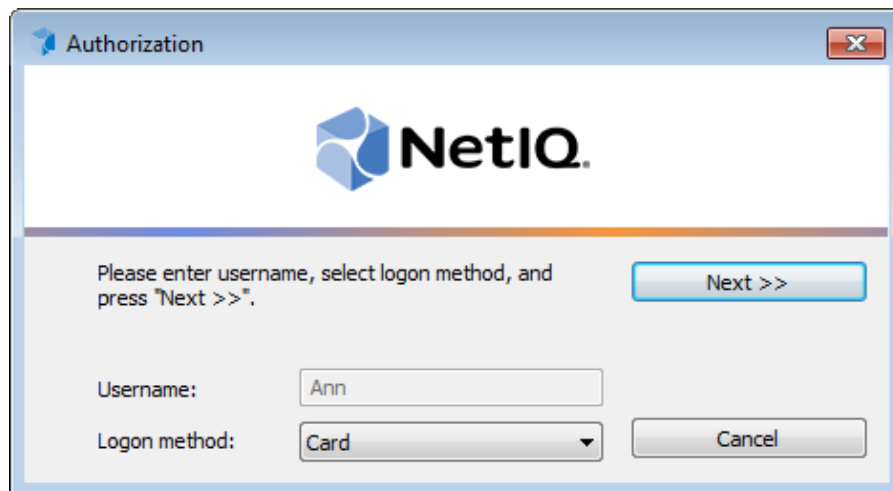
NetIQ Advanced Authentication Framework User Viewer allows you to change NetIQ Advanced Authentication Framework user properties and manage authenticators.

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 Advanced Authentication Framework 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.



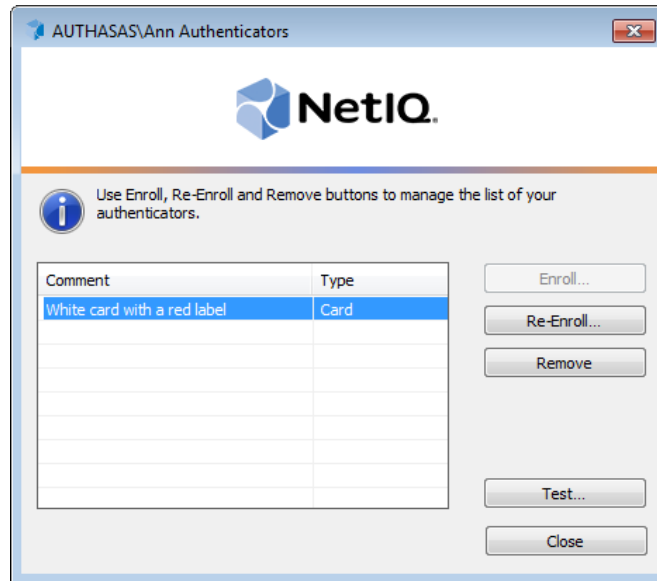
User name and domain name cannot be changed.


- 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.




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

 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 the [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 the [Re-enrolling Authenticator](#) chapter at **Active Directory Users and Computers**.

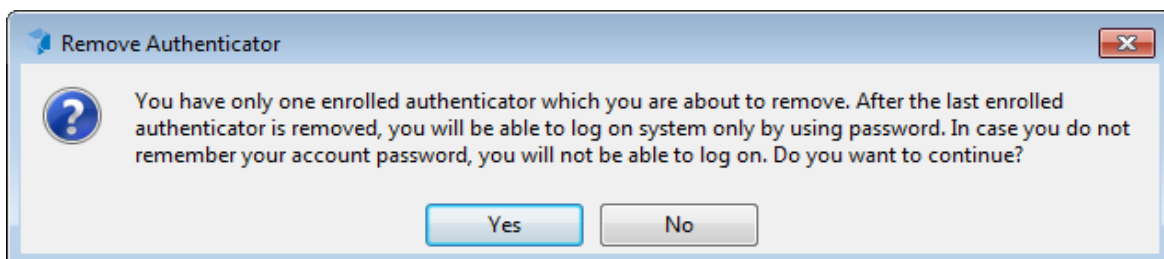
Testing Authenticator

Authenticator testing procedure remains the same for every administrative tool. For more details, see the [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 the [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:

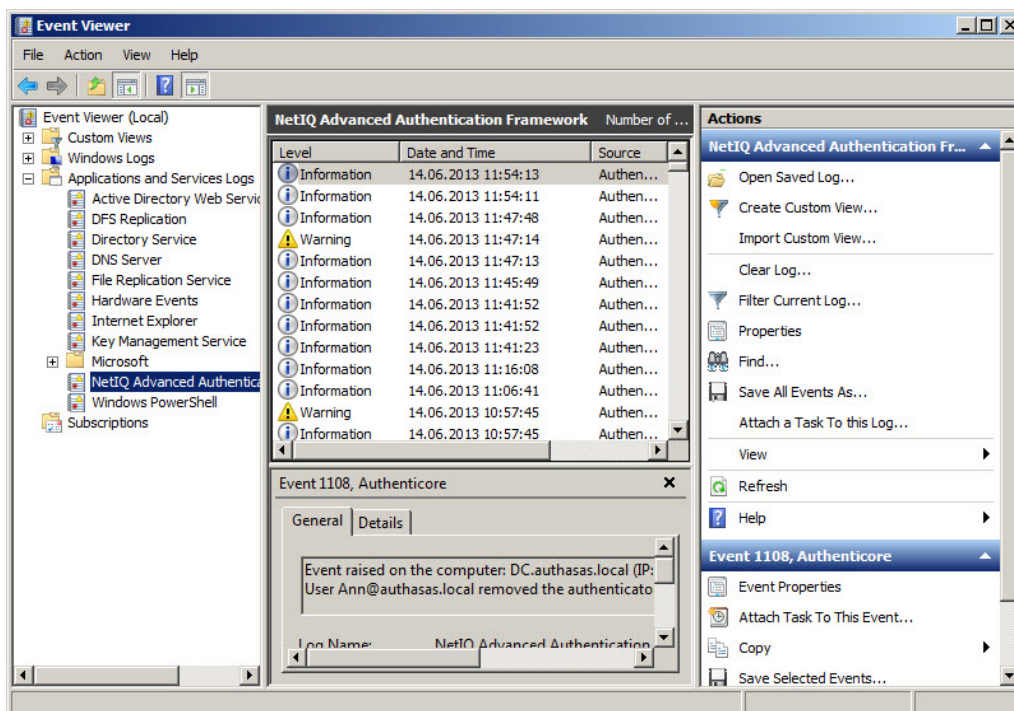
- System modules installation / removing / modifying;
- Users authentication (successful / unsuccessful);
- Enrolling/re-enrolling/removing authenticator ;
- Authenticore server work (server start/stop, server work with Enterprise Key);
- User's password change.

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:



RPC Server Events

Message ID: 1

Server installation was not completed. At the moment, server is awaiting for installation completion. Server is not able to work until the process is finished.

Message ID: 2

Server is already installed. At the moment, it is working normally. Installation completion is not required.

Message ID: 3

Could not impersonalize.

Message ID: 8

Authenticore server could not create Cipher COM-object. Either the object was not registered in the process of system installation or it could not get the Enterprise Key.

Message ID: 9

Server could not create ADUserDataProvider object. Perhaps, the object was not registered while installing the system.

Message ID: 10

Authenticore server could not create KeyManager COM-object. Perhaps, the object was not registered while installing the system.

Message ID: 11

Authenticore server could not create Logon COM-object. Perhaps, the object was not registered while installing the system.

Message ID: 12

Authenticore server could not create Manager COM-object. Perhaps, the object was not registered while installing the system.

Message ID: 13

Could not generate or save Enterprise Key. This computer may have problems either with the CryptoAPI or with keys storing infrastructure.

Message ID: 14

Error calling RpcServerListen.

Message ID: 15

Could not log in as AuthenticoreService.

Possible error causes:

- there is no AuthenticoreService account in the domain;
- account password and AuthenticoreService account unsynchronized;
- AuthenticoreService account was automatically blocked;
- AuthenticoreService account does not have "batch job" logon privileges on this computer.

Message ID: 16

Server could not read the name of user account under which the server must work.

Message ID: 17

Server could not register RPC-interface.

Message ID: 18

Server could not save user account name under which it must work.

Message ID: 19

Server requested the Enterprise Key, is not the domain member or its request is incorrect.

Message ID: 20

Could not get Kerberos Ticket of the Authenticore server which requested the Enterprise Key.

Message ID: 21

This function is intended for the local call only.

Message ID: 22

Could not find Authenticore server or establish connection with it.

Message ID: 23

Could not register Service Provider Name (SPN).

Message ID: 24

Could not get Kerberos Ticket using data received from Authenticore server.

Message ID: 25

Could not get Kerberos Ticket from Authenticore server, which had requested Enterprise Key: SPN is not registered. Most likely, the error occurred because Active Directory data replication had not been completed. In this case, please wait until replication is completed and then click Retry button.

Message ID: 26

Authenticore server, which has requested Enterprise Key, is not included into the Authenticore Servers group. Most likely, the error occurred because Active Directory data replication had not

been completed. In this case, please wait until replication is completed and then click Retry button.

Message ID: 27

The level of impersonalization, allowed by the requested side, is lower than "Delegate" level.

Message ID: 28

Server installation has not been completed. Currently the server is in progress of adding license.

Message ID: 29

Computer account is not trusted for delegation.

Message ID: 30

Cannot connect to the Authenticore server. Please, ensure that for your account the "Account is sensitive and cannot be delegated" option is turned off.

Message ID: 1100

The user was successfully authenticated by provided authenticator.

Message ID: 1101

Could not authenticate the user by provided authenticator.

Message ID: 1102

The user was successfully authenticated.

Message ID: 1103

Could not authenticate the user by the entered password. The error could also occur if the entered account was invalid.

Message ID: 1104

User re-enrolled the authenticator successfully.

Message ID: 1105

User could not re-enroll the authenticator.

Message ID: 1106

User added new authenticator successfully.

Message ID: 1107

User could not add new authenticator.

Message ID: 1108

User removed the authenticator successfully.

Message ID: 1109

User could not remove the authenticator.

Message ID: 1110

Authenticore Server service is stopped.

Message ID: 1115

Could not find Authenticore server.

Message ID: 1118

Could not find Authenticore server with valid license.

Message ID: 1119

The user was successfully authenticated by provided authenticator.

Message ID: 1120

License was applied successfully.

Message ID: 1121

Could not add license.

Message ID: 1122

Authenticore Server started successfully but the License is invalid.

Message ID: 1123

Could not authenticate the user by provided authenticator.

Message ID: 1125

Could not add license.

Message ID: 1127

The user was successfully authenticated by provided authenticator of linked account.

Message ID: 1210

User is allowed to use authenticators.

Message ID: 1211

Could not permit User to use authenticators.

Message ID: 1212

User is not allowed to use authenticators.

Message ID: 1213
Could not forbid using authenticators for User.

Message ID: 1216
Settings for User were successfully modified.

Message ID: 1217
User is allowed to add authenticators.

Message ID: 1218
User is not allowed to add authenticators.

Message ID: 1219
User is allowed to re-enroll his/her authenticators.

Message ID: 1220
User is not allowed to re-enroll his/her authenticators.

Message ID: 1221
User is allowed to delete his/her authenticators.

Message ID: 1222
User is not allowed to delete his/her authenticators.

Message ID: 1223
User is allowed to have authenticator(s).

Message ID: 1224
Automatic password generation is allowed for user.

Message ID: 1225
Automatic password generation is not allowed for user.

Message ID: 1227
The amount of allowed authenticators is reduced for user (reduced authenticators were deleted).

Message ID: 1228
Could not initialize settings for User.

Message ID: 1229
The list of enrolled authenticators of user was successfully cleared.

Message ID: 1230
Could not clear the list of enrolled authenticators of user.

Message ID: 1231
Could not initialize settings for computer.

Message ID: 1232
Computer users are allowed to cache authenticators.

Message ID: 1233
Computer users are not allowed to cache authenticators.

Message ID: 1234
Could not obtain settings for User.

Message ID: 1235
Could not get the list of enrolled authenticators of user.

Message ID: 1236
Could not change password for user.

Message ID: 1237
Could not set password for user.

Message ID: 1243
User re-enrolled the authenticator successfully.

Message ID: 1244
User could not re-enroll the authenticator.

Message ID: 1245
User added new authenticator successfully.

Message ID: 1246
User could not add new authenticator.

Message ID: 1247
User removed the authenticator successfully.

Message ID: 1248
User could not remove the authenticator.

Message ID: 1300
Authenticore Server service was successfully started.

Message ID: 1301
Authenticore Server service was successfully stopped.

Message ID: 1302
Could not start Authenticore Server service.

Message ID: 1303
Authenticore Server service could not read data from Active Directory.

Message ID: 1304
Authenticore Server service could not write data into Active Directory.

Message ID: 1305
Authenticore Server service could not decrypt data retrieved from Active Directory. Either data was corrupted or the Enterprise Key has been changed.

Message ID: 1306
Enterprise Key was successfully transferred to server.

Message ID: 1307
Could not transfer Enterprise Key to server.

Message ID: 1308
Enterprise Key was successfully received from server.

Message ID: 1309
Could not get Enterprise Key from server.

Message ID: 1310
Authenticore server exported Enterprise Key successfully.

Message ID: 1311
Could not export Enterprise Key.

Message ID: 1312
Enterprise Key was successfully imported.

Message ID: 1313
Could not import Enterprise Key.

Message ID: 1314
Enterprise Key was successfully generated.

Message ID: 1315
Could not generate Enterprise Key.

Message ID: 1316
Active Directory is offline.

Message ID: 1724
Logon refused by security rules.

Message ID: 1725
Error occurred while checking security rules.

SrvWrapper Events

Message ID: 1111
The user could not be authenticated. The error could occur due to:

1. Authenticore server was not found.
2. The authentication method is not supported by available Authenticore servers (required BSP module is missing on server).
3. Lost communication with Domain Controller.
4. The required subsystem was not installed.

Message ID: 1112
The user could not be authenticated. The error could occur due to:

1. Authenticore server was not found.
2. The authentication method is not supported by available Authenticore servers (required BSP module is missing on server).
3. Lost communication with Domain Controller.
4. The required subsystem was not installed.

Message ID: 1113
Authenticators of user successfully cached on computer.

Message ID: 1114
Cached authenticators of all users successfully removed from computer.

Message ID: 1116
Either user account or authenticator is invalid.

Message ID: 1117
Authentication Failed. Press OK to try again.

Message ID: 1124
Authenticore server not found. User logged in using authenticator from cache.

Message ID: 1126
Authenticore server not found. User could not be logged in using authenticator from cache.

Password Filter Events

Message ID: 1400
Password was successfully changed for user.

Message ID: 1401
Password was successfully reset for user.

Message ID: 1402
Error while resetting password for user.

Message ID: 1403
Error while changing password for user.

Message ID: 1404
Password filter was successfully loaded.

Password Manager Events

Message ID: 1410
Password Manager service started successfully.

Message ID: 1411
Password Manager service finished its work. As a result user(s) need to change password. Could not change password for them.

Message ID: 1412
Password for user was successfully generated and changed.

Message ID: 1413
An error occurred during Password Manager work.

Message ID: 1414

Could not change password for user. It is recommended to check "Minimal password age" domain setting. In case its value differs from 0, it is possible that password change can be denied because the password has been already changed within the specified time interval. Also, password cannot be changed in case "User cannot change password" account setting is enabled.

Message ID: 1415

The time period specified using command prompt had expired before Password Manager was started. The service has been stopped.

Message ID: 1416

Password Manager has completed the working session.

EventLog Events

Message ID: 1

Event raised on the computer.

Message ID: 1500

Could not get access to remote Log Server. There is either no Log Server, it was turned off, or being reloaded. In case the error persists, it is recommended to check Firewall settings and the correctness of the domain names permission. To optimize work, Authenticore Server service will not attempt to set connection with the faulty Log Server during minutes.

Message ID: 1501

Event described below was delivered with some delay. This can occur if the remote Log Server was offline or unavailable.

BioAPI Events

Message ID: 0

Could not initialize BioAPI framework.

Message ID: 1

Could not load the required BioAPI BSP module.

Message ID: 2

Could not get enrolled authenticator.

Message ID: 3
Could not get authenticator.

Message ID: 4
Could not compare user's authenticators.

Message ID: 5
Could not load authenticators from the memory. Data is corrupt.

Message ID: 6
The type of enrolled authenticator does not correspond to the type of the given authenticator.

Message ID: 7
Authenticator does not correspond to the enrolled authenticator.

Authenticore Server Events

Message ID: 0
Could not create authenticator. The list of user authenticators may be corrupt.

Message ID: 1
Could not load the authenticator. The list of user authenticators may be corrupt.

Message ID: 2
Could not read user authenticators list.

Message ID: 3
Either user account or password value is invalid.

Message ID: 4
Authentication Failed. Press OK to try again.

Message ID: 5
Authentication Failed. Press OK to try again.

Message ID: 6
This operation is forbidden by administrator.

Message ID: 7
The allowed amount of authenticators is exceeded.

Message ID: 8

Could not set connection with the Authenticore server.

Check network connection and try again. If the error persists please contact your system administrator.

Message ID: 9

The passwords were unsynchronized.

Message ID: 10

Could not change password for the user. The generated value does not satisfy the security policies. It is recommended to check "Minimal password age" domain setting. In case its value differs from 0, the password change can be denied because the password has been already changed within the specified time interval.

Message ID: 11

Could not change user password. The current security settings forbid the user to change his/her password.

Message ID: 12

Could not change password for the user. The reason is unknown.

Message ID: 13

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 desynchronization between user computer and Authenticore server or criminal attempt to use authenticator intercepted over network.

Message ID: 14

Could not load BioAPI BSP module. Either the required BSP module is not installed on the Authenticore server or it failed to load. The system will attempt to authenticate on another Authenticore server.

Message ID: 15

System resources are not enough to change password for the user.

Message ID: 16

This authenticator was already enrolled for a different user.

Message ID: 1238

Authenticator for user was successfully removed by administrator.

Message ID: 1239
Administrator failed to remove authenticator for user.

Message ID: 1240
Link from to was added.

Message ID: 1241
Link from to was removed.

Message ID: 1242
Failed to change linked accounts for the.

Message ID: 1726
Logon refused by security rules.

Message ID: 1727
Logon by password was denied.

Message ID: 1729
Your account was disabled by domain administrator.

Message ID: 1730
Your account was locked.

Message ID: 1733
Your account has expired.

Authentication Providers Events

Message ID: 0
The user was not found.

Message ID: 1
Could not get access to user data.

Message ID: 2
The property was not found. Perhaps the Active Directory scheme is not extended by additional attributes.

Message ID: 3
User is already allowed to use authenticators.

Message ID: 4
Could not create users sorting object.

Message ID: 5
Could not start user search.

Message ID: 6
Access is denied. Not enough permissions.

Message ID: 9
Unable to get object data in AD.

Message ID: 10
Unable to get object data in ADAM.

Message ID: 11
Could not get access to ADAM server.

Cryptography Events

Message ID: 1
User data corrupted.

Message ID: 2
Either user data or the Enterprise Key is corrupt.

Message ID: 3
Could not initialize required Crypto Service Provider (CSP).

Message ID: 4
Could not generate or export cryptographic keys.

Message ID: 5
Could not import cryptographic keys.

Message ID: 6
Data is corrupted.

Manager Events

Message ID: 1

Several authenticators were deleted because the allowed amount of authenticators was reduced.

Message ID: 2

The operation is not supported while the domain redirection policy is enabled.

Message ID: 1732

Operation denied by group policy.

Plugins Events

Message ID: 0

The specified Plug-in is not registered on the server.

Message ID: 1

Could not create registered Addon.

Message ID: 2

The user was authenticated by password.

Message ID: 3

The operation is forbidden.

Licensing Events

Message ID: 1

Invalid format of license data.

Message ID: 2

License not found.

Message ID: 3

License storage data is corrupted.

Message ID: 4

License data was changed or corrupted.

Message ID: 5

Your license does not match the time period restriction, the product version restriction or the domain name is wrong.

Message ID: 6

Cannot validate digital signature of the license. Certificate may be missing or corrupt.

Message ID: 7

This Addon does not support licensing.

Message ID: 8

Actual number of installed Authenticore Servers exceeds the number allowed by the License.

Message ID: 9

Actual number of NetIQ-enabled accounts exceeds the number allowed by the License.

Message ID: 10

The license you are trying to add allows fewer number of licensed objects than you have now.

Backup Provider Events

Message ID: 1

Bad password or data corrupted.

Administrative Tools Events

Message ID: 1

You don't have rights for changing settings on this page. Please, ensure that you are the member of the NetIQ Advanced Authentication Framework Admins group and these rights are delegated to the NetIQ Advanced Authentication Framework Admins group.

Message ID: 2

You don't have rights for changing settings on this page. Please, ensure that these rights are delegated to you.

GINA Events

Message ID: 1601

User unplug logon device.

Message ID: 1602

User has locked the workstation.

Message ID: 1603
User has ended the logon session.

Message ID: 1604
The user was successfully authenticated.

Message ID: 1605
Could not authenticate the user by the entered password. The error could also occur if the entered account was invalid.

Data Events

Message ID: 1
The field value is not set.

Message ID: 2
The subfield value is not set.

Message ID: 3
Subsystem is not found.

Message ID: 4
Data access denied.

Message ID: 5
The user was authenticated by password.

Message ID: 6
Record is not found.

Message ID: 7
Invalid field name.

Message ID: 8
Bad schema signature.

Message ID: 9
Subsystem users license is not found.

Message ID: 10
Subsystem servers license is not found.

Message ID: 11
User is not using given subsystem.

Message ID: 12
Actual number of the subsystem-enabled accounts exceeds the number allowed by the License.

Message ID: 1701
Unable to get the subsystem data for the user.

Message ID: 1702
User is unable to get the subsystem data.

Message ID: 1703
The subsystem data for user successfully retrieved.

Message ID: 1704
User successfully received the subsystem data.

Message ID: 1705
Unable to make user the client of the subsystem.

Message ID: 1706
User failed to be a client of the subsystem.

Message ID: 1707
User is allowed to use the subsystem data.

Message ID: 1708
User became the subsystem client.

Message ID: 1709
Unable to change the subsystem data for the user.

Message ID: 1710
The subsystem data for user successfully changed.

Message ID: 1711
User is unable to change the subsystem data.

Message ID: 1712
User successfully changed the subsystem data.

Message ID: 1713

The password was reset for user. Could not reset special data for subsystem.

Message ID: 1714

The password was reset for user.

Message ID: 1715

Unable to deny user to use the subsystem.

Message ID: 1716

User was denied to use the subsystem.

Message ID: 1717

User was unable to quit using the subsystem.

Message ID: 1718

User successfully quite using the subsystem.

Message ID: 1719

The password was reset for user. Could not reset special data for subsystem.

Message ID: 1720

The password was reset for user. Could not reset special data for subsystem. The subsystem data was reset completely.

Message ID: 1721

The password was reset for user. Special data for subsystem was successfully reset.

Message ID: 1722

The subsystems list for user is invalid and was cleared.

Message ID: 1723

The subsystems list for user is invalid and was cleared.

Message ID: 1728

Data container is not defined in the schema.

NPS Events

Message ID: 1800

The user was successfully authenticated by provided authenticator.

Message ID: 1801

Could not authenticate the user by provided authenticator.

Web Service Events

Message ID: 1731

Failed to connect to the configured web service. Please contact system administrator.

Group Policies


NetIQ Advanced Authentication Framework solution has 42 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.
 - [Default method for Other user](#) - allows you to specify the authentication method that will be used by default on the logon screen for the “Other user”.
 - [Disabled PIN host list](#) - allows you to logon just by a device.
 - [Disable random password generation by default](#) – defines the default state of the Generate random password for account setting.
 - [Do not allow administrators to remove user credentials](#) - disables the ability for administrator to remove individual enrollments for a user.
 - [Enable caching](#) - allows you to enable authenticators caching.
 - [Enable PIN caching](#) – allows you to enable a user to only type in PIN once every 8 hours.
 - [Hide password mode from logon UI](#) - disables the Password mode in authentication methods menu on workstations with NetIQ Client installed.
 - [Lock account on failed logon](#) - allows you to lock the user account after invalid logon attempts.
 - [Number of cached users](#) - allows you to define the number of cached users.
 - [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.
 - [Use domain password as PIN](#) - allows you to use the domain password together with a card.
- The **Event Log** section includes policies allowing 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 **Network** section includes policies allowing to enable or disable dynamic/static port.
 - [Always resolve client name](#) - allows you to resolve the name of the client. Force to use NTLM authentication during logon
 - [Force to use NTLM authentication during logon](#) - allows you to use automatically NTLM authentication during logon.
 - [RPC dynamic port selection allowed](#) - allows you to use a dynamic port for client-server interaction.
 - [RPC static port selection allowed](#) - allows you to use static port for client-server interaction.
- The **Runtime Environment** section includes a policy allowing to enable or disable showing of the user who has enrolled card when other user attempts to enroll the same card.
 - [Show enrolled card owner](#) - allows you to enable or disable showing of the user who has enrolled card when other user attempts to enroll the same card.
- The **Users and Groups** section includes a policy allowing to specify users and groups settings manually.
 - [Customize users and groups settings](#) - allows you to specify users and groups settings manually.
- The **Workstation** section includes policies allowing 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 first logon enroll wizard](#) - allows to disable the NetIQ first logon wizard autostart.
 - [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.

- [Enable device detection for all](#) - allows to perform a device detection when logged in with card or flash drive.
 - [Enhanced reaction on device events](#) – allows custom actions during device in and out events.
 - [Lifetime of notification about password reset](#) – allows you to setup lifetime of user’s notification about user’s password reset by administrator.
 - [Linked logon behavior](#) - determines the behavior of a linked logon.
 - [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.
 - [Web service client timeout](#) - allows you to set duration of authentication timeout for non-domain joined clients.
- The **Repository** section includes policies allowing to edit NetIQ repository.
 - [ADAM settings](#) – allows you to configure whether ADAM/AD-LDS is used as a repository.
 - [Enable Novell support](#) - 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.
 - [Repository](#) – allows you to choose whether to use native Active Directory or ADAM/AD-LDS as NetIQ repository.
 - The **UI Look & Feel** section includes policies designed for terminal clients.
 - [Show Cache Messages](#) - allows not to show the message on a workstation that caching is enabled or disabled.
 - [Show OSD Num Pad](#) - provides an On Screen Keyboard option during logging on.

Adding Group Policies

 It is required to have at least Microsoft Windows Server 2008 or Microsoft Windows 7 with RSAT to manage group policy settings.

The main policy templates (Security, Event Log, and Workstation) are stored locally in **NAAF.admx** file in **C:\Windows\inf** folder. After the unattended installation, policies appear in **Group Policy Management Editor** under **Computer Configuration > Policies > Administrative Templates: Policy definitions**.

Security Policies

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

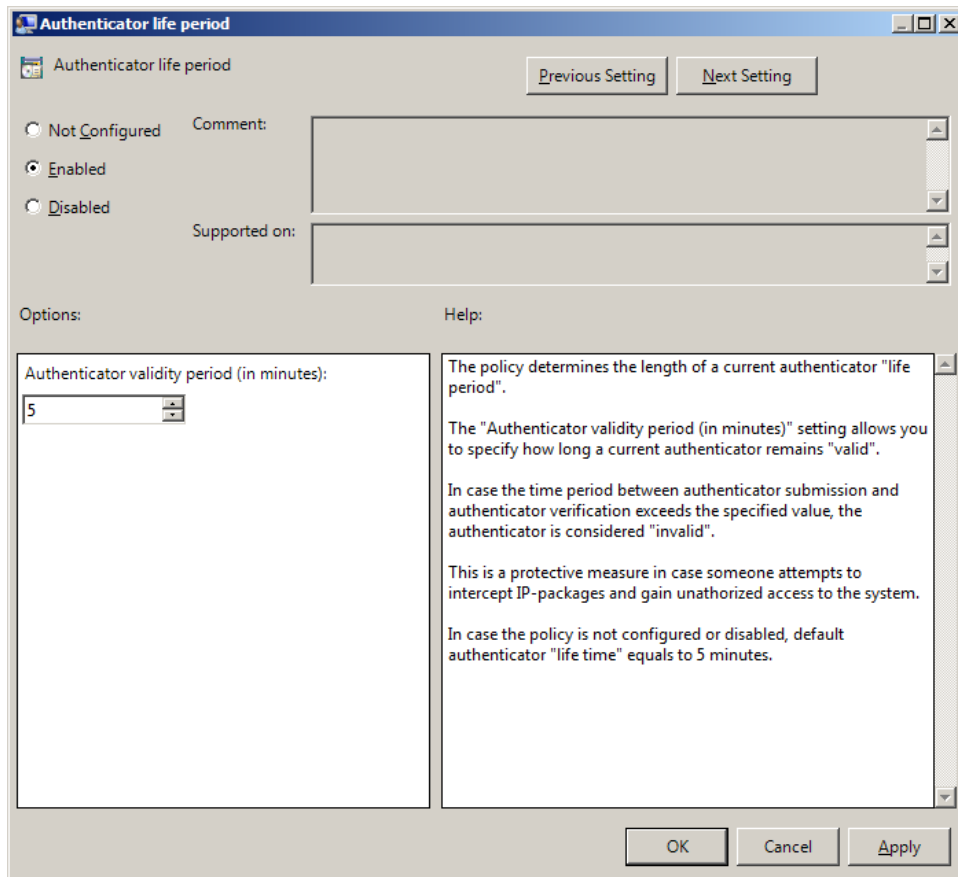
It includes:

- [Authenticator life period](#)
- [Credential providers filter settings](#)
- [Default method for Other user](#)
- [Disabled PIN host List](#)
- [Disable random password generation by default](#)
- [Enable caching](#)
- [Enable PIN caching](#)
- [Hide password mode from logon UI](#)
- [Lock account on failed logon](#)
- [Number of cached users](#)
- [Password length](#)
- [PIN restrictions](#)
- [Use domain password as PIN](#)

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.




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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: AuthenticatorLifePeriod (REG_DWORD)

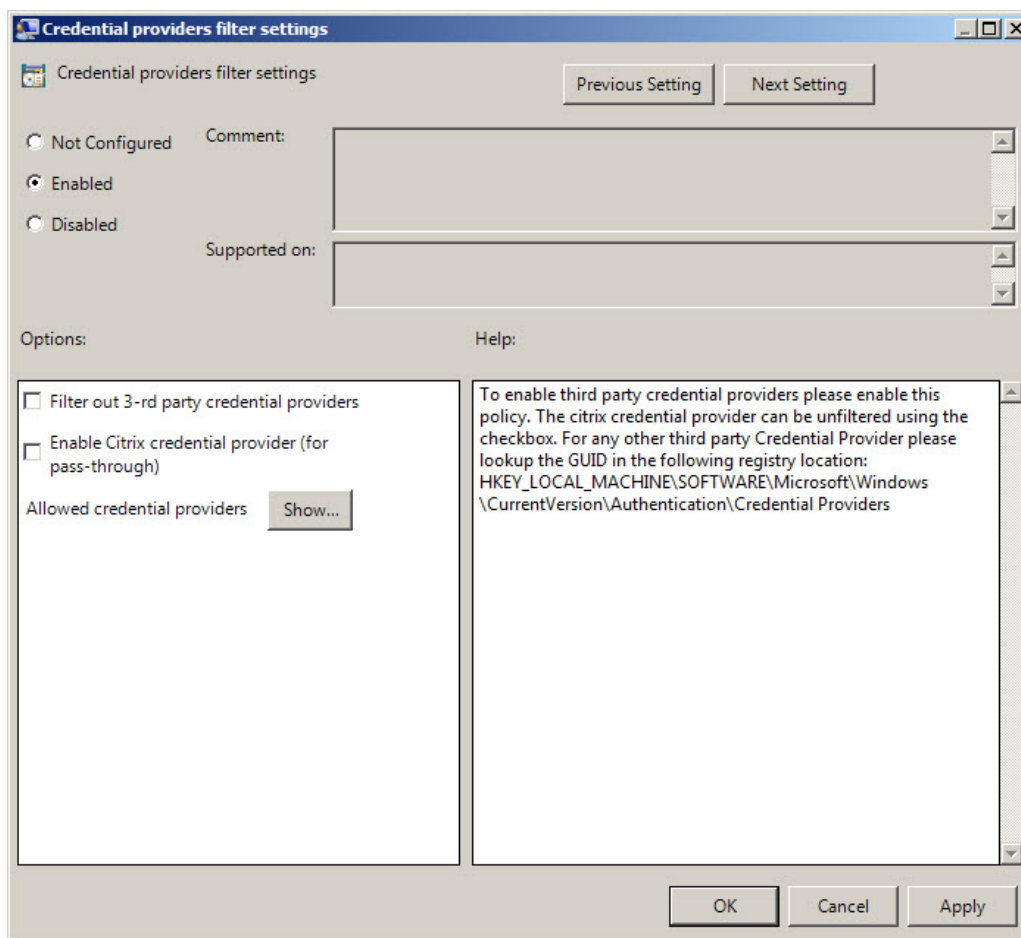
value: 0x00000005 (5)

5 displays the authenticator validity period (in minutes)

 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 is 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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\Filter\AllowedCPs

parameter: 1 (REG_SZ)

value: 5

5 displays the configured number of the allowed credential providers

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

Default method for Other user

The **Default method for Other user** policy allows you to specify the authentication method that will be used by default on the logon screen for the "Other user".

The screenshot shows a Windows-style dialog box titled "Default method for Other user". 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:" section with a dropdown menu. Underneath, there are "Options:" and "Help:" sections. The "Options:" section contains a "Default method GUID" label and a text input field. The "Help:" section contains a text area with the following text: "The policy allows you to specify the authentication method that will be used by default on the logon screen for the 'Other User'. To configure the authentication method that will be used by default on the logon screen for the 'Other User', specify the BSP GUID in the format (the required BSP GUID). For example, 9D5D01EF-76B0-1749-838B-C1441F7E23B3 means that Security Questions method of authentication is used by default for the 'Other User'." At the bottom of the dialog box are "OK", "Cancel", and "Apply" buttons.

To configure the authentication method that will be used by default on the logon screen for the "Other user", specify the GUID BSP in the format {the required GUID BSP}.

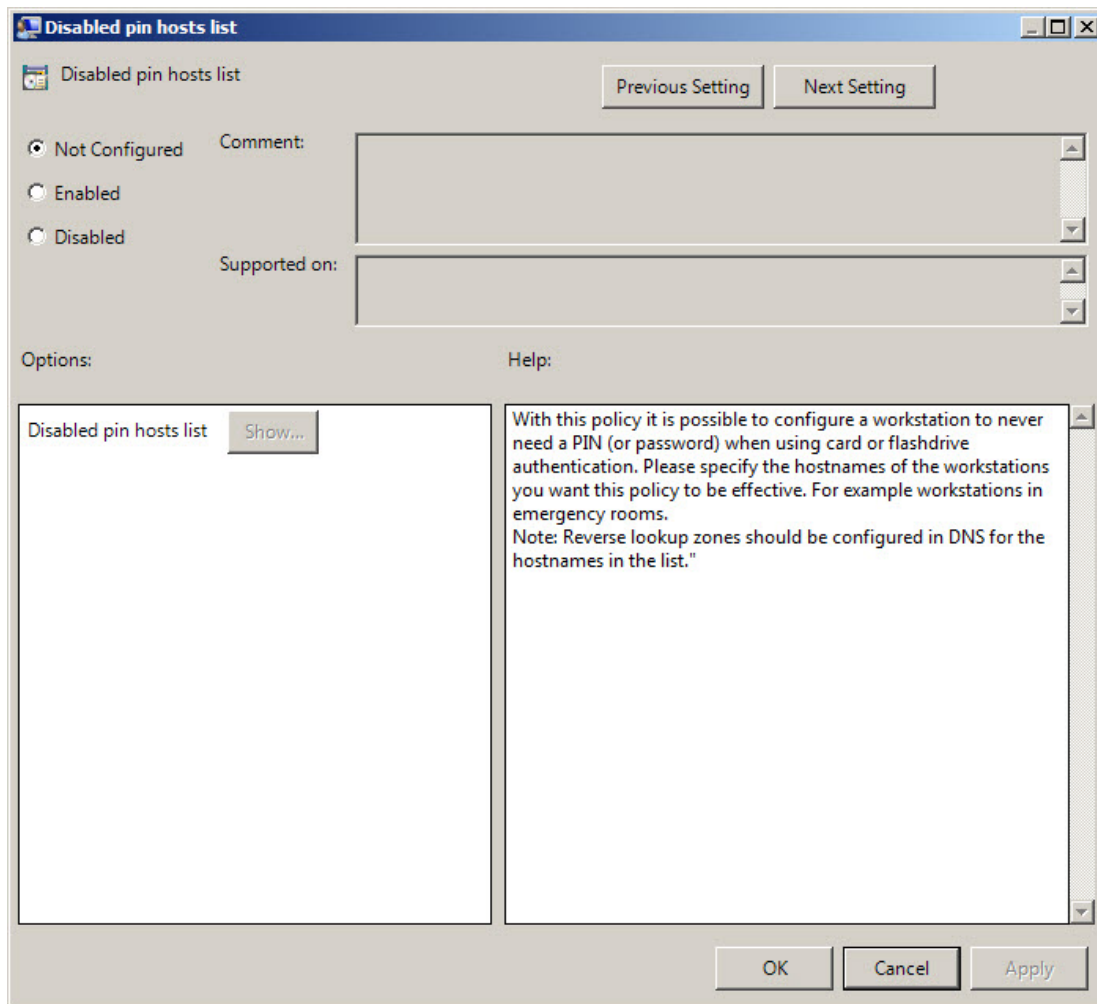
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: OtherUserDefMethod (REG_SZ)
value: {9D5D01EF-76B0-1749-838B-C1441F7E23B3}
{9D5D01EF-76B0-1749-838B-C1441F7E23B3} means that Security Questions method of authentication is used by default for the "Other user".

 The **Default method for Other user** policy works only with version 4.10 and newer.

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 List** policy. The following window will be displayed:



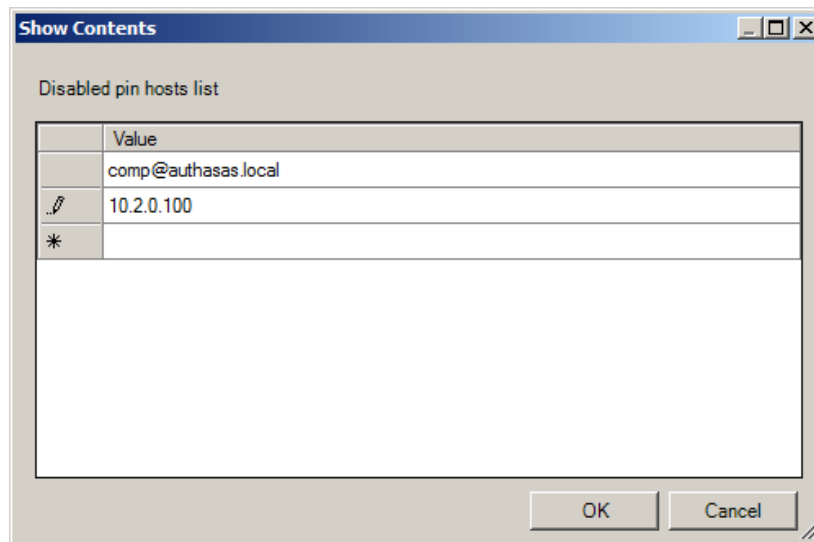
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\DisabledPinHostList
parameter: Host1 (REG_SZ) (the specified host name is displayed in the registry parameter)
value: 1
1 displays the value that was added to the Show Contents window

* 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.

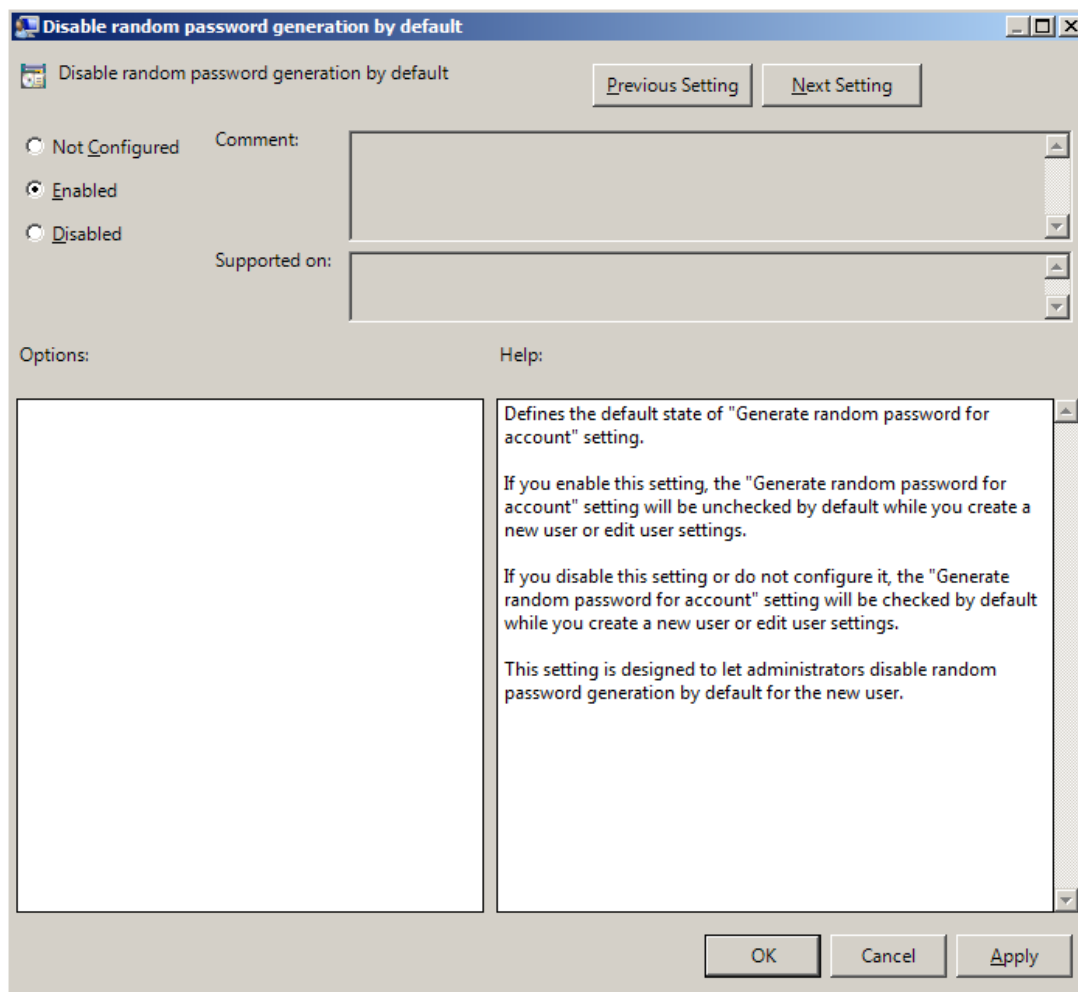


After all computers and IP addresses that will not need to enter PIN to logon are added, click the **OK** button to save changes. Then click the **Apply** button to save all the changes.



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

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.

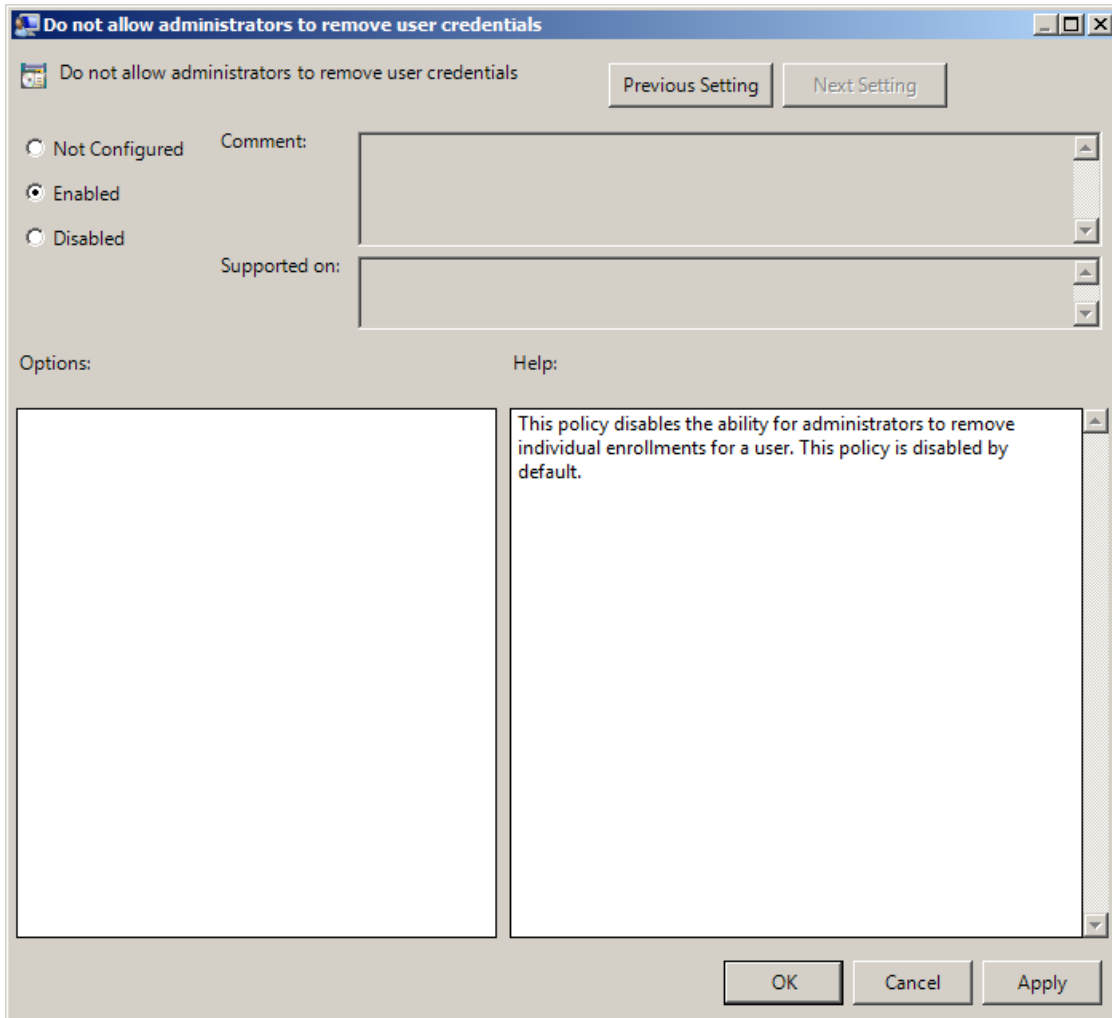


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DisableRandomPassword (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled.

-  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.

Do not Allow Administrators to Remove User Credentials

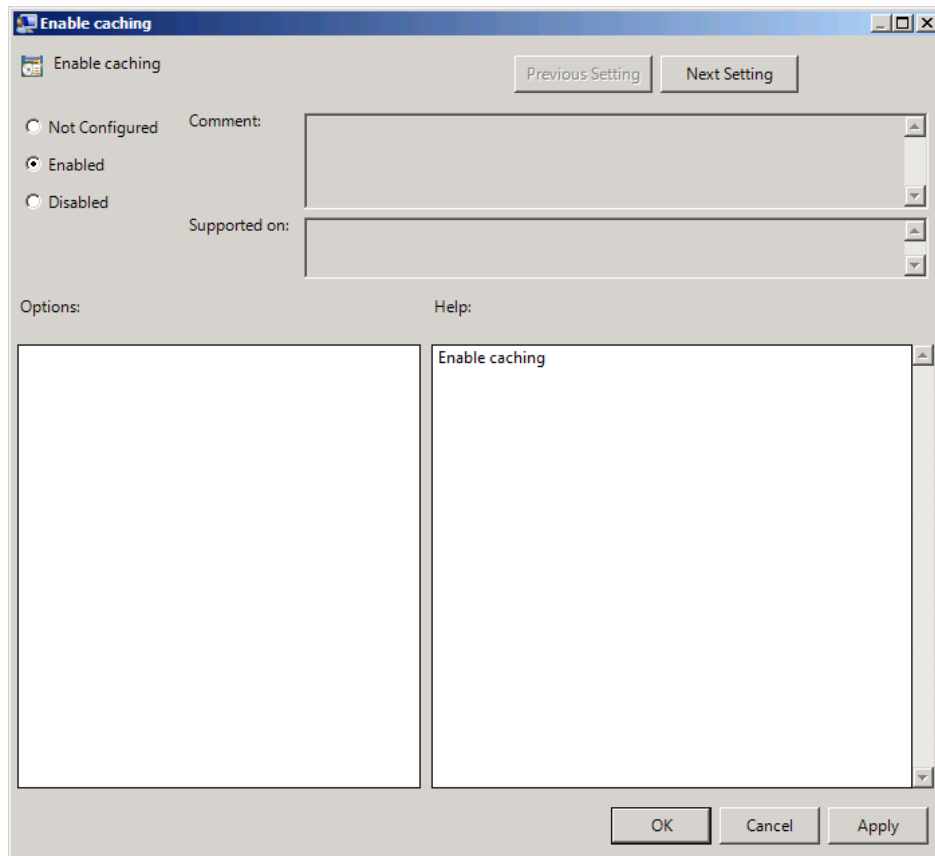
The **Do not allow administrators to remove user credentials** policy disables the ability for administrator to remove individual enrollments for a user. The policy is disabled by default.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DisableRemoveTemplatesByAdmin (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled


Enable Caching

The **Enable caching** policy allows you to disable local authenticators caching on workstations with the installed Client.



The **Enable caching** policy is enabled by default.

To disable caching, click the **Disabled** radio button. To save changes, click the **Apply** button.

 The changes take effect only after group policy refresh.

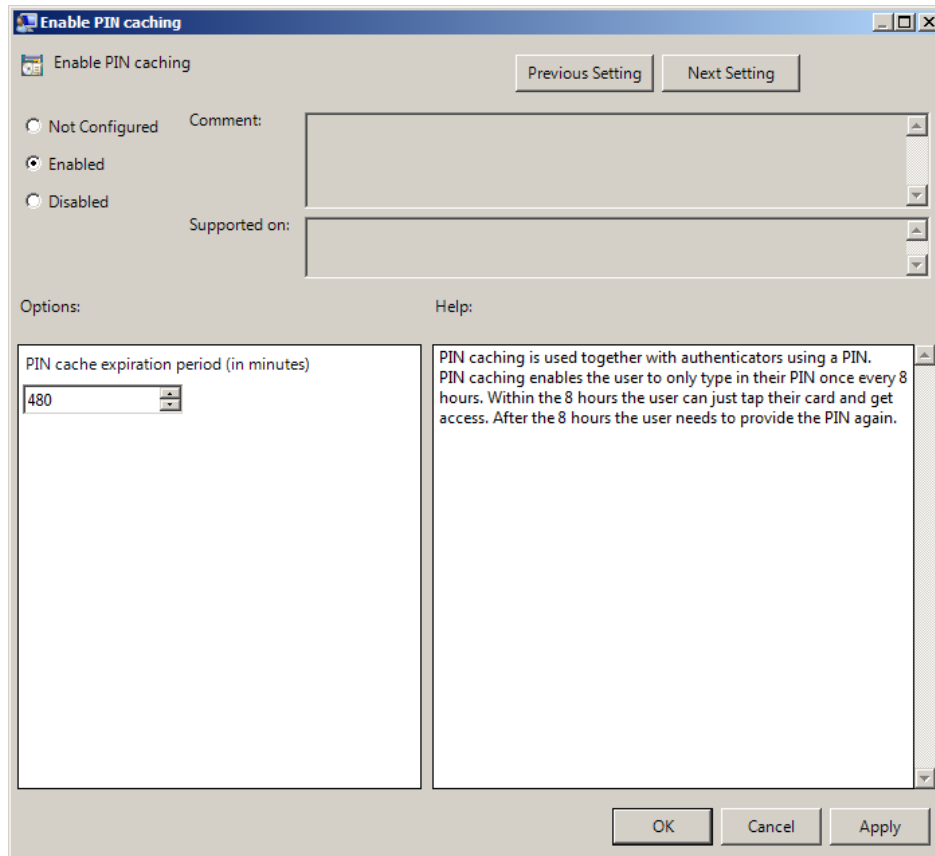
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: IsCacheEnabled (REG_DWORD)

value: 0x00000001 (1)

1 means that the caching is enabled

Enable PIN Caching

The **Enable PIN caching** policy is used together with authenticators using a PIN. The **Enable 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.




HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: LastLogonDBEnabled (REG_DWORD)


LastLogonDBExpirePeriod (REG_DWORD)


value: 0x00000001 (1), 0x000001e0 (480)

1 means that the policy is enabled

480 displays the configured PIN cache expiration period (in minutes)

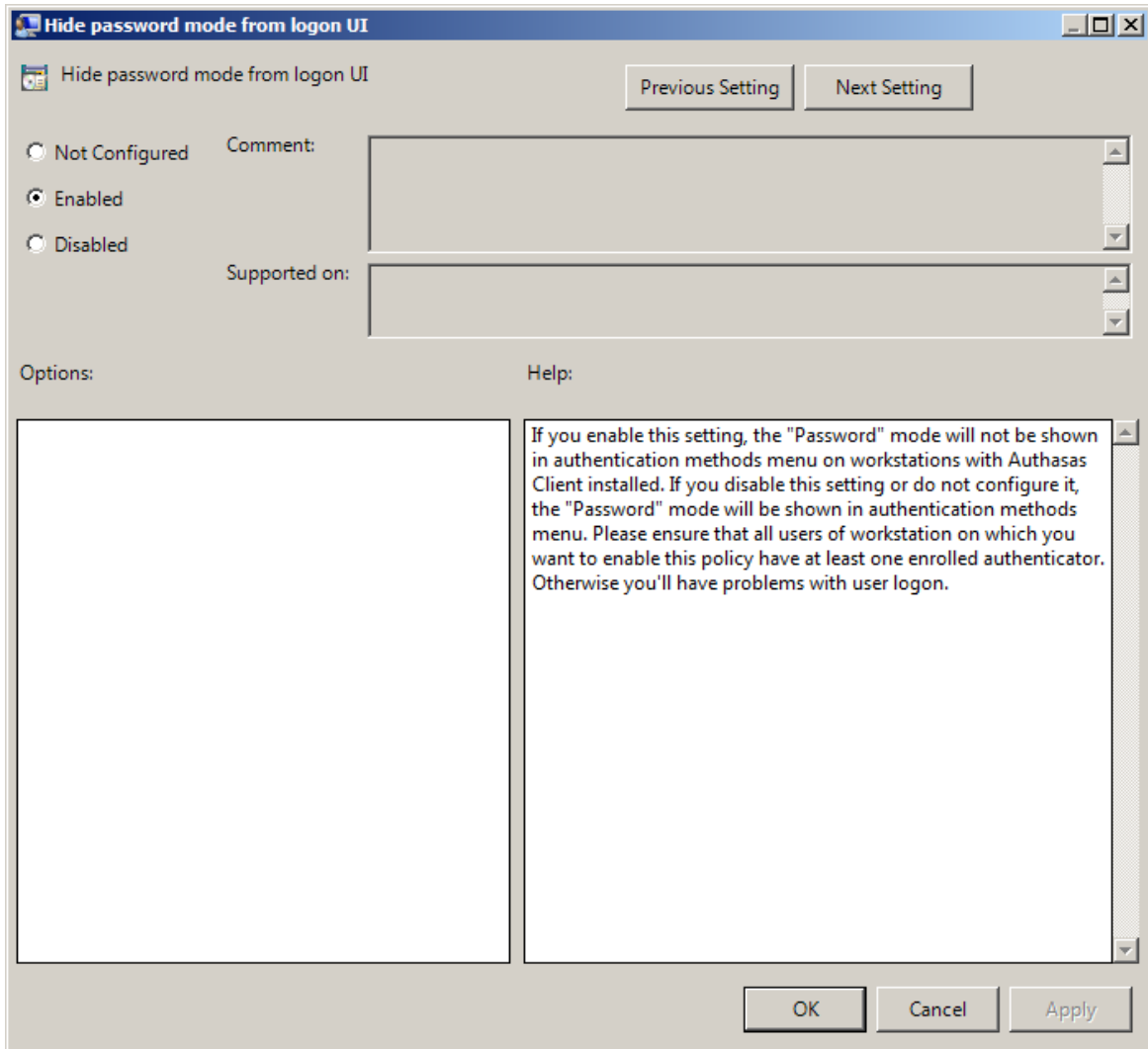
 If the policy is not defined or is disabled, the user should type in his/her PIN during every authentication process.

 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.

 PIN caching is updated once per 5 minutes in the background. That's why it may be required to enter PIN/password once again during 5 minutes after the authentication when both tapping the card and entering the PIN/password were used.

Hide password mode from logon UI

If you enable this setting, the **"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 **"Password"** mode will be shown in authentication methods menu.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: HidePasswordMode (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled



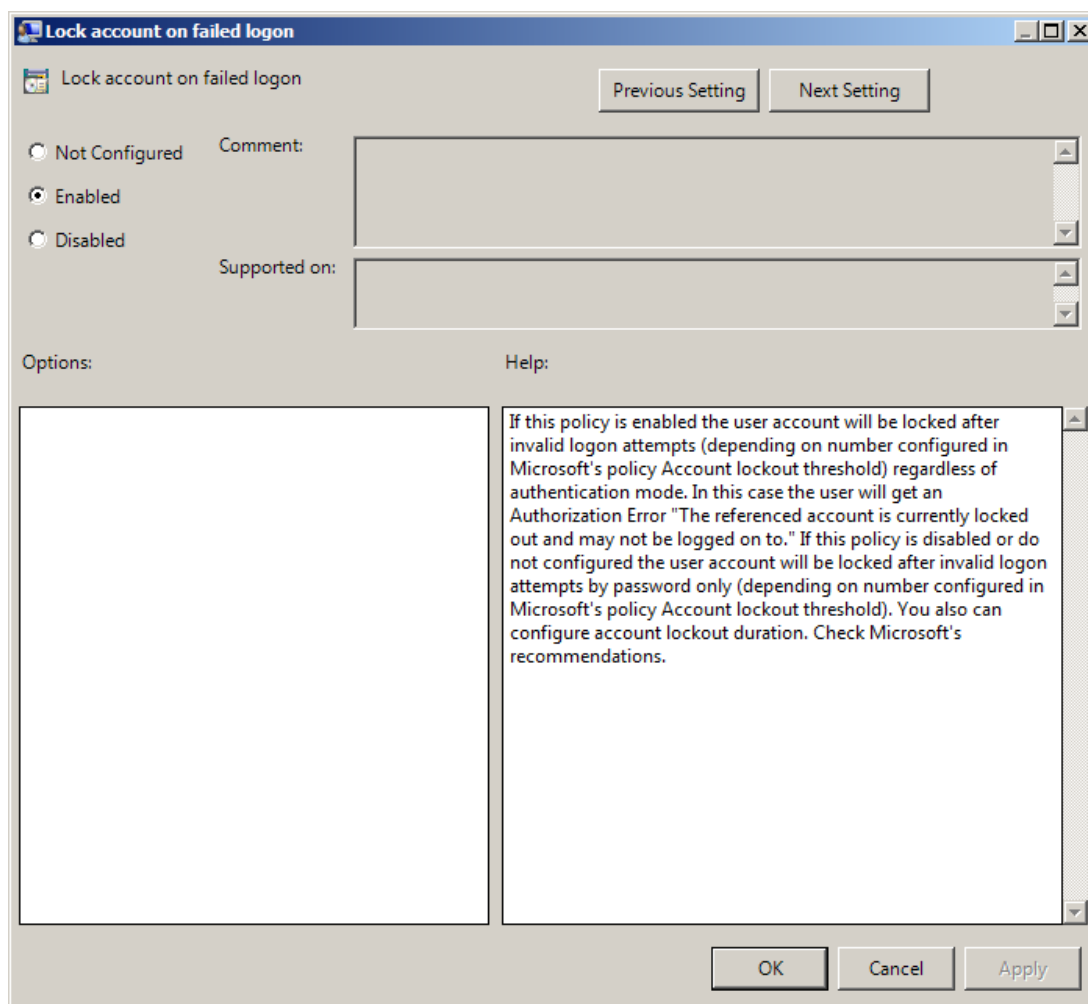
Please ensure that all users of workstation on which you want to enable this policy have at least one enrolled authenticator. Otherwise, you will have problems with user logon.

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 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](#).

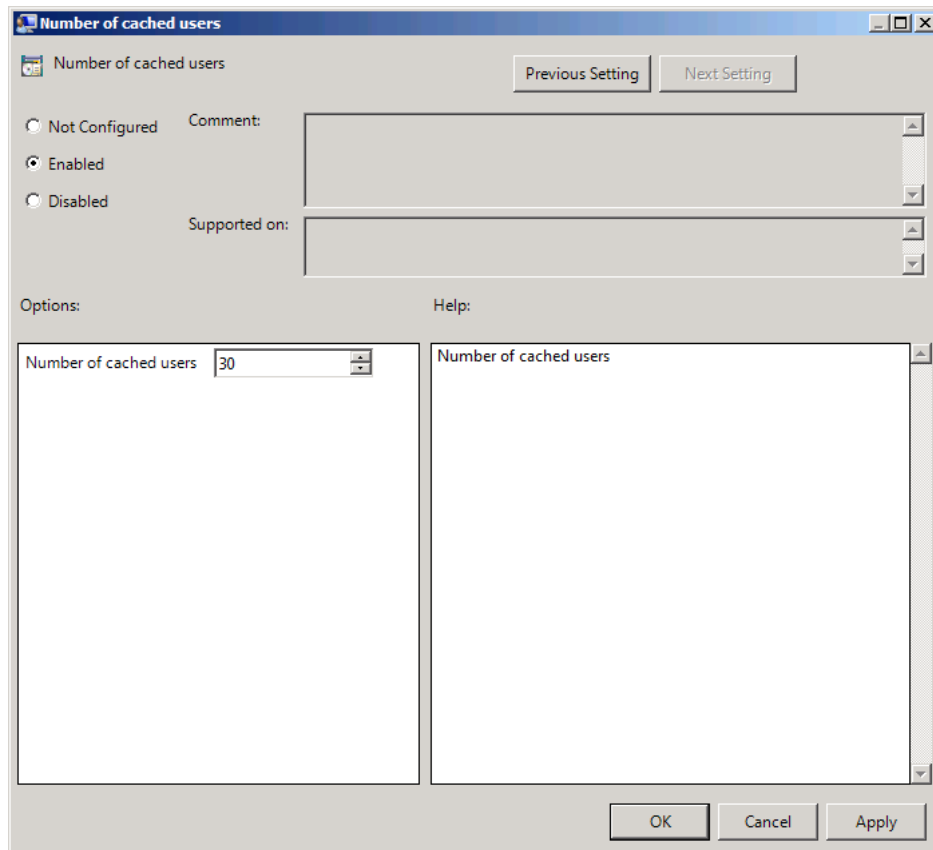


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: LockAccountOnFailedLogon (REG_DWORD)

value: 0x00000001 (1)
1 means that the policy is enabled

Number of Cached Users

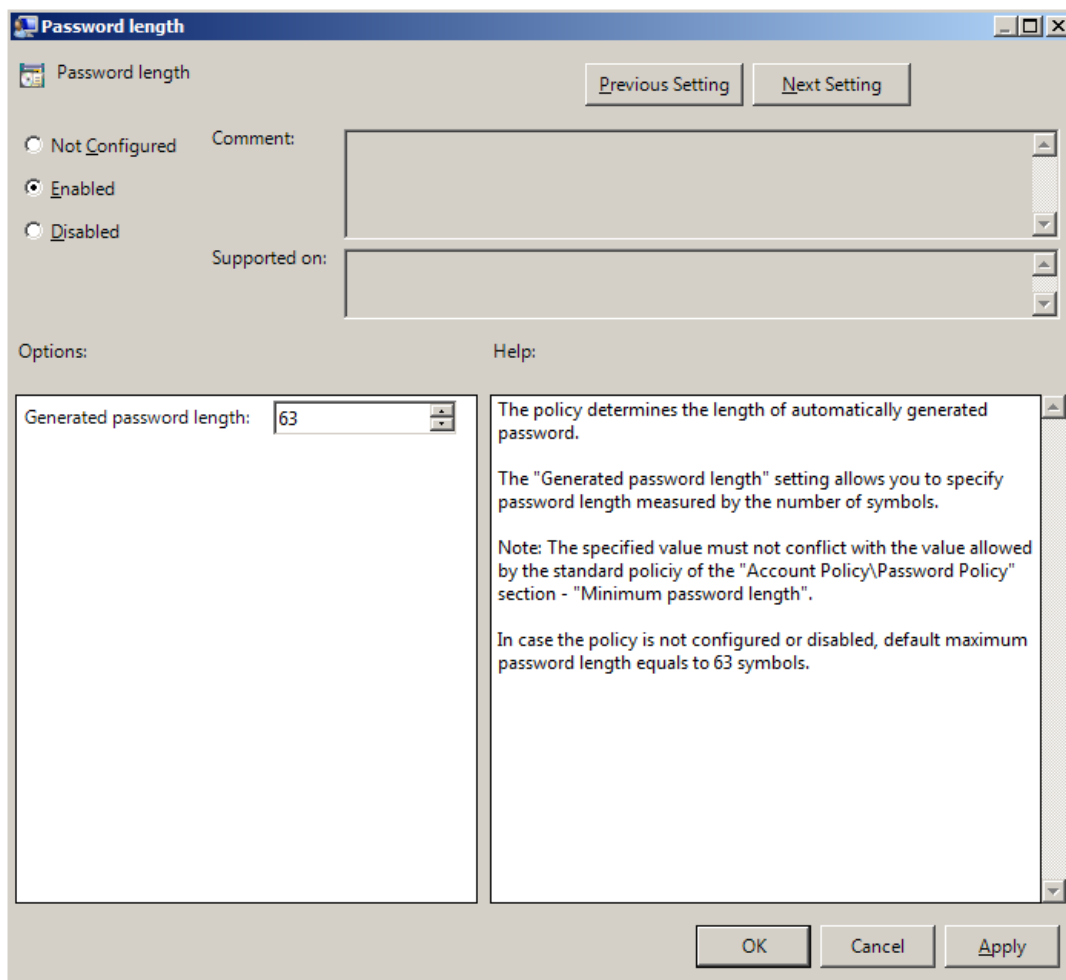
The **Number of cached users** policy allows you to define the number of user accounts that can be stored in the computer cache. When the number of cached user accounts reaches the number that is specified in the **Number of cached users** policy, then the latest user account is deleted from the computer cache after adding the new user account to it.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: NumberOfCachedUsers (REG_DWORD)
value: 0x0000001e (30)
30 displays the number of user accounts that can be stored in the computer cache

Password Length

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




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


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: GeneratePasswordLength (REG_DWORD)

value: 0x00000003f (63)

63 displays the generated password length

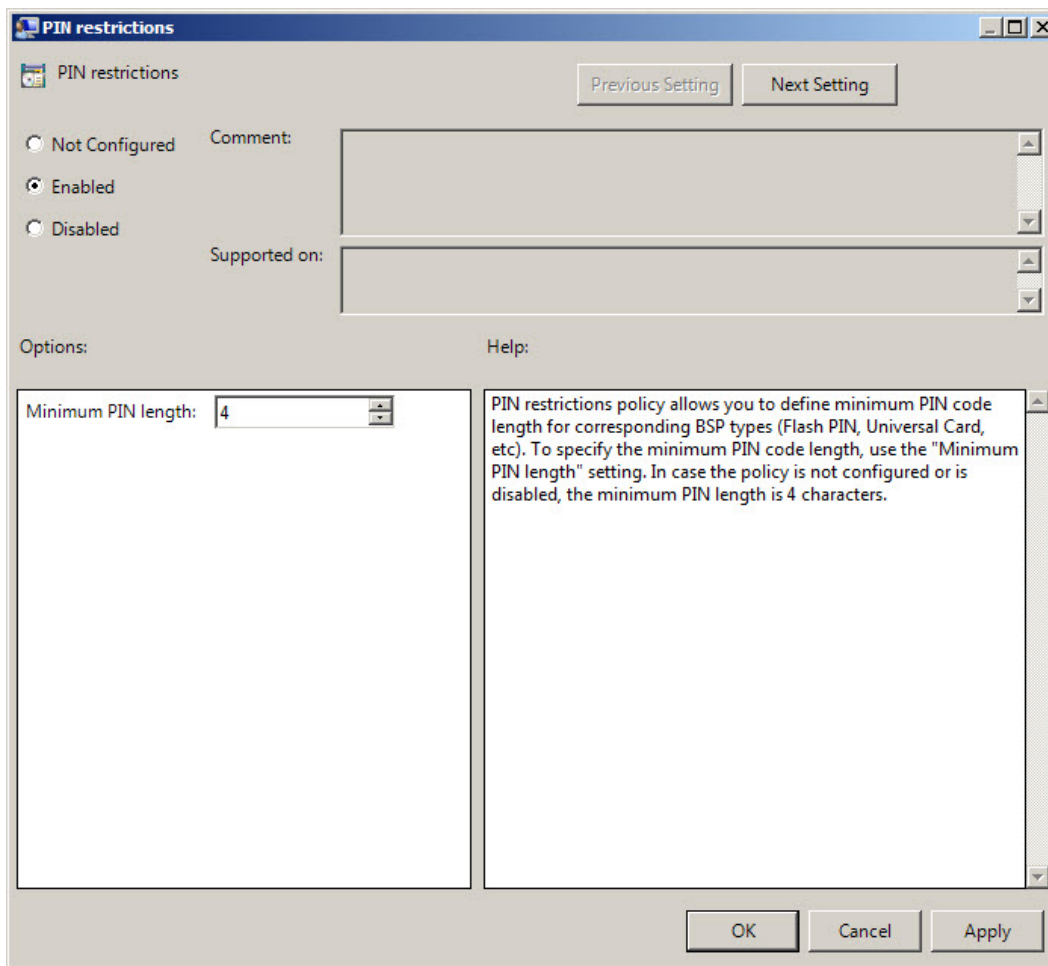
 The specified value and the frequency of passwords change must not conflict with the values defined by the standard policies of the Account Policy/Password Policy section:

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

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BSP\PINRestrictions

parameter: MinLength (REG_DWORD)

value: 0x00000004 (4)

4 displays the configured minimum PIN length

 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.

The screenshot shows a Windows-style dialog box titled "Use domain password as PIN". 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 of the dialog, there are "Options:" and "Help:" sections. The "Options:" section is empty, and the "Help:" section contains the text: "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." At the very bottom of the dialog are "OK", "Cancel", and "Apply" buttons.


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DomainPasswordAsPin (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled



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

 To enable the **Use domain password as PIN** policy, it is required to install Password Filter on all Domain Controllers. Otherwise if the password is reset, changed or generated automatically, the password will be desynchronized and it will be required to re-enroll authenticators.

Event Log Policies

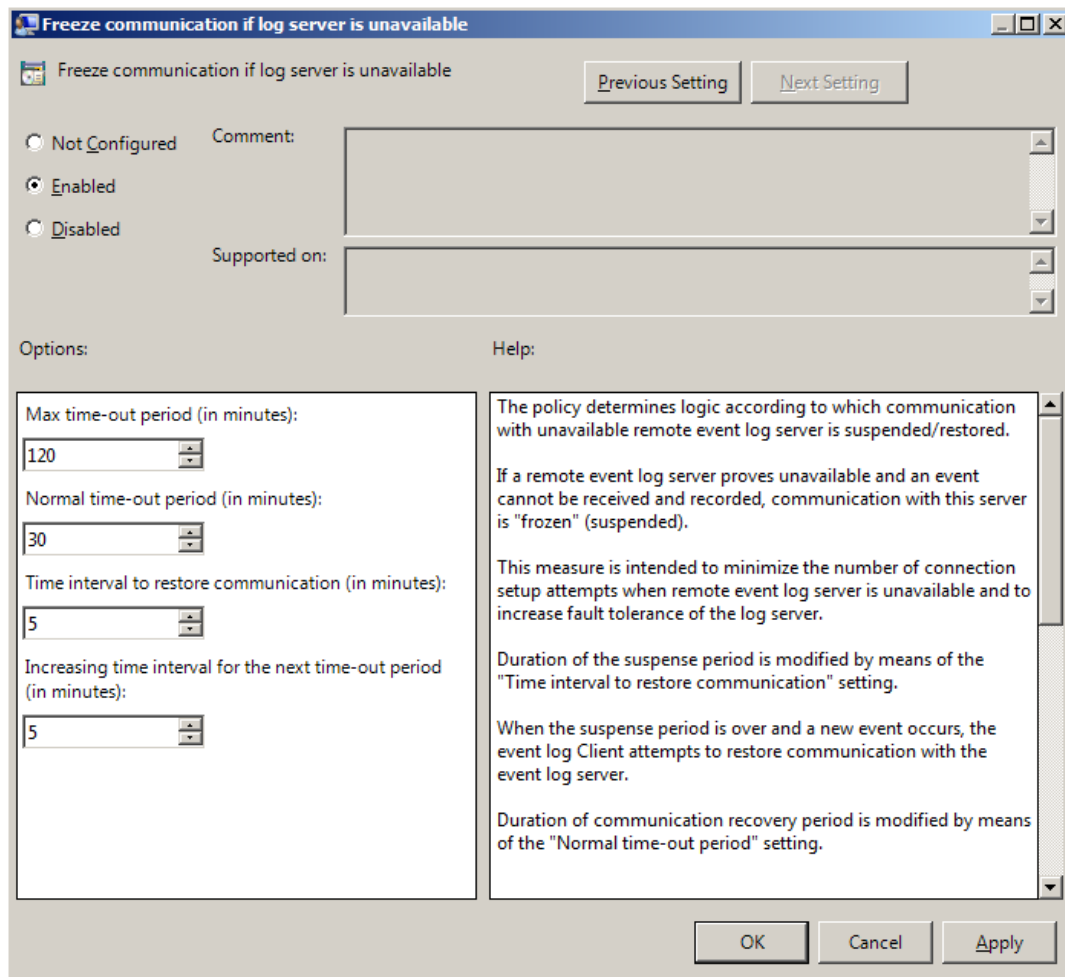
The **Event Log** section includes policies allowing you to determine logging settings.

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.



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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: MaxTimeoutPeriod (REG_DWORD)

ReconnectPause (REG_DWORD)

ReconnectPauseIncrement (REG_DWORD)

TimeoutPeriod (REG_DWORD)

value: 0x00000078 (120), 0x00000005 (5), 0x00000005 (5), 0x0000001e (30)

120 displays the max time-out period (in minutes)

5 displays time interval to restore communication (in minutes)

5 displays increasing time interval for the next time-out period (in minutes)

30 displays normal time-out period (in minutes)



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

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

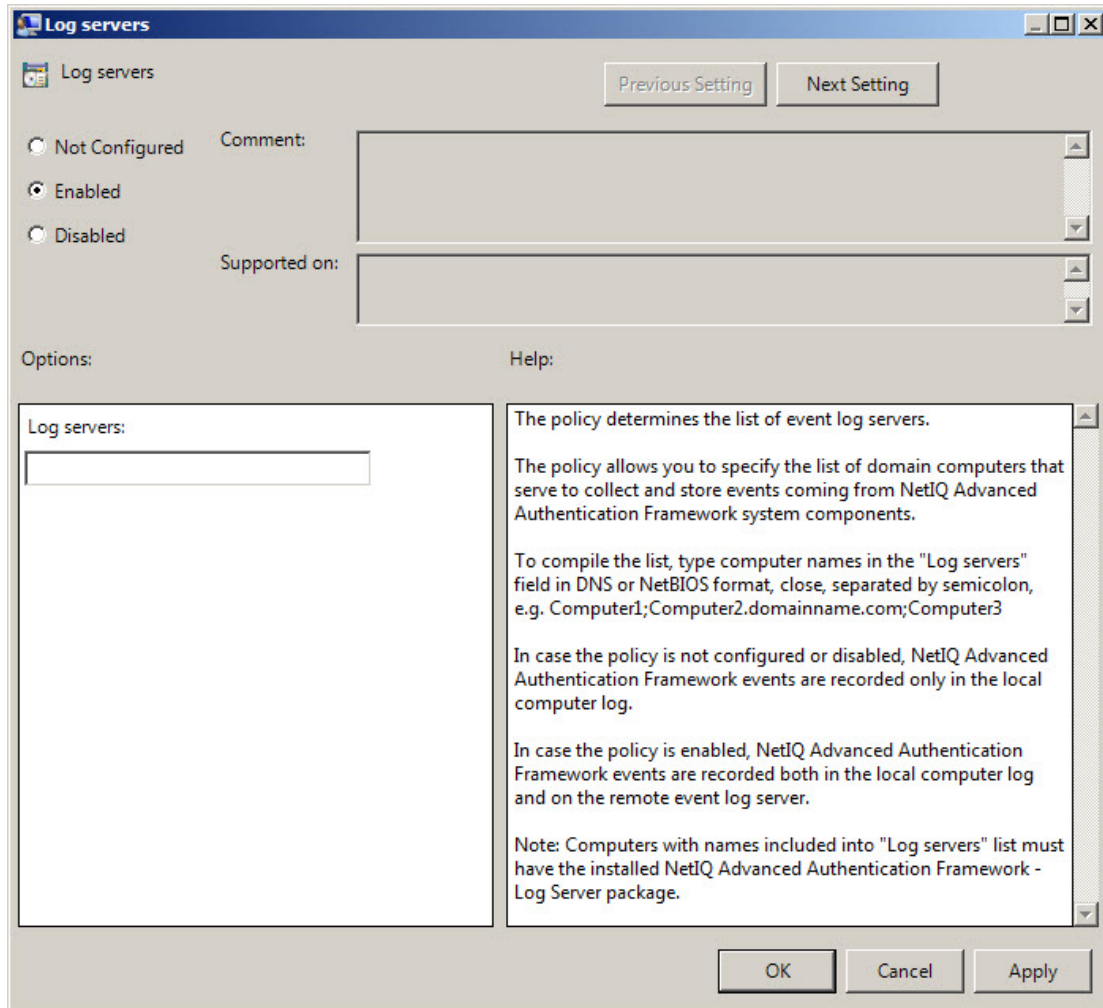
Normal time-out period (in minutes): 30;

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.






This **Log servers** box should contain the list of log server 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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: Logging Servers (REG_SZ)

value: Computer1, Computer2, Computer3

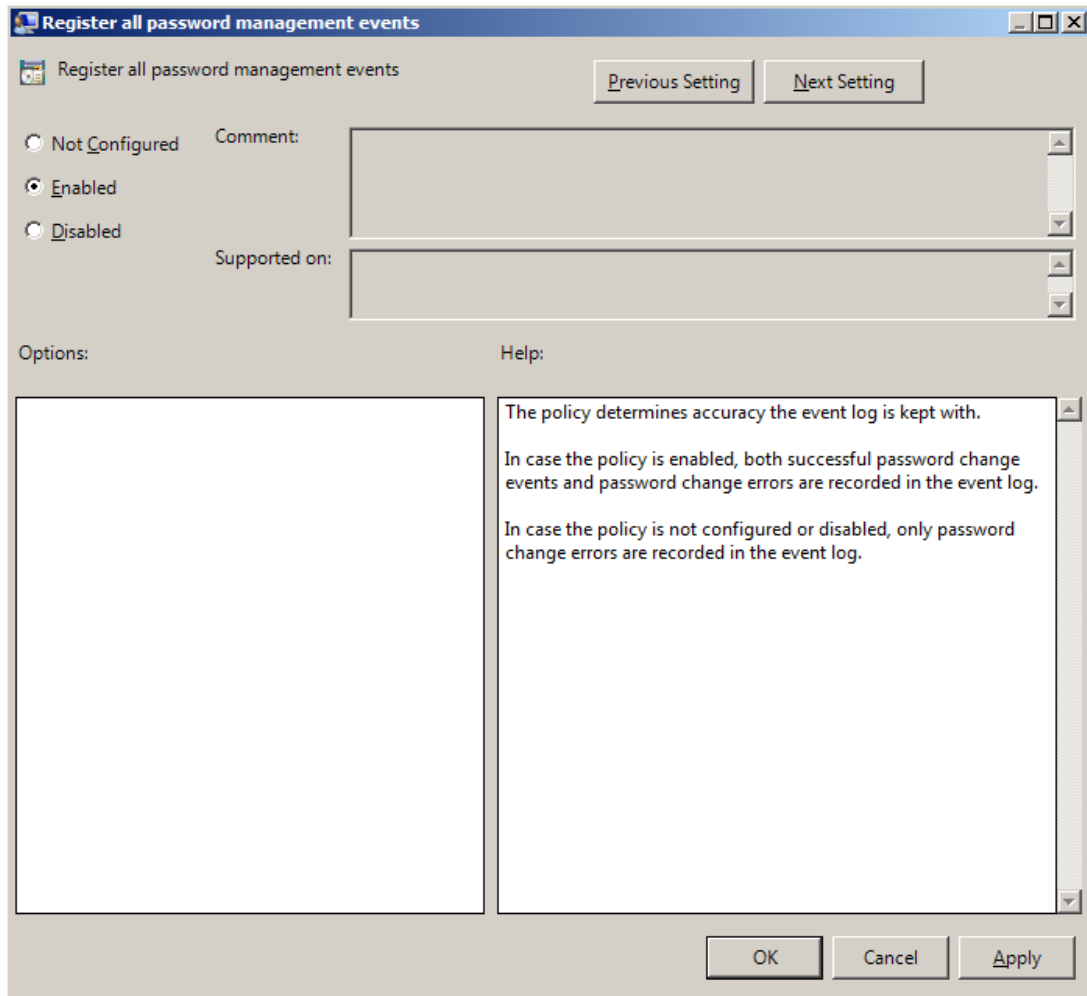
Computer1, Computer2, Computer3 is the list of the defined log servers

 The "NetIQ Advanced Authentication Framework – Log Server" package should 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.



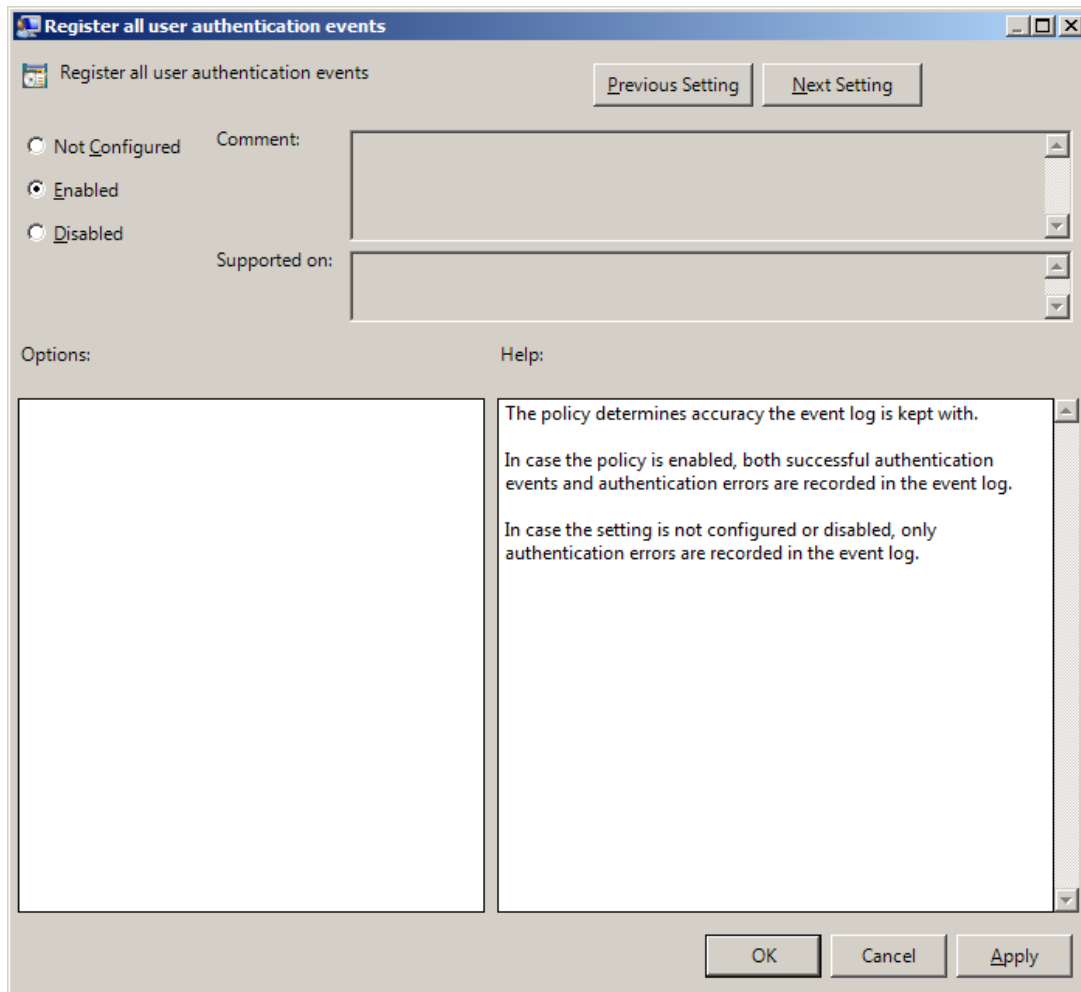
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: PasswordManagement_AllEvents (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled

 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.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: UserAuthentication_AllEvents (REG_DWORD)

value: 0x00000001 (1),

1 means that the policy is enabled

* 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.

Network Policies

The **Network** section includes network policies allowing you to enable or disable dynamic/static port.

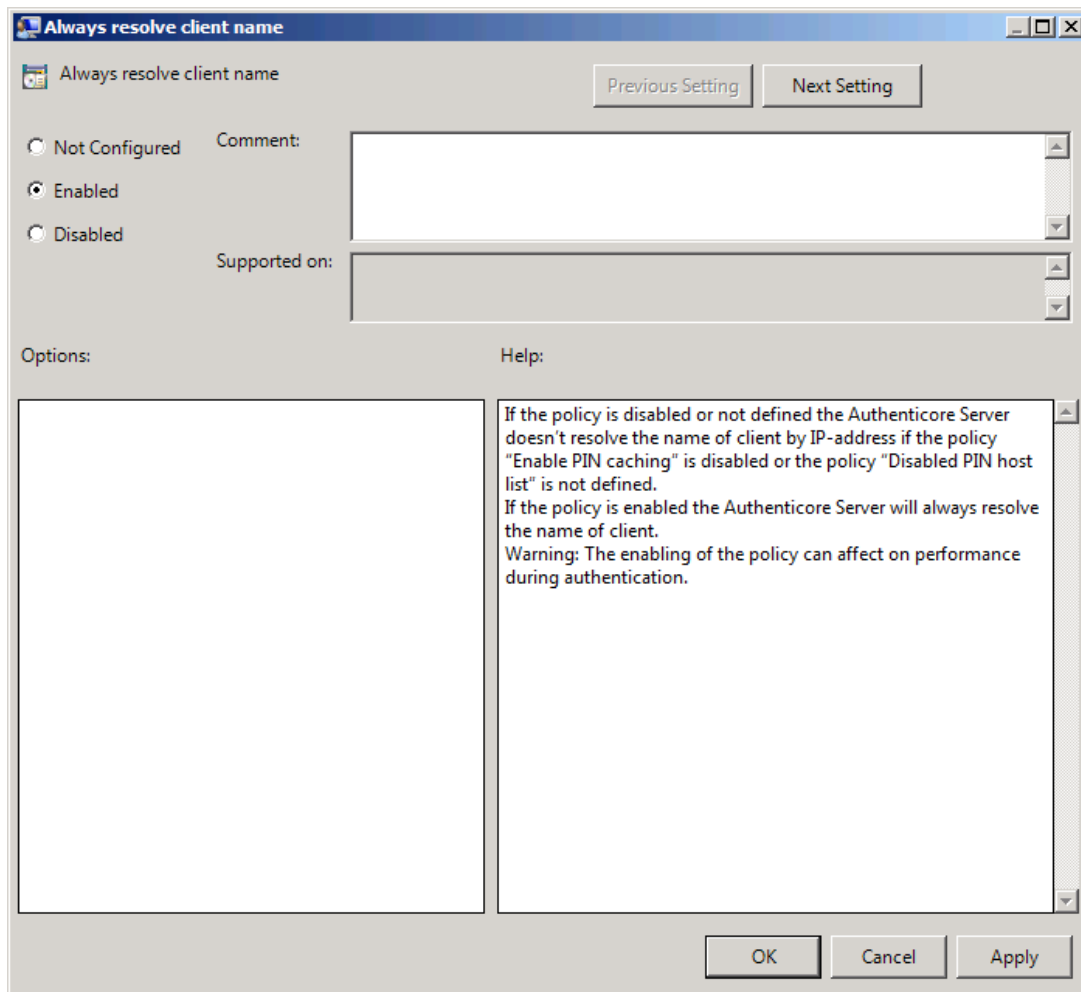
It includes:

- [Always resolve client name](#)
- [Force to use NTLM authentication during logon](#)
- [RPC dynamic port selection allowed](#)
- [RPC static port selection allowed](#)


Always resolve client name

If the **Always resolve client name** policy is disabled or not defined, the Authenticore Server doesn't resolve the name of client by IP-address if the **Enable PIN caching** policy is disabled or the **Disabled PIN host list** policy is not defined.

If the **Always resolve client name** policy is enabled, the Authenticore Server will always resolve the name of client.

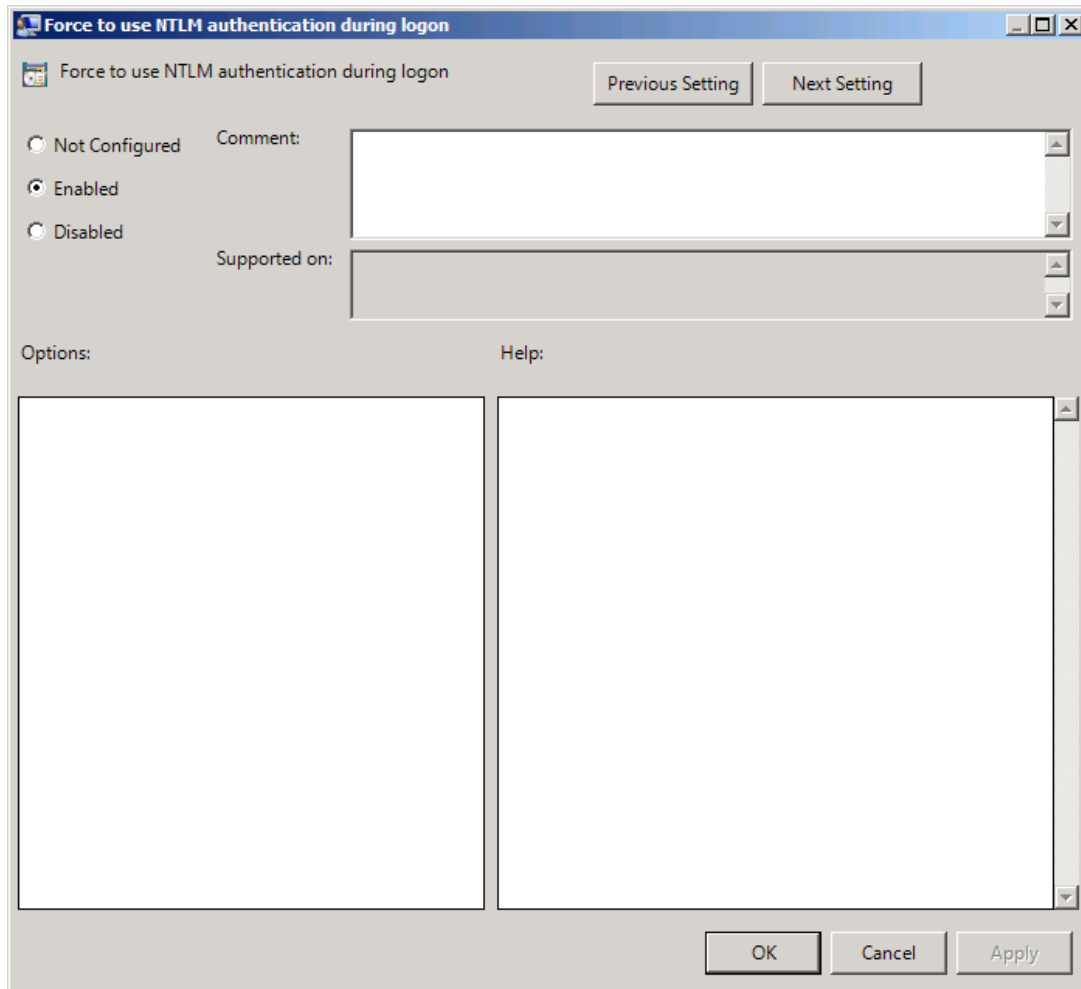


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: AlwaysResolveClientName (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled

 The enabling of the policy can affect the performance during authentication.

Force to use NTLM authentication during logon

If the **Force to use NTLM authentication during logon** policy is enabled, NTLM authentication will be automatically used during logon.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: RpcForceNtlmAtLogon (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled

RPC dynamic port selection allowed

If the **RPC dynamic port selection allowed** policy is enabled, the Authenticore Server uses a dynamic port for client-server interaction. By default the policy is enabled.

RPC dynamic port selection allowed

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Options:

Help:

If the policy is enabled the Authenticore Server uses a dynamic port for client-server interaction. By default the policy is enabled.


OK Cancel Apply

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: RpcDynamicPortAllowed (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled



If both **RPC dynamic port selection allowed** and **RPC static port selection allowed** policies are enabled then:

- Server will register both endpoints;
- Client will first try to use static port endpoint and then switch to dynamic if static bind failed.

 The server should be restarted after applying the policy.

RPC static port selection allowed


If the **RPC static port selection allowed** policy is enabled, the Authenticore Server uses a static port for client-server interaction. By default the policy is disabled.

The screenshot shows a Windows-style dialog box titled "RPC static port selection allowed". It features a "Previous Setting" and "Next Setting" button pair at the top right. On the left, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text area. Below that is a "Supported on:" list box. The "Options:" section contains a text box labeled "RPC static port:" with the value "28214". The "Help:" section contains a text box with the text: "If the policy is enabled the Authenticore Server uses a static port for client-server interaction. By default the policy is disabled." At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: RpcStaticPort (REG_DWORD)
RpcStaticPortAllowed (REG_DWORD)
value: 0x00006e36 (28214), 0x00000001 (1),
28214 is the port number in case of using static port for client-server interaction (the default port number is 28214)
1 means that the policy is enabled

 If both **RPC dynamic port selection allowed** and **RPC static port selection allowed** policies are enabled then:

- Server will register both endpoints;
- Client will first try to use static port endpoint and then switch to dynamic if static bind failed.

 The server should be restarted after applying the policy.

Runtime Environment

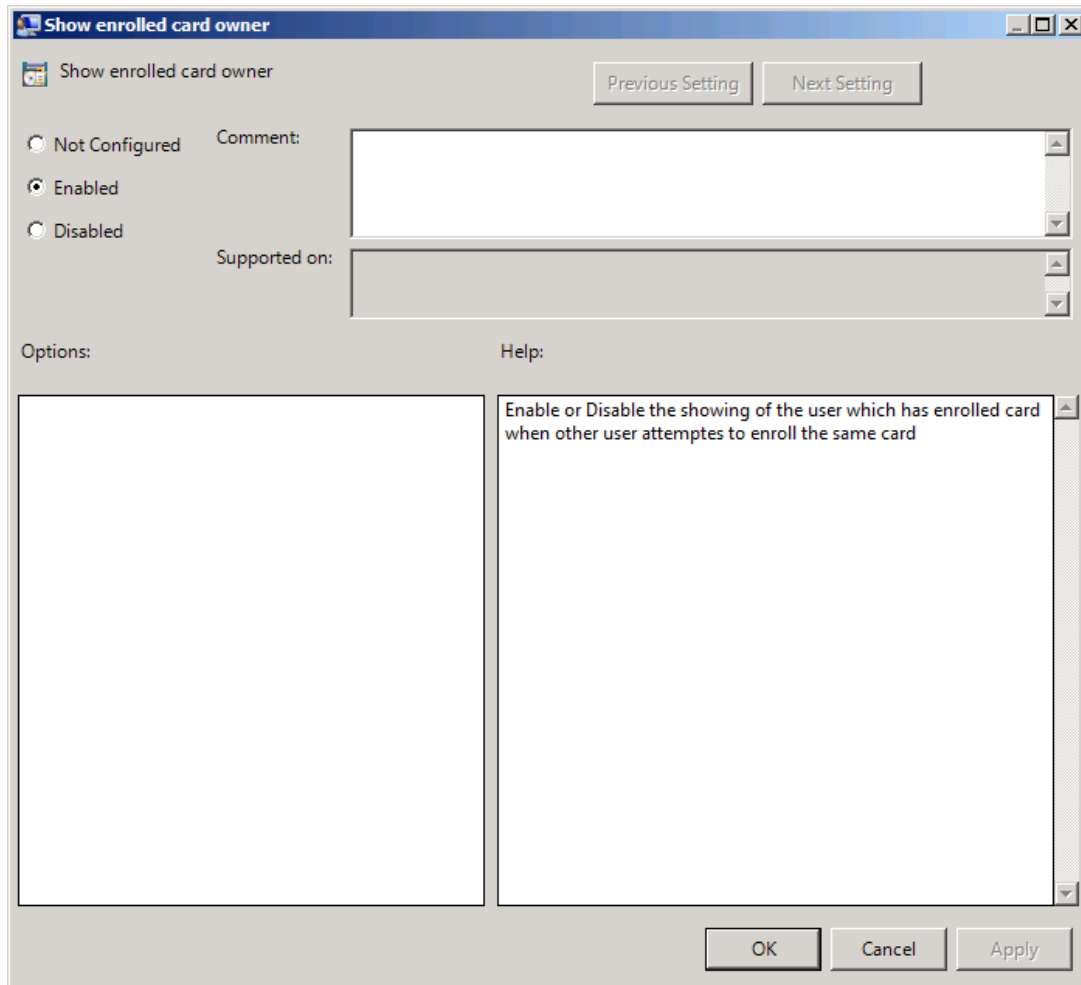
The **Runtime Environment** section includes a policy allowing to enable or disable showing of the user who has enrolled card.

It includes:

- [Show enrolled card owner](#)

Show Enrolled Card Owner

The **Show enrolled Card Owner** policy allows you to enable or disable showing of the user who has enrolled card when other user attempts to enroll the same card.



HKEY_ LOCAL_ MACHINE\SOFTWARE\Policies\ NetIQ \ NetIQ Advanced Authentication Framework\ RTE

parameter: RTEShowEnrolledCardOwner(REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled

Users and Groups

The **Users and Groups** section includes a policy allowing to specify users and groups settings manually.

It includes:

- [Customize users and groups settings](#)

Customize Users and Group Settings

The **Customize users and group settings** policy allows you to specify users and groups settings manually. If this policy is enabled and configured, Authenticore Server will use the specified users and groups names.

Customize users and groups settings

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Options:

Help:

Username for Authenticore Service

Groupname for Authenticore Servers

Groupname for Authenticore Admins

Groupname for ADAM Servers

Groupname for Product Admins

This policy provide users and groups settings. If this policy enabled and configured, Authenticore Server will be use custom users and groups

OK Cancel Apply

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\UsersAndGroups
parameters: ADAMServersGroups (REG_SZ)
AuthenticoreAdminsGroup (REG_SZ)
AuthenticoreServersGroup (REG_SZ)
AuthenticoreServiceUser (REG_SZ)
ProductAdminsGroup (REG_SZ)
UsersAndGroups (REG_DWORD)

values: NetIQ Advanced Authentication Framework ADAM Servers, Authenticore Admins, Authenticore Servers, AuthenticoreService, NetIQ Advanced Authentication Framework Admins, 0x00000001 (1)

NetIQ Advanced Authentication Framework ADAM Servers displays the specified groupname for ADAM Servers.


Authenticore Admins displays the specified groupname for Authenticore Admins.


Authenticore Servers displays the specified groupname for Authenticore Servers.


AuthenticoreService displays the specified username for Authenticore Service.

NetIQ Advanced Authentication Framework Admins displays the specified groupname for Product Admins.

1 means that the policy is enabled.

 Please, take into consideration that user account cannot contain periods or spaces, or end in a period. Any leading periods or spaces are cropped.

 Use of the @ symbol is not supported with the logon format for Windows NT 4.0 and earlier.

 During schema extension batch file cannot find registry key, if the **Customize users and group settings** policy is disabled. In this case only default values can be found by batch file.

Workstation Policies


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

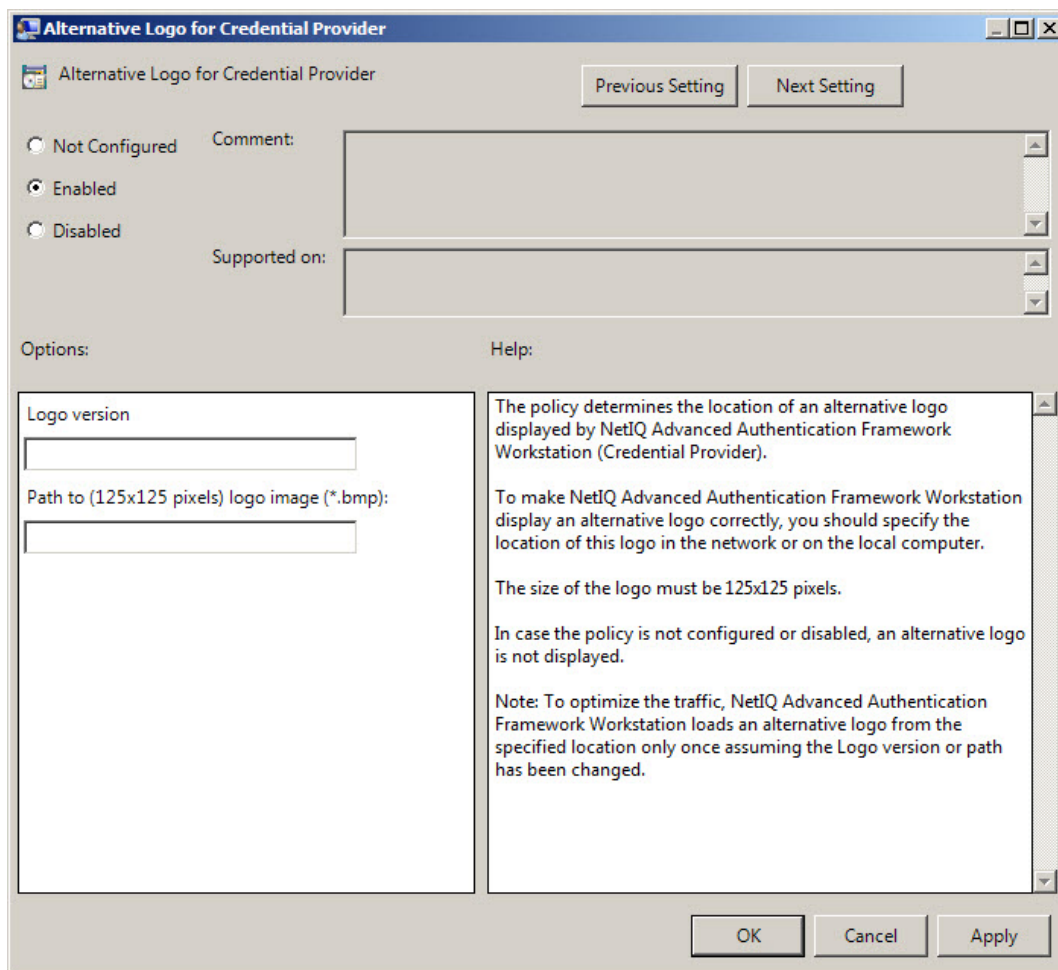
It includes:

- [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 first logon enroll wizard](#)
- [Disable "Use Dial-up connection" option](#)
- [Do not allow to skip welcome window](#)
- [Enable device detection for all](#)
- [Enhanced reaction on device events](#)
- [Lifetime of notification about password reset](#)
- [Linked logon behavior](#)
- [Tap and Go](#)
- ["Use current settings as defaults" option management for PC unlocking](#)
- ["Use current settings as defaults" option management](#)
- [Web service client timeout](#)

Alternative Logo for Credential Provider

The **Alternative logo for Credential Provider** 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.



To ensure that 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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\Brand




parameter: CLogo (REG_SZ)

CLogoVersion (REG_SZ)

value: 1, \\netiq\logos\cplogo.bmp


1 displays the configured logo version

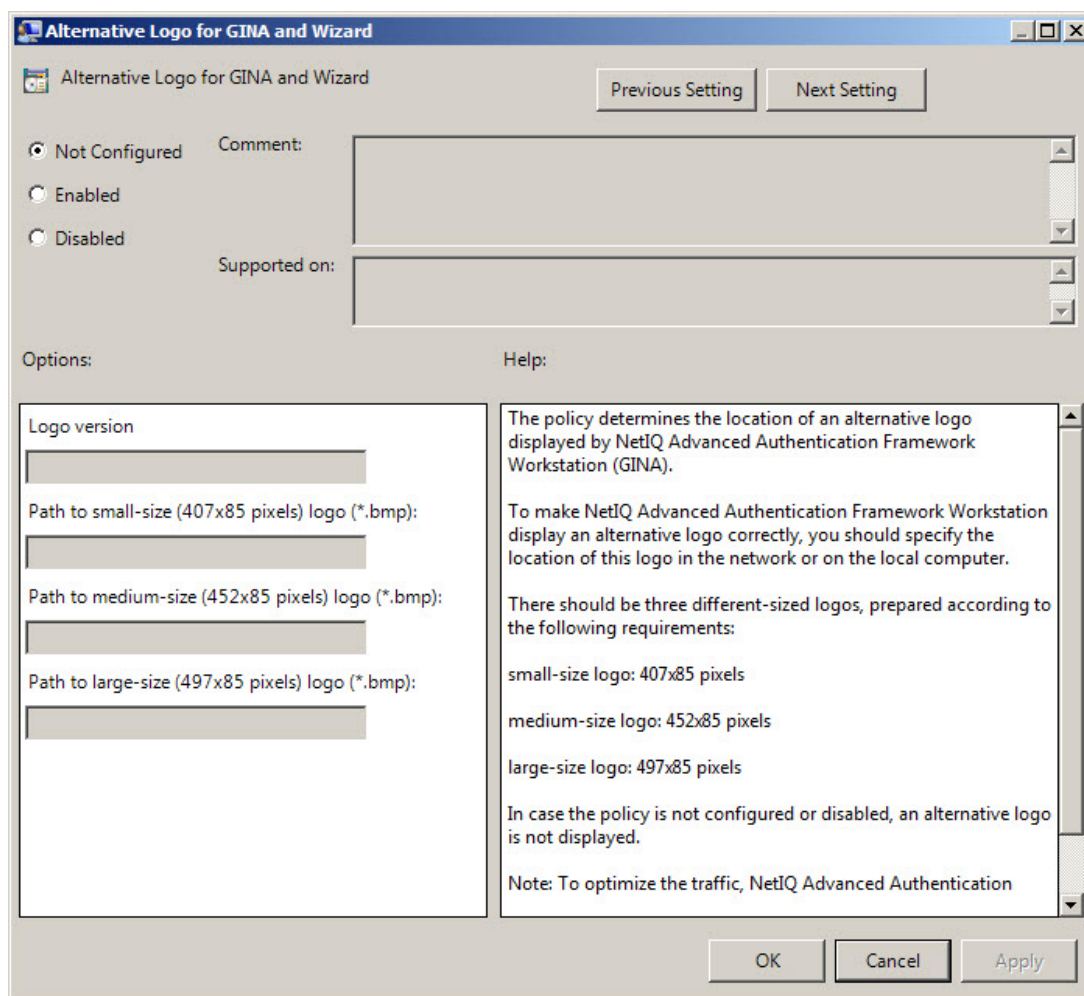
\\netiq\logos\cplogo.bmp displays the configured path to logo image

-  To specify the path to the logo file, you should use the server name, NOT its IP-address.
-  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 for GINA and Wizard** 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 Server 2003 operation systems; it is responsible for user authentication and credentials verification.



The screenshot shows a Windows-style dialog box titled "Alternative Logo for GINA and Wizard". At the top, there are "Previous Setting" and "Next Setting" buttons. Below these 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:" dropdown menu. Underneath, there are two sections: "Options:" and "Help:". The "Options:" section contains four text boxes for specifying logo paths: "Logo version", "Path to small-size (407x85 pixels) logo (*.bmp):", "Path to medium-size (452x85 pixels) logo (*.bmp):", and "Path to large-size (497x85 pixels) logo (*.bmp):". The "Help:" section contains a scrollable text area with the following text: "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". At the bottom of the dialog box are "OK", "Cancel", and "Apply" buttons.

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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\Brand

parameter: LargeLogo (REG_SZ)

LogoVersion (REG_SZ)

MediumLogo (REG_SZ)

SmallLogo (REG_SZ)


value: \\netiq\logos\cplogolarge.bmp, 1, \\netiq\logos\cplogomedium.bmp, \\netiq\logos\cplogosmall.bmp


\\netiq\logos\cplogolarge.bmp displays the path to large-size logo

1 specifies the configured logo version

\\netiq\logos\cplogomedium.bmp displays the path to medium-size logo


\\netiq\logos\cplogosmall.bmp displays the path to small-size logo

 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:

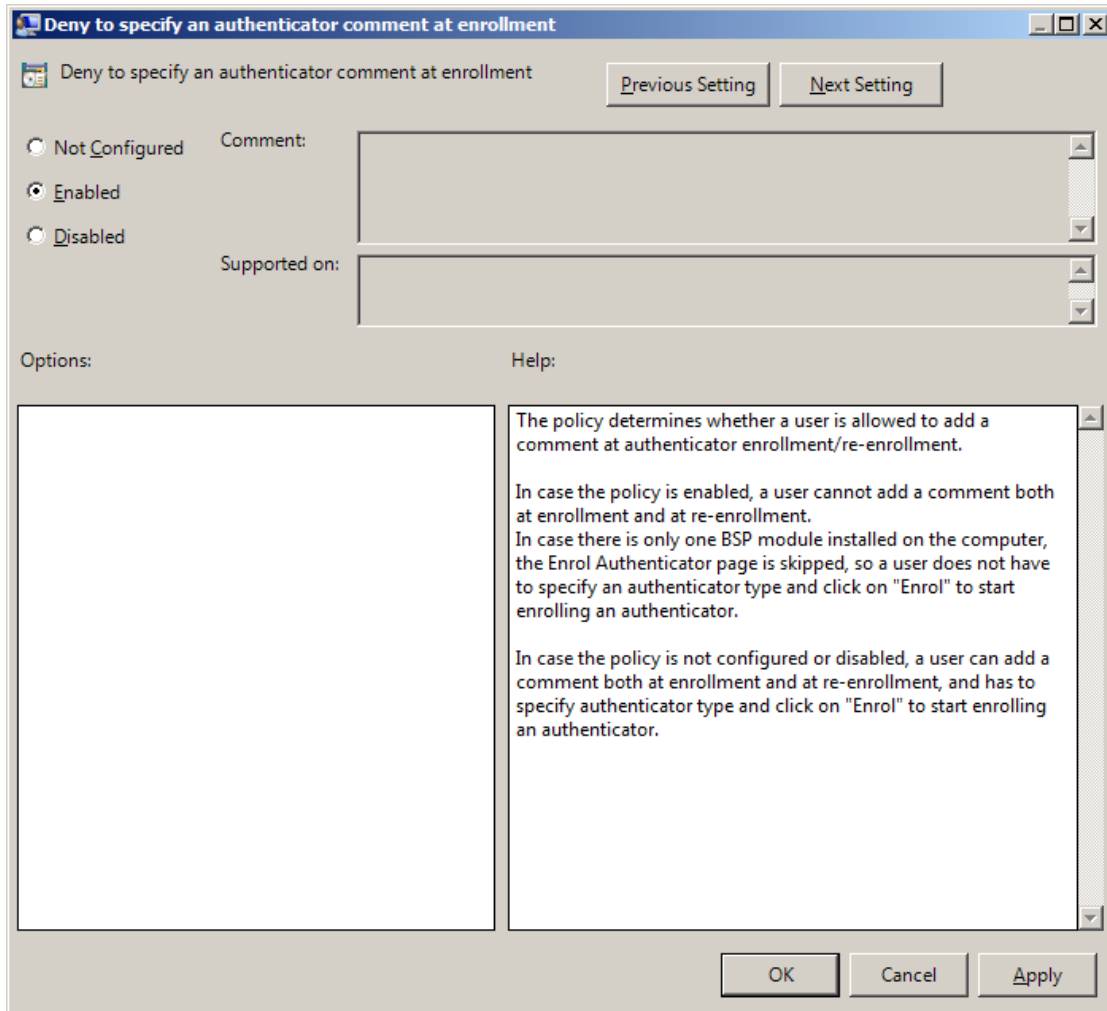
- small-size logo: 406x85 pixels;
- medium-size logo: 451x85 pixels;
- large-size logo: 495x85 pixels.

 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.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DenyAuthenticatorComment (REG_DWORD)

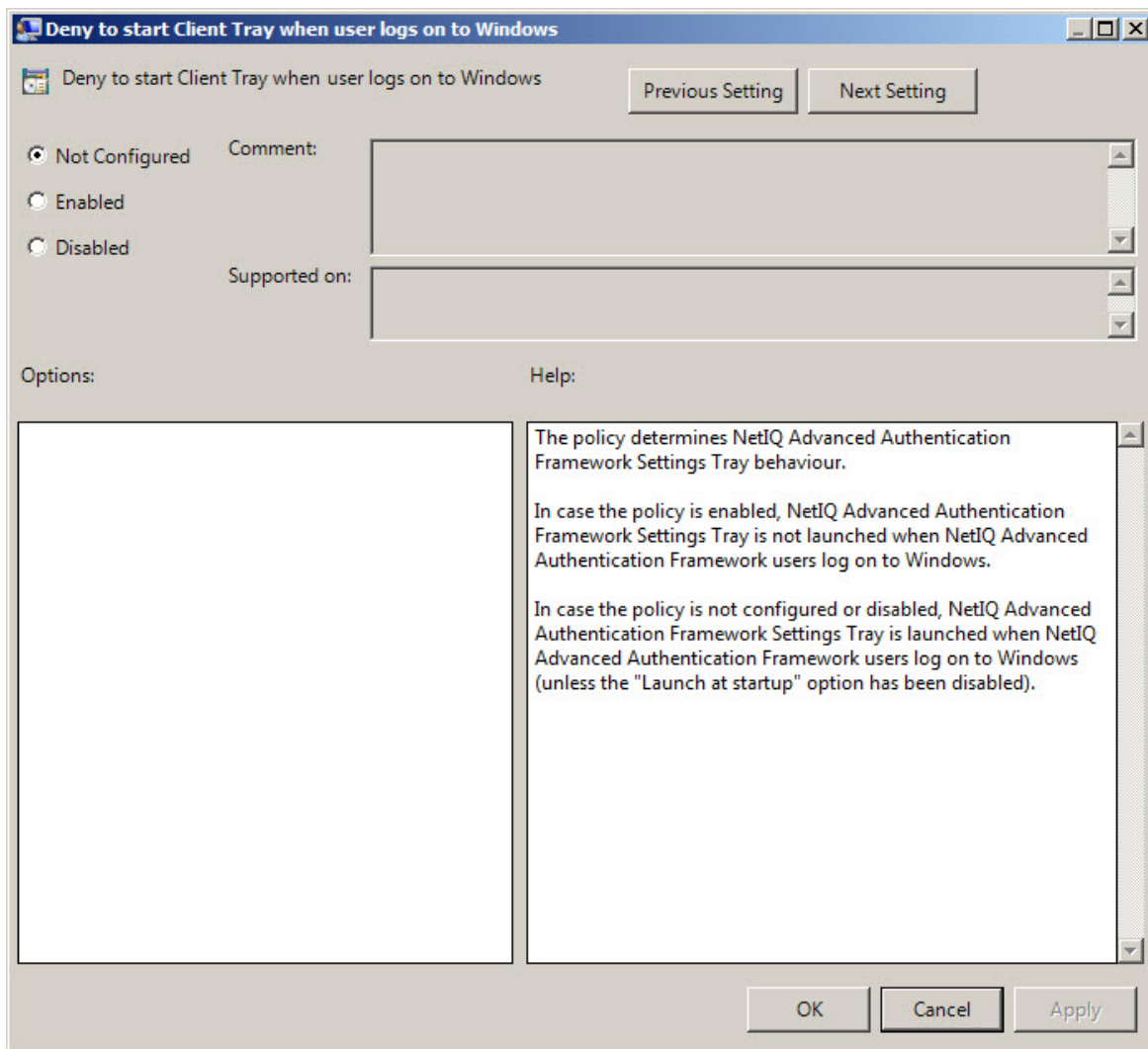
value: 0x00000001 (1)

1 means that the 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.


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.



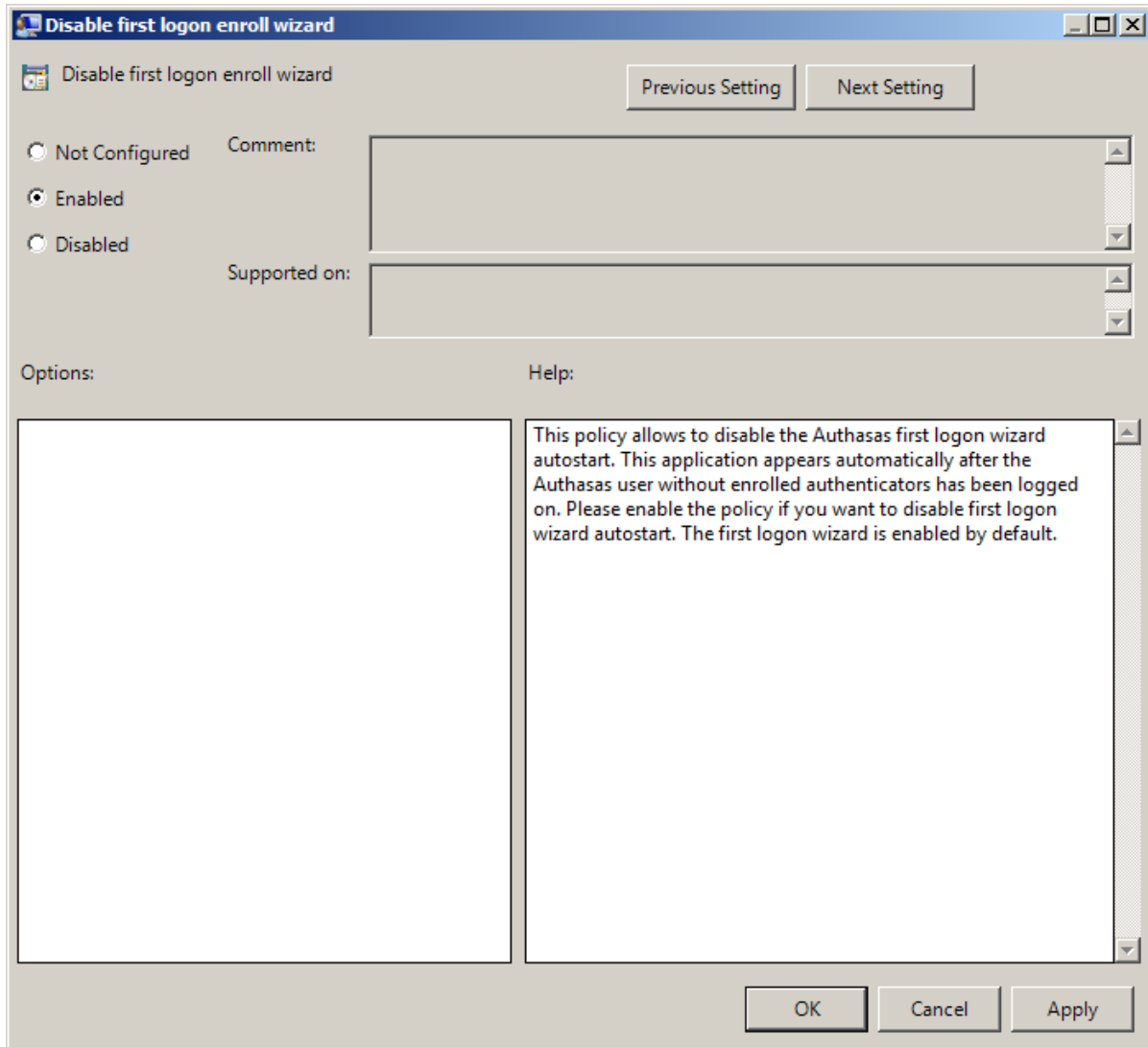
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DenyClientTrayAutoStart (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled

 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 First Logon Enroll Wizard

The **Disable first logon enroll wizard** policy allows to disable the NetIQ first logon wizard autostart. This application appears automatically after the NetIQ user without enrolled authenticators has been logged on.



Please enable the policy if you want to disable first logon wizard autostart. The first logon wizard is enabled by default.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DisableFirstLogonEnrollWizard (REG_DWORD)

value: 0x00000001 (1)

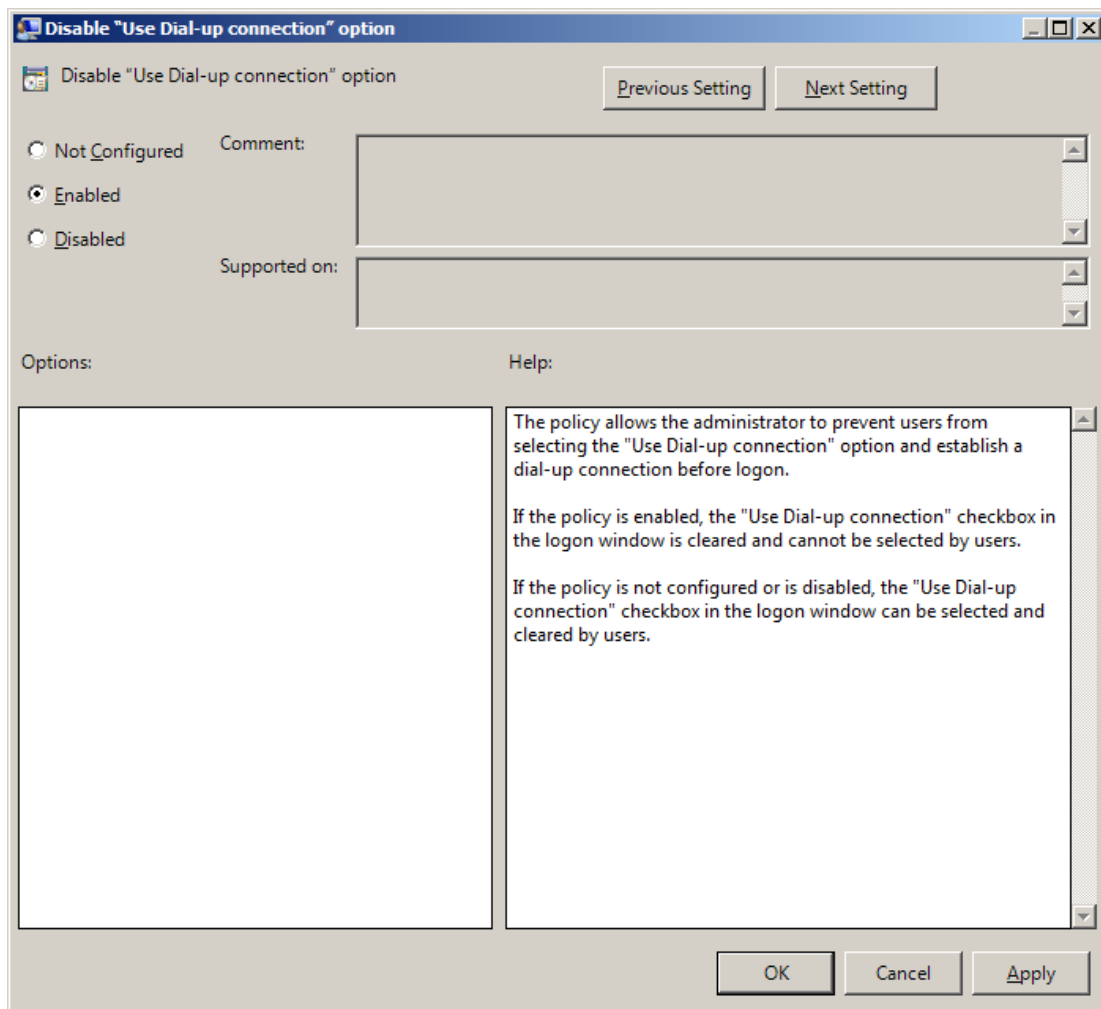
1 means that the policy is enabled

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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: GinaDisableDialUp (REG_DWORD)

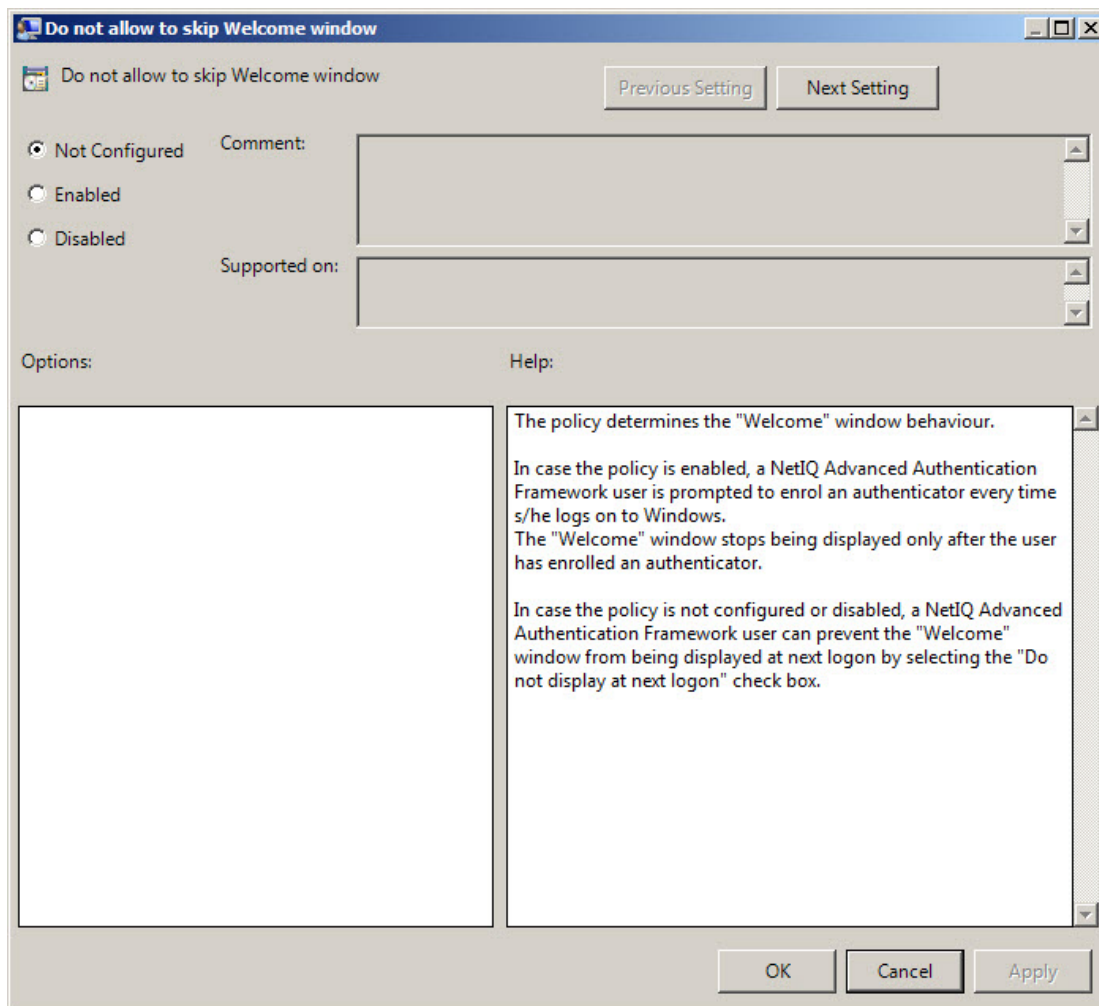
value: 0x00000001 (1)

1 means that the policy is enabled


 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, doesn't allow users to skip the **Welcome to NetIQ Advanced Authentication Framework System** at the first logon without enrolling at least one authenticator.



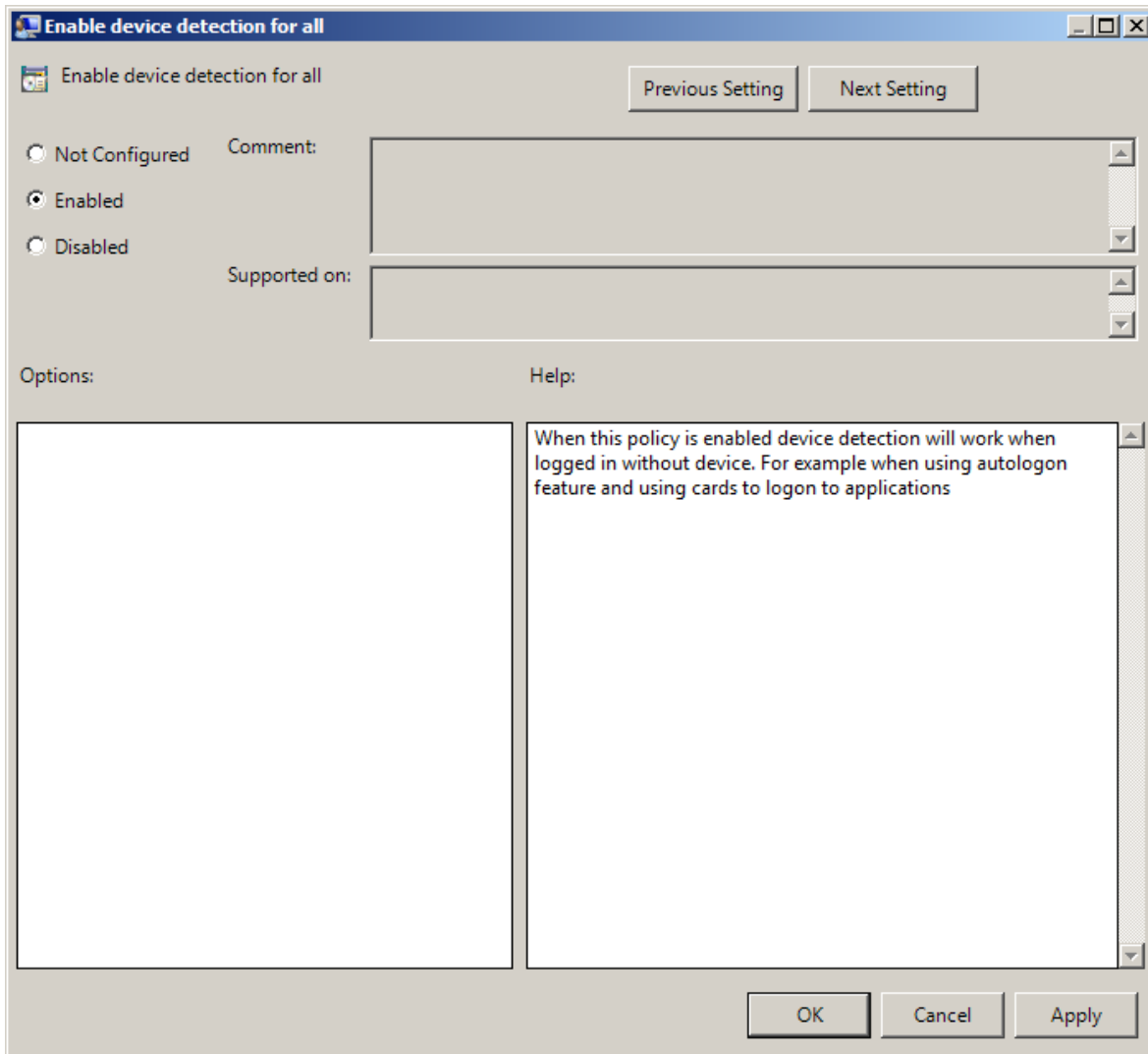
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: ShowFirstLogonWizardAlways (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled

 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 with card or flash drive (not only when logged in with the same card or flash drive, but also when logged in with another card or flash drive, other method of authentication or domain password). *For example*, when using autologon feature and using cards to logon to applications.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: IsDeviceDetectionForAllEnabled (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled

 The **Enable device detection for all** policy is supported only by card and flash drive authentication providers.

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

Enhanced reaction on device events

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Options:

Command line for plugged in event

Command line for plugged out event

Help:

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.






HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: PluggedInCommand (REG_SZ)

PluggedOutCommand (RED_SZ)

value: cmd /c C:\!\OnStart.cmd, cmd /c C:\!\OnEnd.cmd

cmd /c C:\!\OnStart.cmd displays the command line for plugged in event

cmd /c C:\!\OnEnd.cmd displays the command line for plugged out event

-  The **Enhanced reaction on device events** policy is supported only by card and flash drive authentication providers.
-  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.
-  The **Enhanced reaction on device events** policy for plugged-out events may conflict with **Interactive logon: Smart card removal behavior** system policy.
-  Environment variables are not supported.

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.

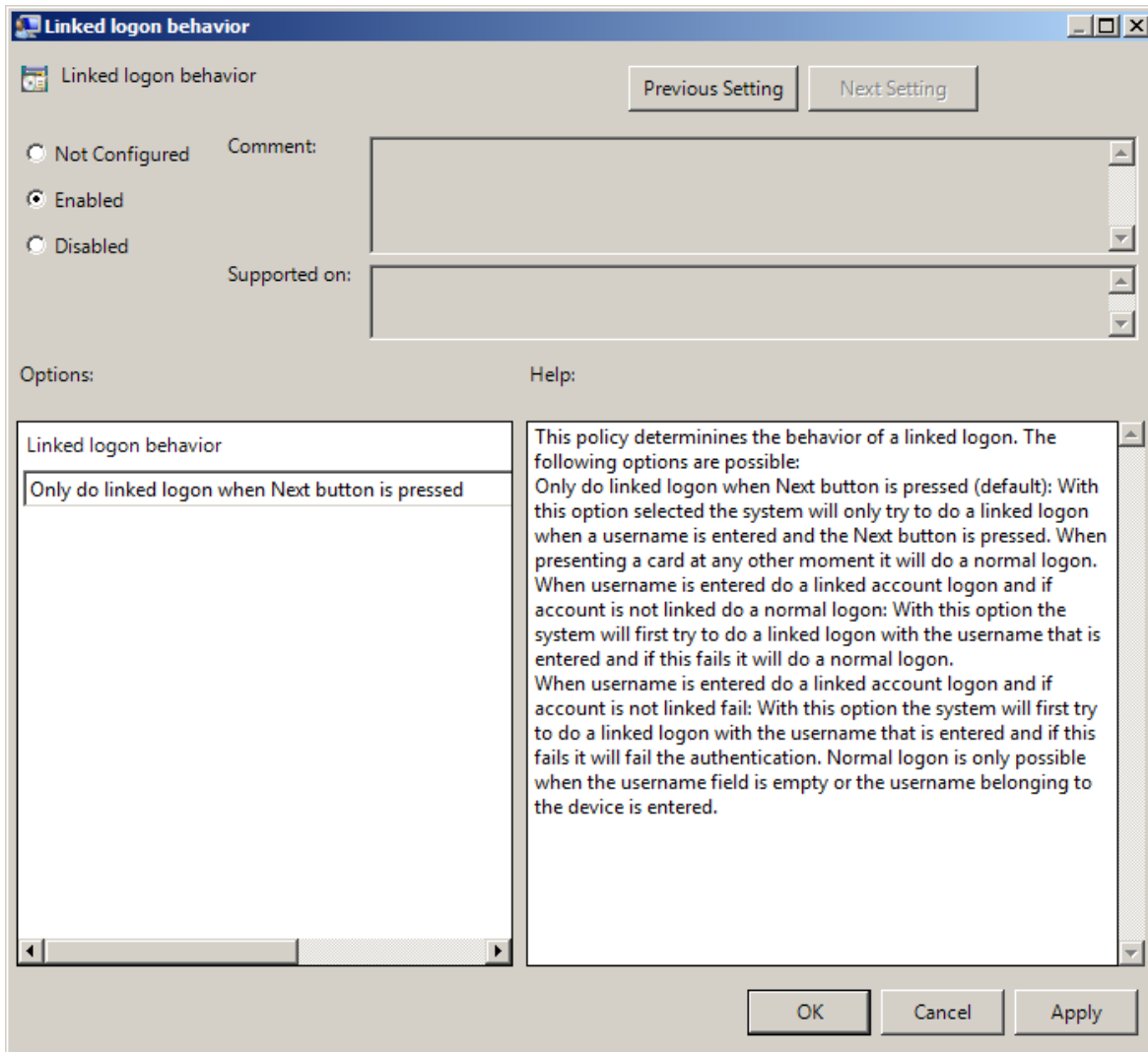
The screenshot shows a Windows-style dialog box titled "Lifetime of notification about password reset". At the top right, there are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the 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 spin box labeled "Lifetime of notification about password reset (in days)" with the value "14" displayed. To the right of the spin box is a "Help:" 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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: ResetPasswordNotificationLifeTime (REG_DWORD)
value: 0x0000000e (14),
14 displays lifetime of notification about password reset (in days)


Linked Logon Behavior

The **Linked logon behavior** policy determines the behavior of a linked logon. The following options are possible:

- Only do linked logon, when the **Next** button is pressed (default). If this option is selected, the system will only try to do a linked logon when a username is entered and the **Next** button is pressed. When pressing a card at any other moment, it will do a normal logon.
- When username is entered, do a linked account logon and if account is not linked, do a normal logon. With this option the system will first try to do a linked logon with the username that is entered and if this fails, it will do a normal logon.
- When username is entered, do a linked logon account logon and if account is not linked fail. With this option the system will first try to do a linked logon with the username that is entered and if this fails, it will fail the authentication. Normal logon is only possible when the username field is empty or the username that belongs to the device is entered.

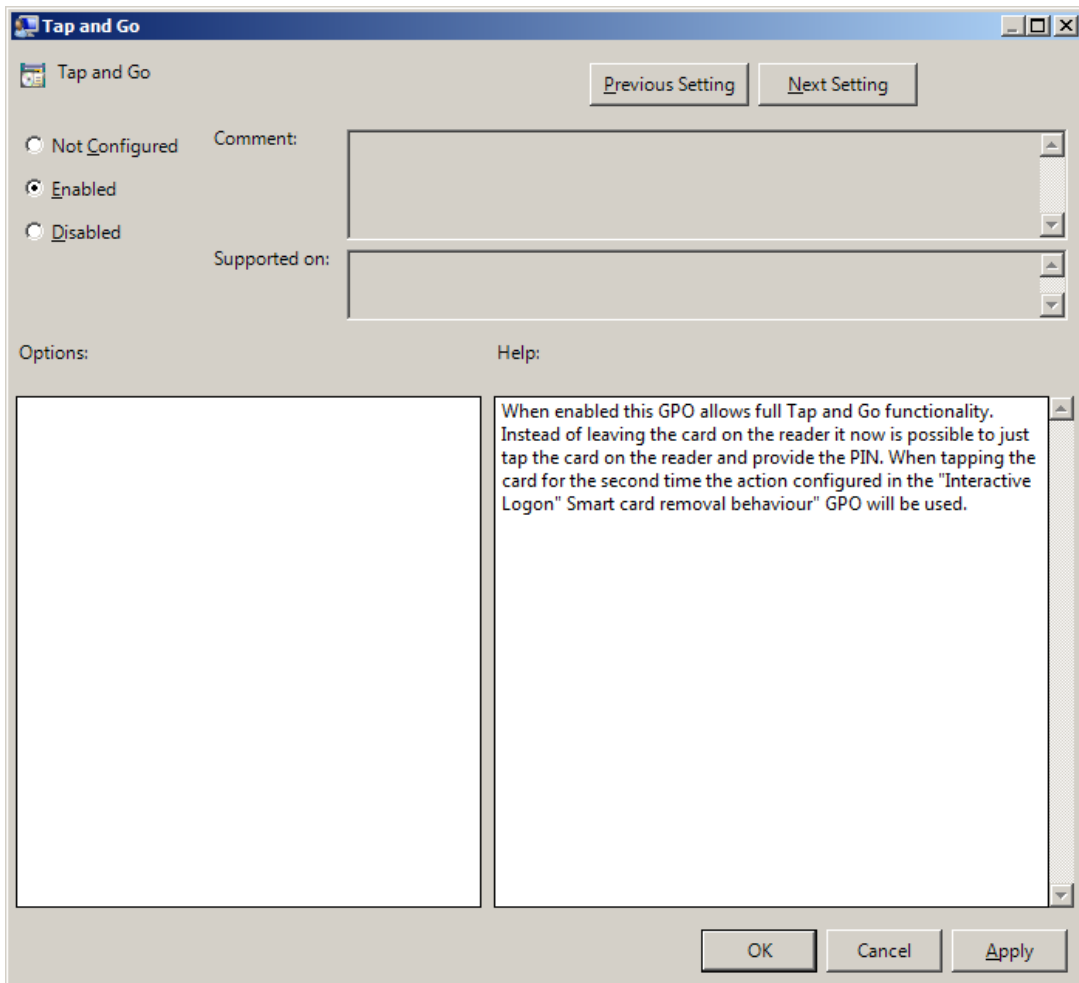


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
 parameter: LinkedLogonBehavior (REG_DWORD)
 value: 0x00000000 (0), 0x00000000 (0), 0x00000000 (0)
 0 means that the policy is enabled

 The **Linked logon behavior** policy works currently only for Microsoft Windows Server 2003/ Microsoft Windows Server 2003 R2.

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.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: TapAndGo (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled



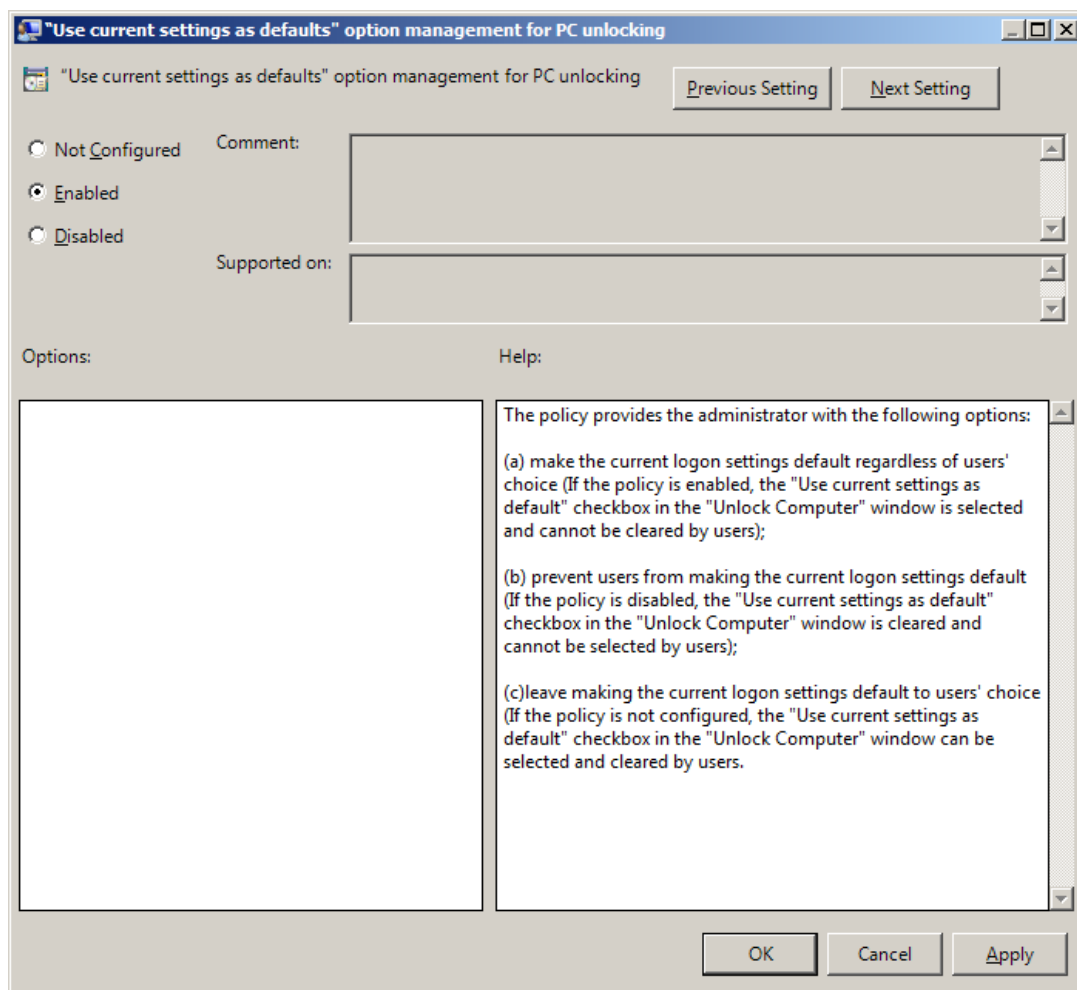
If the policy is not configured or is disabled, user cannot take the card from the reader until the Logon process is finished.

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

The **"Use current settings as defaults" option management for PC unlocking** 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 canceled by users.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework parameter: GinaCurrentAsDefaultUnlock (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled

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

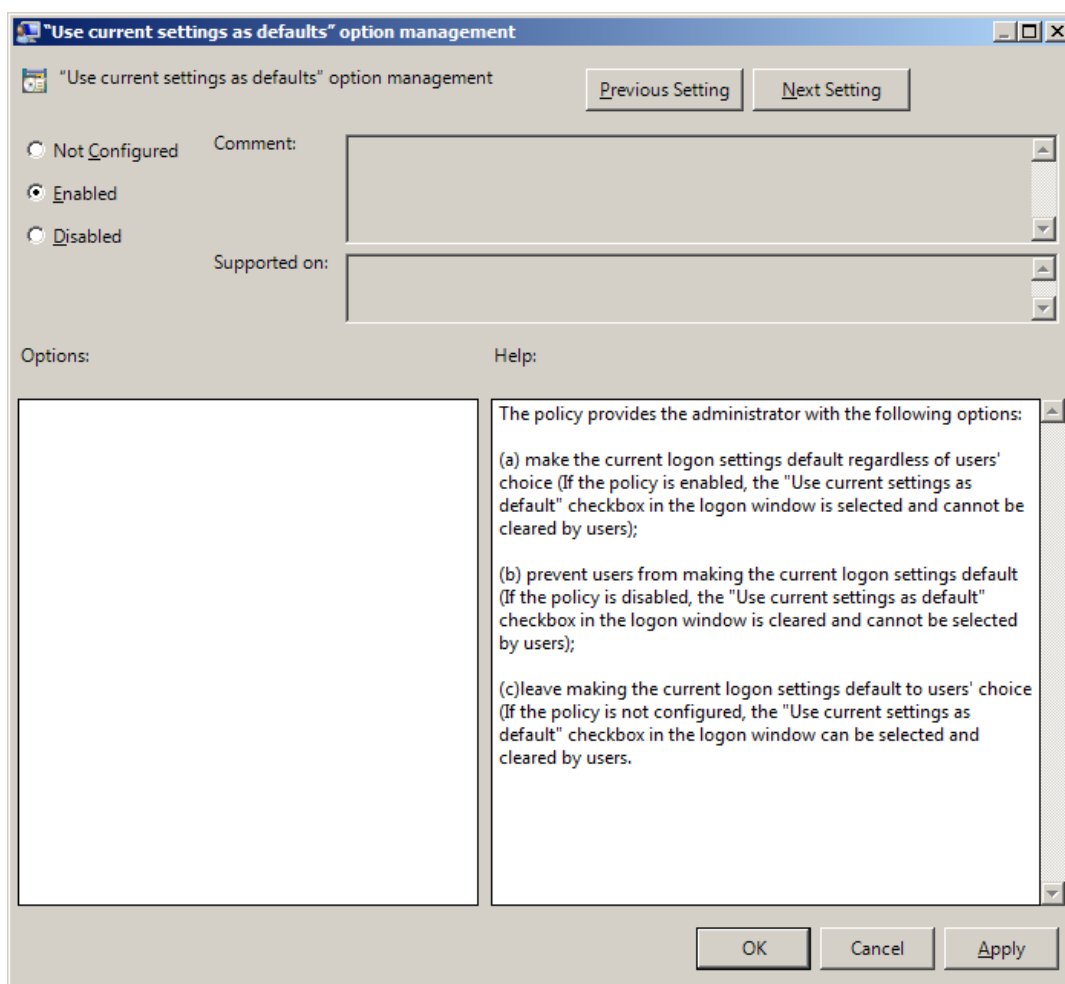
 If the policy is not configured, the **Use current settings as defaults** option is enabled and can be selected or canceled by users.

"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.



HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: GinaCurrentAsDefault (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled

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 canceled by users.

Web service client timeout

The **Web service client timeout** policy allows you to increase the timeout value for Web Service as with the default timeout value when using Voice Call via Web Service the timeout can expire before entering the PIN.

Web service client timeout

Previous Setting Next Setting

Not Configured Comment:

Enabled


Disabled

Supported on:

Options: Help:

Web service client timeout: 10 Web service client timeout

OK Cancel Apply

 It is required to set at least 30 seconds of authentication timeout for Voice Call authentication method and at least 45 seconds for SMS authentication method.


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: WebServiceClientTimeout (REG_DWORD)
value: 0x0000000a (10)
10 displays duration of authentication timeout in seconds

Repository Policies

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

It includes:

- [ADAM settings](#)
- [Enable Novell support](#)
- [Repository](#)

 Before the configuration the AAA_REPOSITORY.adm and AAA_REPOSITORY_ADAM.adm files should be copied from **\Tools\Policies** of NetIQ distributives folder to **%SYSTEMROOT%\Inf** folder.

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. It features a title bar with the text 'ADAM Settings' and standard window controls. Below the title bar, there are two buttons: 'Previous Setting' and 'Next Setting'. The main area is divided into several sections. On the left, 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:' list box. The bottom section is split into two panes. The left pane is labeled 'Options' and contains two input fields: 'LDAP path to root element' with the value 'CN=NAAF' and 'ADAM servers port number' with a spin box set to '50000'. The right pane is labeled 'Help' and contains the text 'Configure if ADAM / AD-LDS is used as repository.'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: Port (REG_DWORD)

RootPath (REG_SZ)

value: 0x0000c350 (50000), CN=AAA

50000 displays ADAM server port number

CN=NAAF is a LDAP path to root element

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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\Repository

parameter: NovellSupportEnabled (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled

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' configuration dialog box. It has a title bar with 'Repository' and standard window controls. 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 is a 'Comment:' text box. Below the radio buttons is a 'Supported on:' dropdown menu. At the bottom, there are two sections: 'Options:' and 'Help:'. The 'Options:' section has a 'Repository Type' dropdown menu currently set to 'ADAM instance'. The 'Help:' section contains a text box with 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 three buttons: 'OK', 'Cancel', and 'Apply'.

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

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

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\Repository
parameter: Type (REG_DWORD)
value: 0x00000002 (2)

2 means that ADAM instance is chosen.

UI Look & Feel Policies

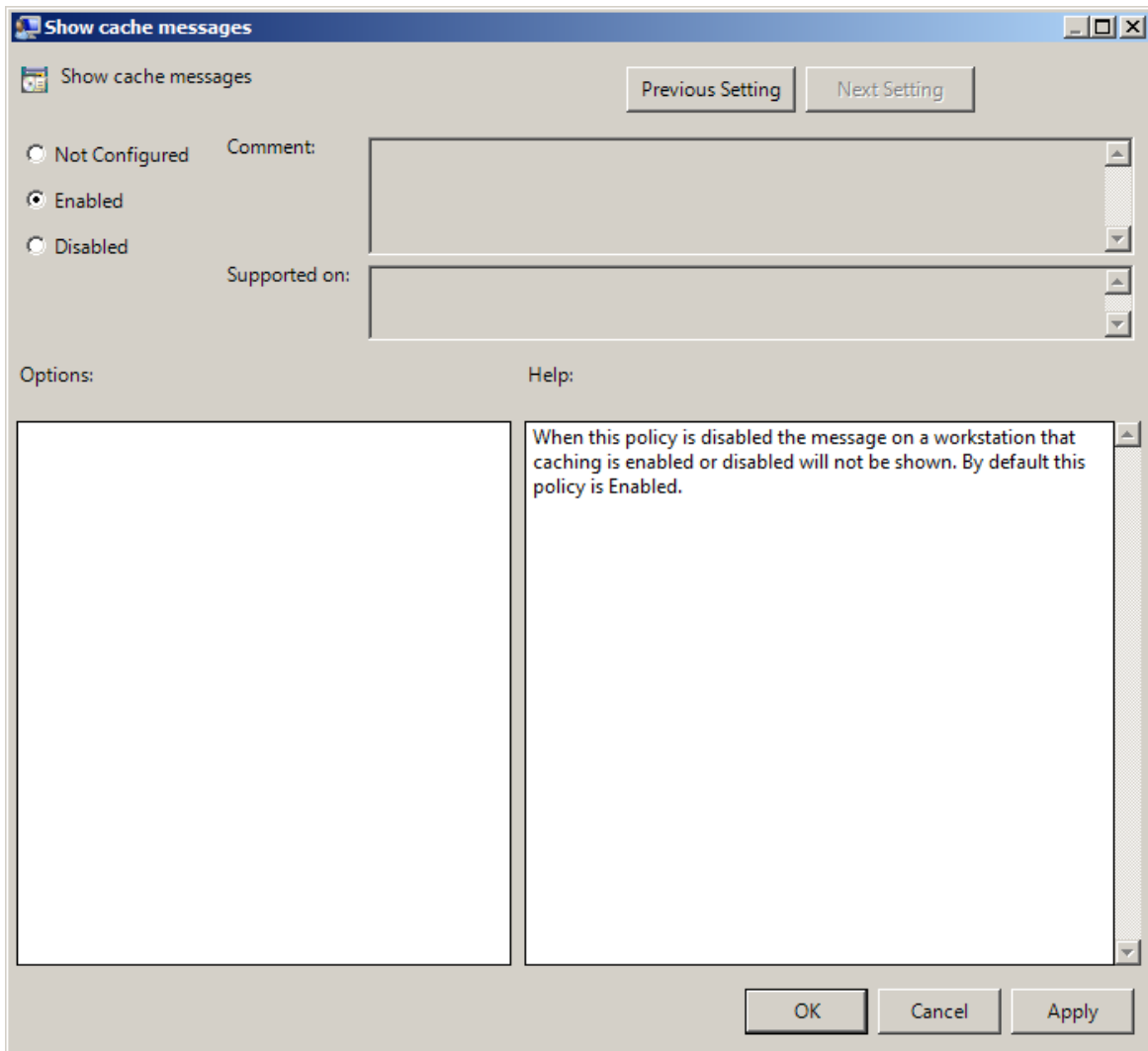
The **UI Look & Feel** section includes policies designed for terminal clients. The **UI Look & Feel** section is located in **Group Policy Management Editor** under **User Configuration -> Policies -> Administrative Templates: Policy definitions -> NetIQ Advanced Authentication Framework**.

It includes:

- [Show cache messages](#)
- [Show OSD](#)

Show Cache Messages

When the **Show cache messages** policy is disabled, the message on a workstation that caching is enabled or disabled will not be shown.

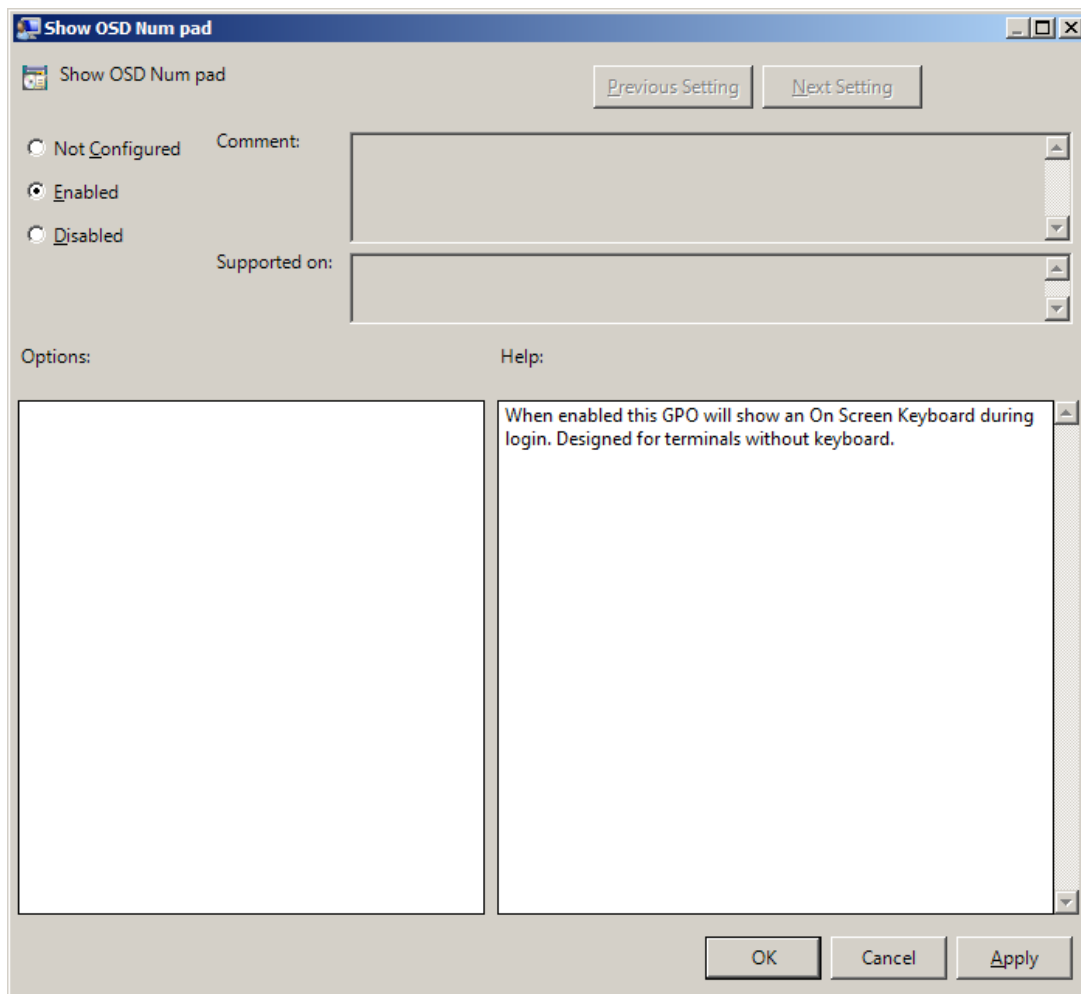


By default this policy is enabled.

HKEY_CURRENT_USER\Software\Policies\NetIQ\NetIQ Advanced Authentication
parameter: ShowCacheMessages (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled

Show OSD Num Pad

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



HKEY_CURRENT_USER\Software\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: OSDNumPadEnabled (REG_DWORD)

value: 0x00000001 (1)

1 means that the policy is enabled

Configuration of Windows Firewall with Advanced Security

To configure Windows Firewall with Advanced Security, do the following:

1. Right click the **Inbound Rules** inlay and select **New Rule...**
2. The **New Inbound Rule Wizard** will be displayed. To configure **Custom** type of rules, follow the steps:

- **Rule Type:** Select the **Custom** type of rule to create. Click **Next** to continue.
- **Program:** Select **All programs** to apply the rule to all connections on the computer that match the other rule properties. Click **Next** to continue.
- **Protocol and Ports:** Specify the protocols and ports to which the rule applies. **Local port:** RPC Dynamic Ports; **Remote port:** All Ports. Click **Next** to continue.
- **Scope:** Specify the local and remote IP addresses to which the rule will be applied. Select **Any IP address** for both local and remote IP addresses. Click **Next** to continue.
- **Action:** Specify the action to be taken when a connection matches to conditions specified in the rule. Select **Allow the connection** to include connections that are protected with IPsec as well as those are not. Click **Next** to continue.
- **Profile:** Specify the profiles for which this rule applies. Select **Domain** (applies when a computer is connected to its corporate domain) and **Private** (applies when a computer is connected to a public network location). Click **Next** to continue.
- **Name:** Specify the name of the new rule. New rule is successfully configured.


3. To configure **Port** type of rule, follow the steps:

- **Rule Type:** Select the **Port** type of rule to create. It will control connections for a TCP or UDP port. Click **Next** to Continue.
- **Protocol and Ports:** Specify the protocols and ports to which the rule applies. Select **TCP** and specify the port. Click **Next** to continue.
- **Action:** Specify the action to be taken when a connection matches to conditions specified in the rule. Select **Allow the connection** to include connections that are protected with IPsec as well as those are not. Click **Next** to continue.
- **Profile:** Specify the profiles for which this rule applies. Select **Domain** (applies when a computer is connected to its corporate domain) and **Private** (applies when a computer is connected to a public network location). Click **Next** to continue.
- **Name:** Specify the name of the new rule. New rule is successfully configured.

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.

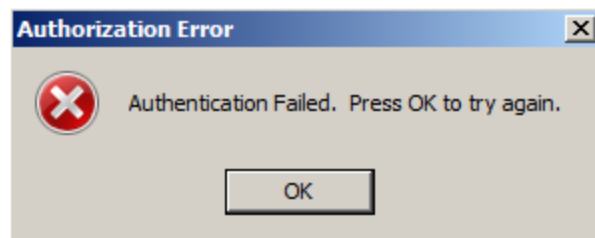
User Authentication Error

Description:

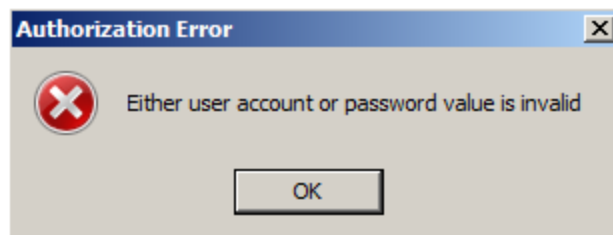
The user cannot log on and receives an error message.

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.

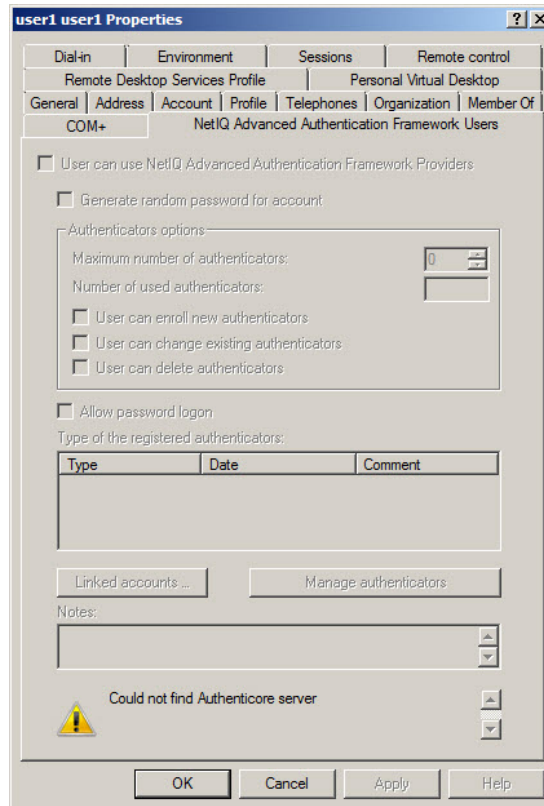


Inbound rules are required (See the [Configuration of Windows Firewall with Advanced Security](#) chapter.)

NetIQ Users Settings in ADUC are not Active

Description:

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



Cause:

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

Solution:

- Check the Network and Firewall settings.
- 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.

A

Account 62, 98, 101
Active Directory 7, 9-10, 12-13, 15-19, 25, 39, 41, 45, 47, 55-56, 61, 72, 82, 151, 154, 162
Administrator 1, 5-6, 12-13, 27, 72
ADUC 16, 18, 41, 53, 163
Authentication 1, 5-6, 8-9, 11-13, 15-16, 18-19, 25, 38-39, 41-42, 46-47, 50, 52-53, 57-59, 68, 70, 72, 75, 80, 85, 87, 89-90, 92-95, 97-98, 100-101, 104, 108-109, 111-112, 114-116, 118, 121, 123, 126, 128, 130-131, 133-134, 136, 138, 140, 142, 144-146, 148, 150, 152-154, 156-158, 161-162, 164
Authenticator 5, 10-11, 17, 23, 33, 35-37, 55, 70-71, 80, 84-85, 130, 164
Authenticore server 13, 59-60, 67, 71, 85, 162, 164
Automatic logon 46

B

BIO-key 14

C

Caching 16, 91, 94
Card 14, 103, 121
Client 6, 9, 13, 80, 94, 97, 116, 119, 127-128, 140
Client Tray 81, 125, 131
Comment 24, 27, 34-35
Connection 134
Console 50
Control 10-11, 15-16, 25, 42
Create 18, 57
Credential providers 80, 84, 87
Current authenticator 10

D

Data 57, 70, 73, 76
Default 80, 84, 89
Delete 51
Desktop 13
Device 138, 140
Dial-up 81, 125, 134
Domain 11, 15, 67, 82, 129, 153, 159, 162

E

Edit 18
Enroll 10-11, 22, 32-33, 35-36, 51, 54
Enterprise Key 7, 10-11, 60, 73
Error 60, 68, 98, 160-161, 164
Event Log 80, 106
Event Viewer 58-59
Export 57

F

File 47

G

Generate 21, 26, 80, 92
GINA 46, 75, 81, 125, 128

L

License 63, 74, 77
Linked accounts 28
List 90, 96
Local 59, 159
Logo 81, 125-126, 128
Logon 5, 31, 53, 57, 60, 72, 81, 133-134, 143, 145, 148
Lumidigm 14

M

Manage 27, 31, 38, 53
Message 60, 67-70, 72-76, 78-79
Microsoft Windows Server 2003 144
Microsoft Windows Server 2008 39, 83

N

Network 13, 81, 113, 163
Notification 142

O

OATH 14

P

Password 13, 39, 68, 80, 84, 92, 97, 101, 111

PIN 14, 80, 84, 90, 95, 103-104, 114, 145, 150
Policy 13, 83, 156
Properties 9, 17, 38, 41, 53, 162
Protocol 159

R

RADIUS 14
Re-enroll 10-11, 36, 51
Record 76
Reference authenticator 10
Remote 159, 162
Remove 18, 27, 37, 47, 93
Reset 18
RTE 7, 9, 13, 121, 140

S

Screen 82, 158
Security 9-10, 12, 14, 80, 83-84, 89-90, 159
Server 6, 11-13, 15, 58, 60, 69-70, 107, 114, 116, 118, 123, 162-164
Settings 64, 87, 123, 132, 146, 148, 152, 154, 160, 163
Software 157-158
Support 46, 153
System 10, 12, 59, 71, 136

T

Test 24, 32-33, 35, 54

U

User 9-10, 12, 17-19, 23, 25, 34, 39, 41, 50, 53, 68-69, 72-73, 75, 77, 112, 156, 160-161
User Viewer 9, 12-13, 16, 45, 47, 50, 52-53, 57, 161

W

Window 136
Windows 7, 11, 13, 15, 46, 81, 83, 124, 128, 131, 136, 159, 162
Windows Vista 126
Workstation 12, 81, 125