NetIQ Advanced Authentication Framework - Group Policy Templates

Administrator's Guide

Version 5.1.0

Table of Contents

Introduction

About This Document

Purpose of the Document

This Group Policy Templates Guide is intended for system administrators and describes how to control the working environment of user and computer accounts using NetIQ Advanced Authentication Framework Group Policy Templates.

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.

Group Policies

NetIQ Advanced Authentication Framework solution has 45 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.
- Enable 802.11 pre logon authentication - allows you to enable the detection of network connections 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.
- Last used server timeout - allows you to specify time during which the last Authenticore Server can be used for authentication.
- 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.

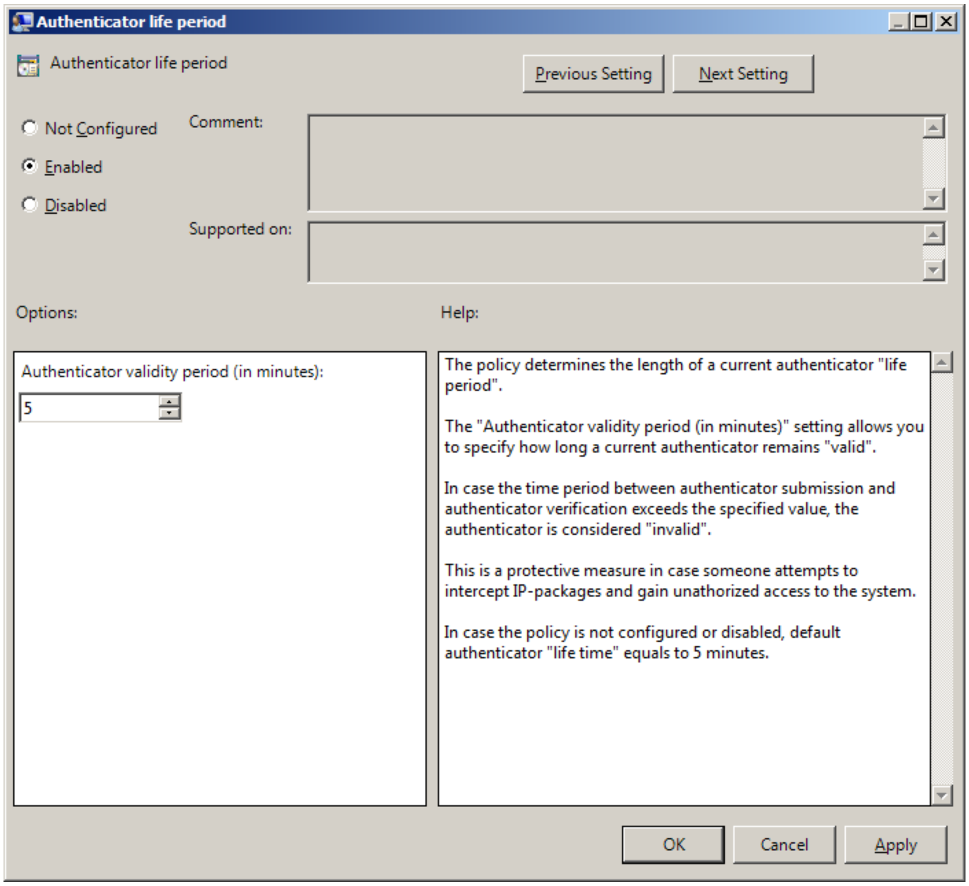
It includes:

- 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.



Authenticator validity period (in minutes): 5

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

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

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

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

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

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
AuthenticatorLifePeriod:

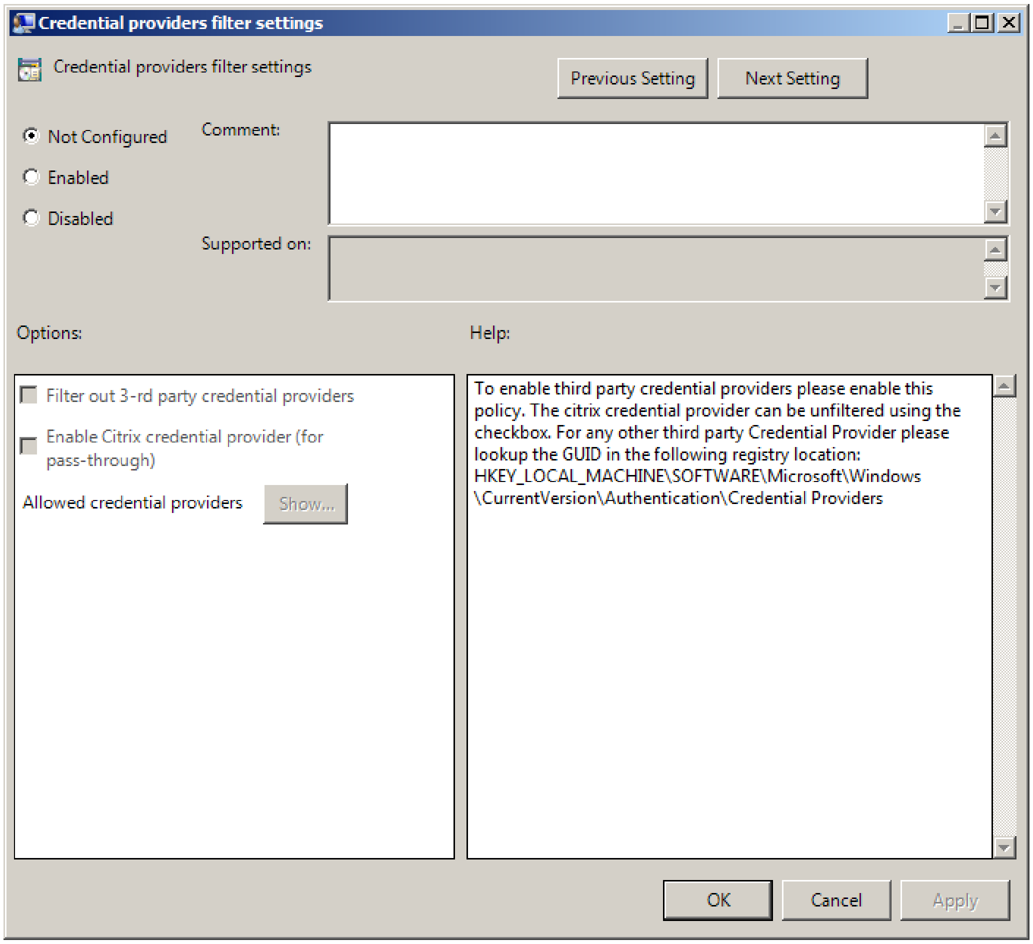
- type: REG_DWORD
- value: 0x00000005 (5)

- description: 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 enable third party credential providers. The citrix credential provider can be unfiltered using the checkbox. For any other third party Credential Provider, please, lookup the GUID in the following registry location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\
Authentication\Credential Providers.



● Not Configured
○ Enabled
○ Disabled

□ Filter out 3-rd party credential providers

□ Enable Citrix credential provider (for pass-through)

Allowed credential providers

To enable third party credential providers please enable this policy. The citrix credential provider can be unfiltered using the checkbox. For any other third party Credential Provider please lookup the GUID in the following registry location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
\CurrentVersion\Authentication\Credential Providers

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.

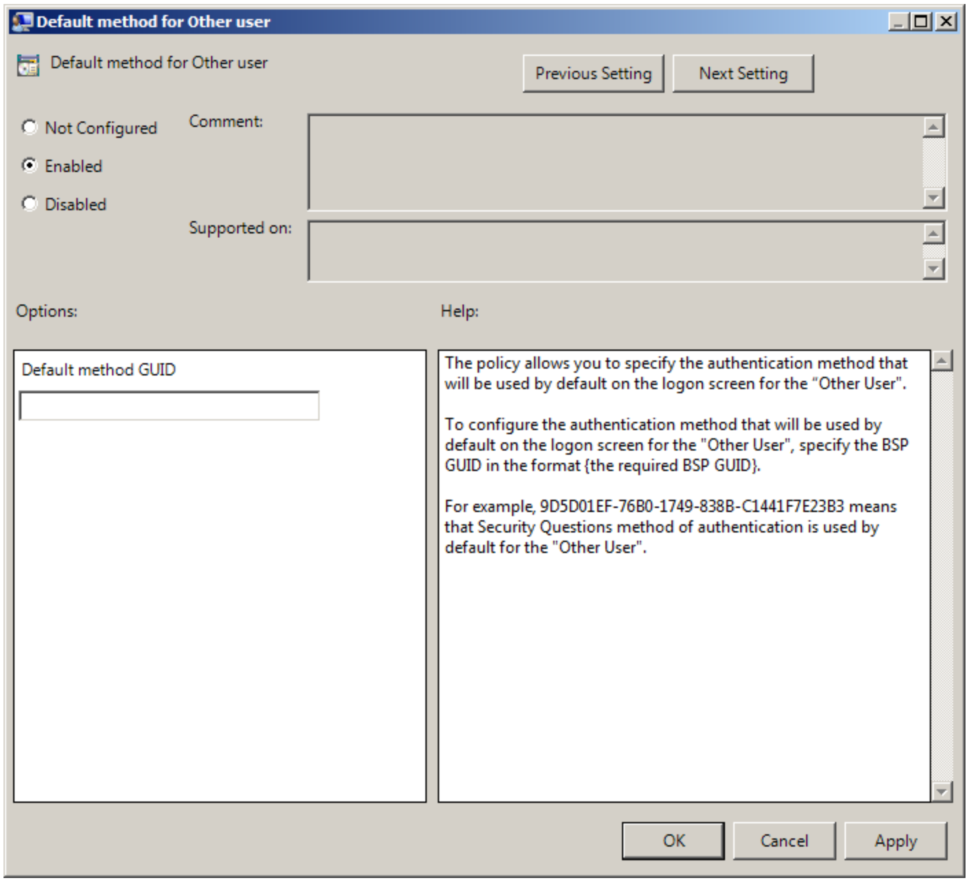
HKEY_ LOCAL_ MACHINE\SOFTWARE\Policies\ NetIQ \ NetIQ Advanced Authentication Framework\Filter\AllowedCPs
1:

- type: REG_SZ
- value: 5
- description: 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”.



○ Not Configured
● Enabled
○ Disabled

Default method GUID

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".

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}.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
OtherUserDefMethod:

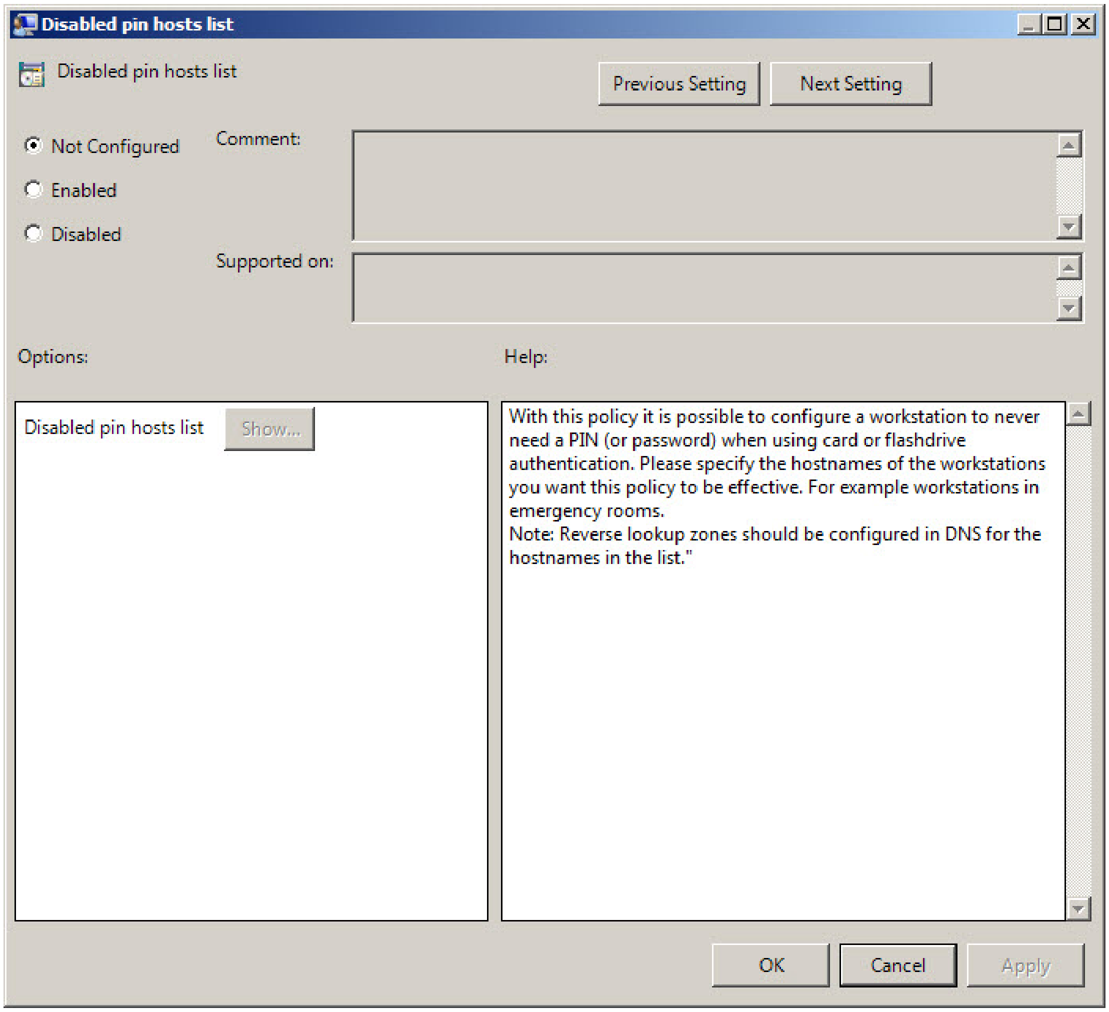
- type: REG_SZ
- value: {9D5D01EF-76B0-1749-838B-C1441F7E23B3}
- description: {9D5D01EF-76B0-1749-838B-C1441F7E23B3} means that Security Questions method of authentication is used by default for the "Other user"

To get the required value of BSP GUID, check the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BSP. It contains subkeys with GUIDs of all installed authentication providers. Check subkeys to find the required authentication method. The subkey name is the required BSP GUID.

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.



Disabled pin hosts list

● Not Configured
○ Enabled
○ Disabled

Disabled pin hosts list

With this policy it is possible to configure a workstation to never need a PIN (or password) when using card or flashdrive authentication. Please specify the hostnames of the workstations you want this policy to be effective. For example workstations in emergency rooms.
Note: Reverse lookup zones should be configured in DNS for the hostnames in the list."

HKEY_ LOCAL_ MACHINE\SOFTWARE\Policies\ NetIQ \ NetIQ Advanced Authentication Framework\DisabledPinHostList
Host1 (the specified host name is displayed in the registry parameter):

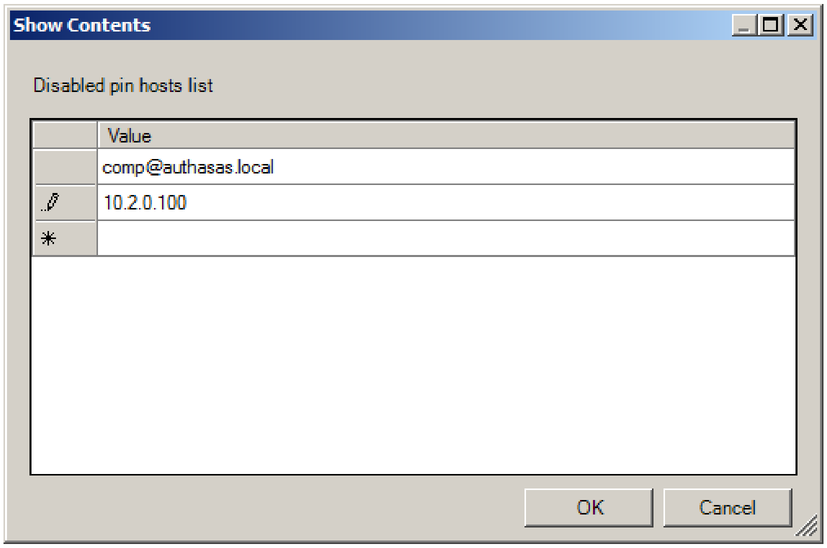
- type: (REG_SZ)
- value: 1
- description: 1 displays the value that was added to the Show Contents window

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.



Disabled pin hosts list

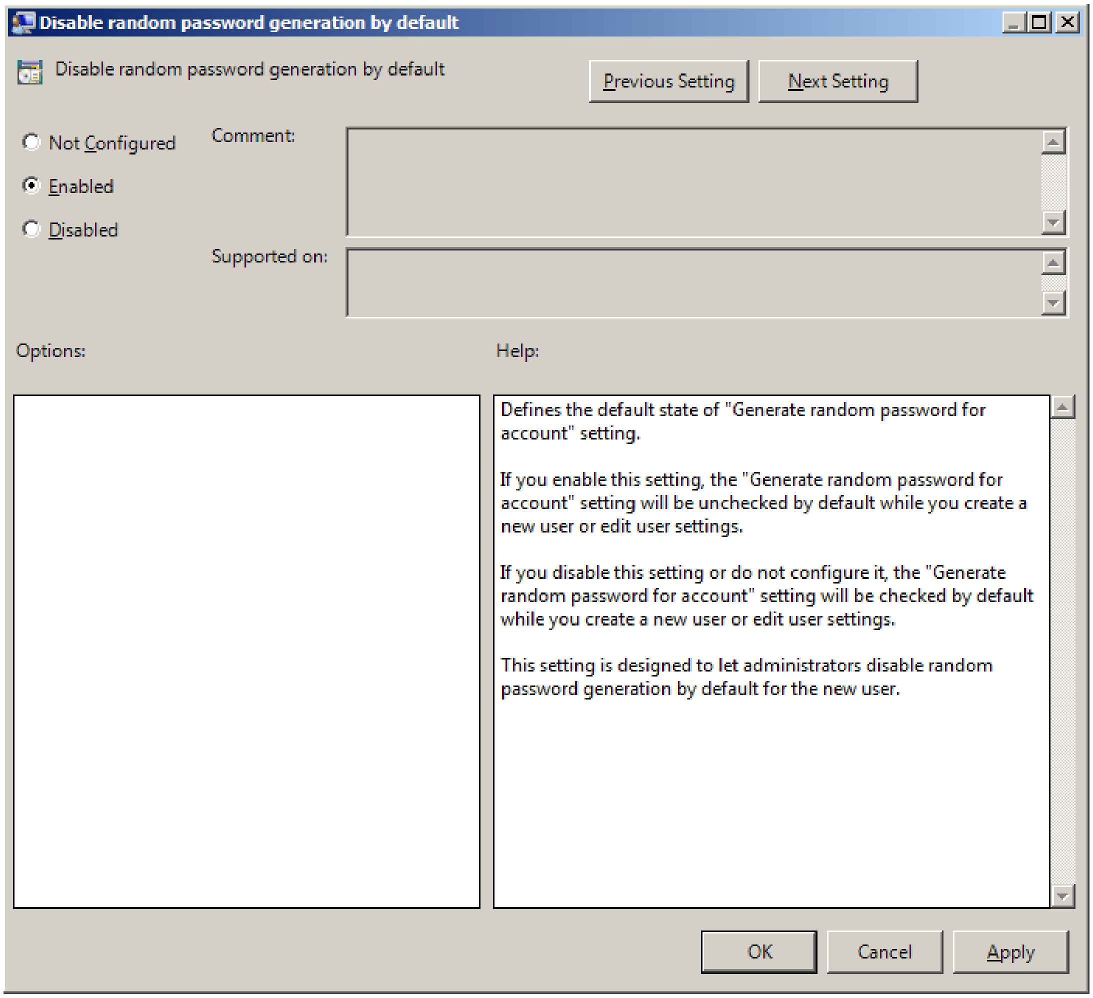
Value
comp@authasas.local
10.2.0.100

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.



Disable random password generation by default
Disable random password generation by default
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Defines the default state of "Generate random password for account" setting.

If you enable this setting, the "Generate random password for account" setting will be unchecked by default while you create a new user or edit user settings.

If you disable this setting or do not configure it, the "Generate random password for account" setting will be checked by default while you create a new user or edit user settings.

This setting is designed to let administrators disable random password generation by default for the new user.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
DisableRandomPassword:

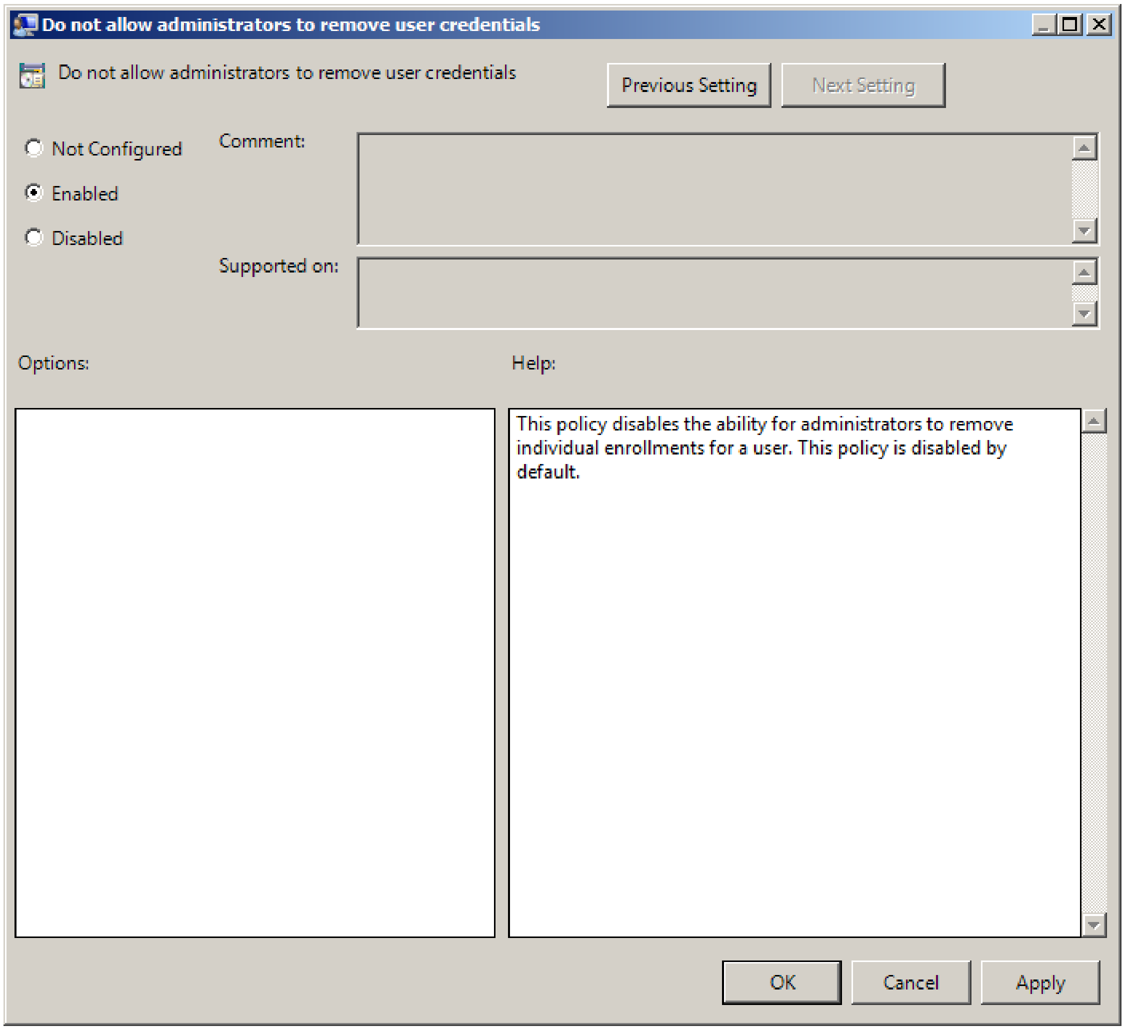
- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

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.



Do not allow administrators to remove user credentials

Do not allow administrators to remove user credentials

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Help:

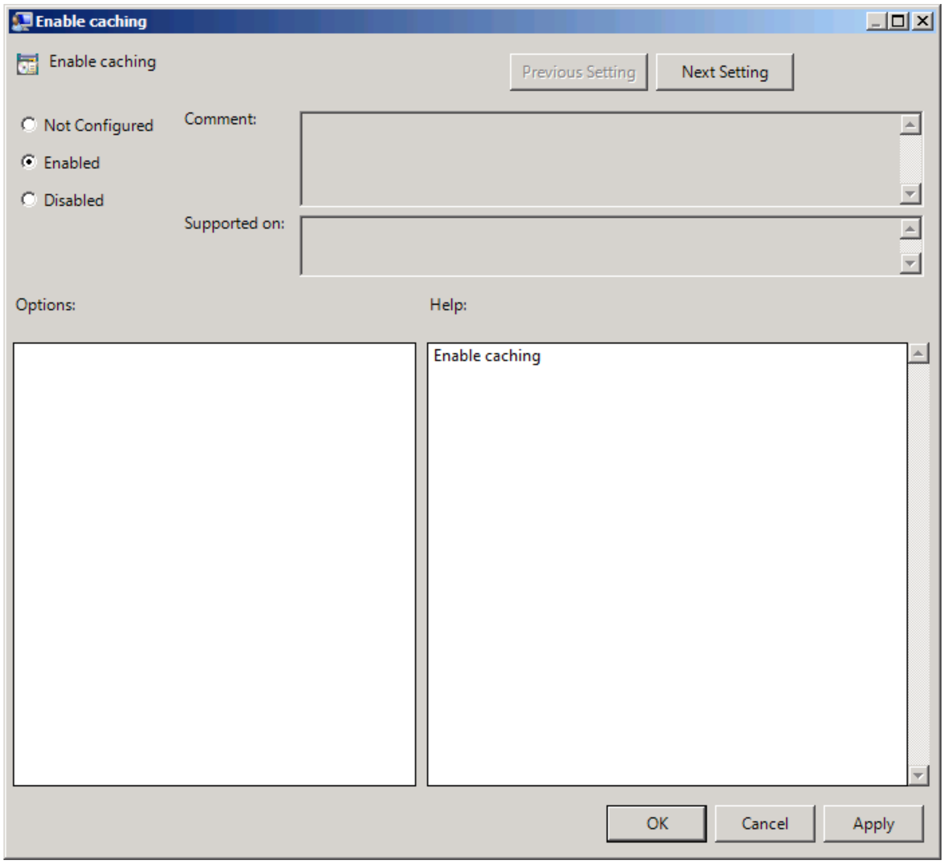
This policy disables the ability for administrators to remove individual enrollments for a user. This policy is disabled by default.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
DisableRemoveTemplatesByAdmin:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.

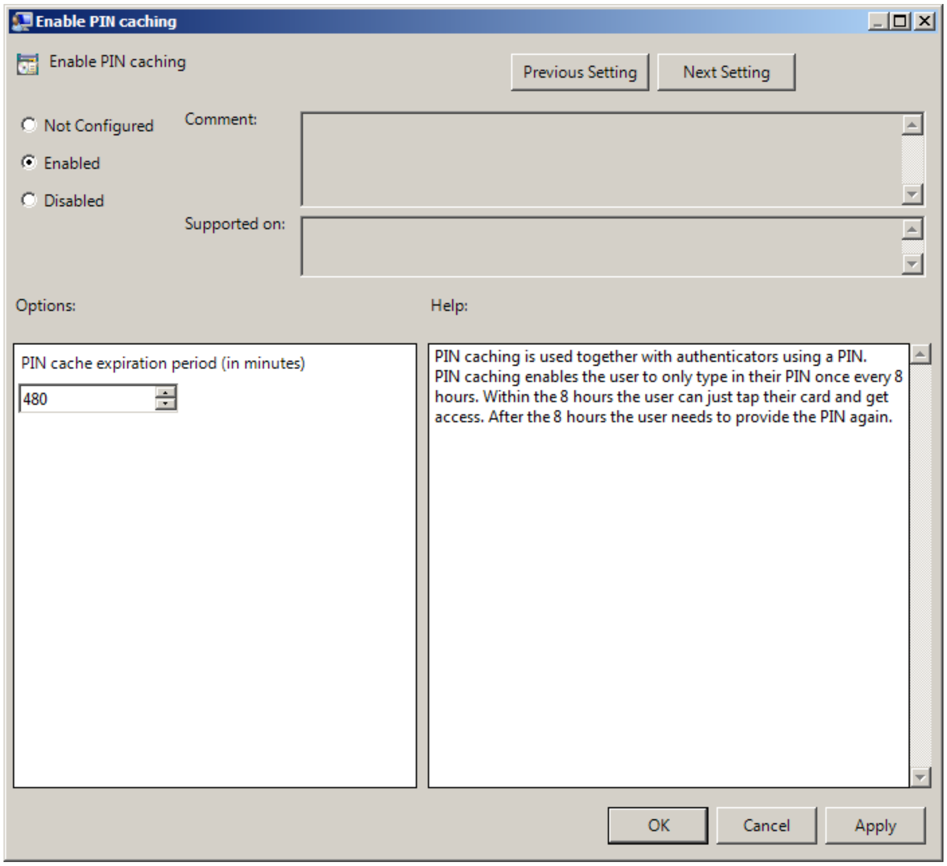
The changes take effect only after group policy refresh.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
IsCacheEnabled:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.



Enable PIN caching

○ Not Configured
● Enabled
○ Disabled

PIN cache expiration period (in minutes)
480

PIN caching is used together with authenticators using a PIN. PIN caching enables the user to only type in their PIN once every 8 hours. Within the 8 hours the user can just tap their card and get access. After the 8 hours the user needs to provide the PIN again.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
LastLogonDBEnabled:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

LastLogonDBExpirePeriod:

- type: REG_DWORD
- value: 0x000001e0 (480)
- description: 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.

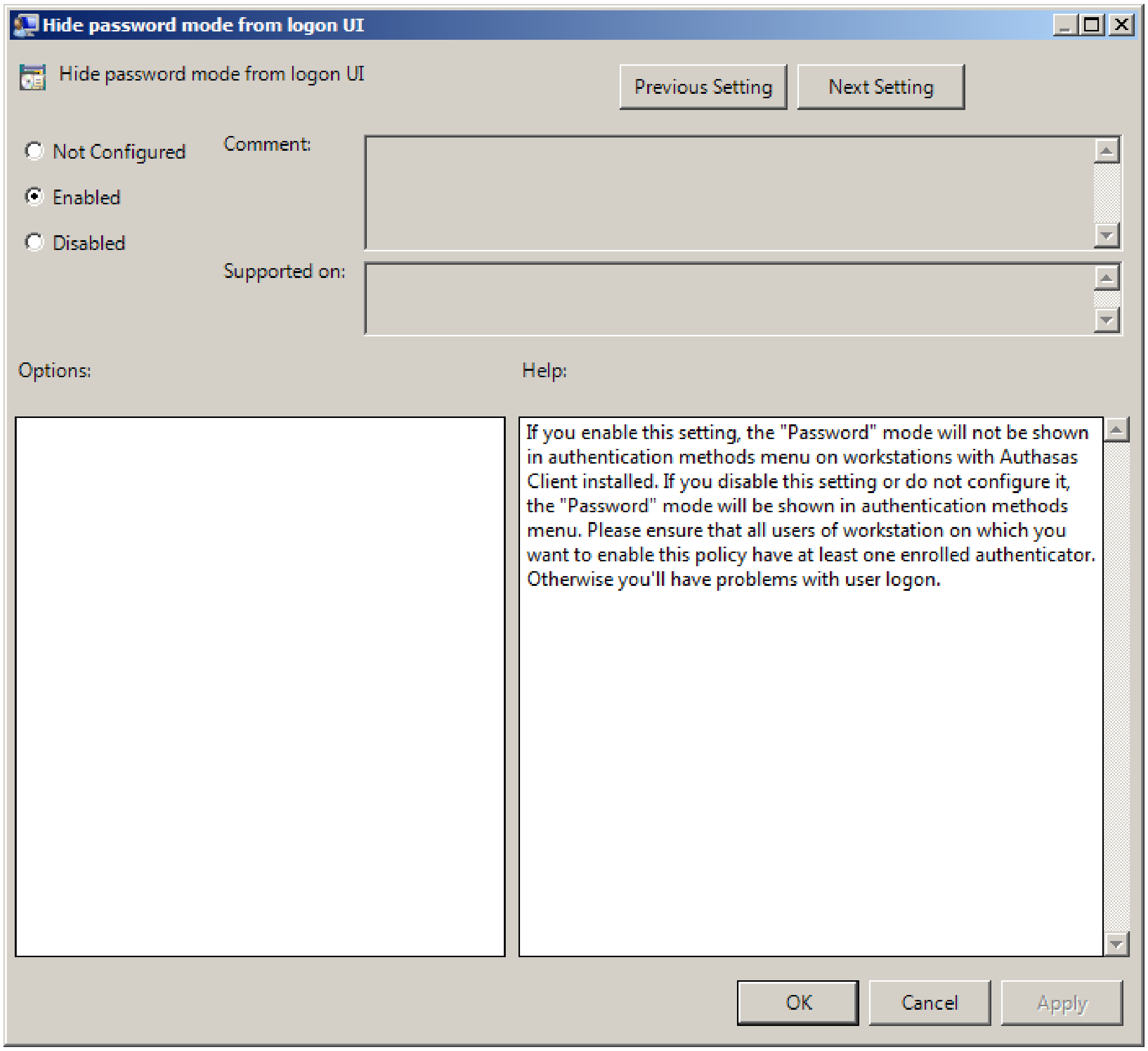
PIN caching is updated:

- once per 5 minutes in the background in case Authenticore Server and Client are within one AD site;
- once per 60 minutes in the background in case Authenticore Server and Client are not within one AD site.

It may be required to enter PIN/password once again during cache synchronization 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.



If you enable this setting, the "Password" mode will not be shown in authentication methods menu on workstations with Authasas Client installed. If you disable this setting or do not configure it, the "Password" mode will be shown in authentication methods menu. Please ensure that all users of workstation on which you want to enable this policy have at least one enrolled authenticator. Otherwise you'll have problems with user logon.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
HidePasswordMode:

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

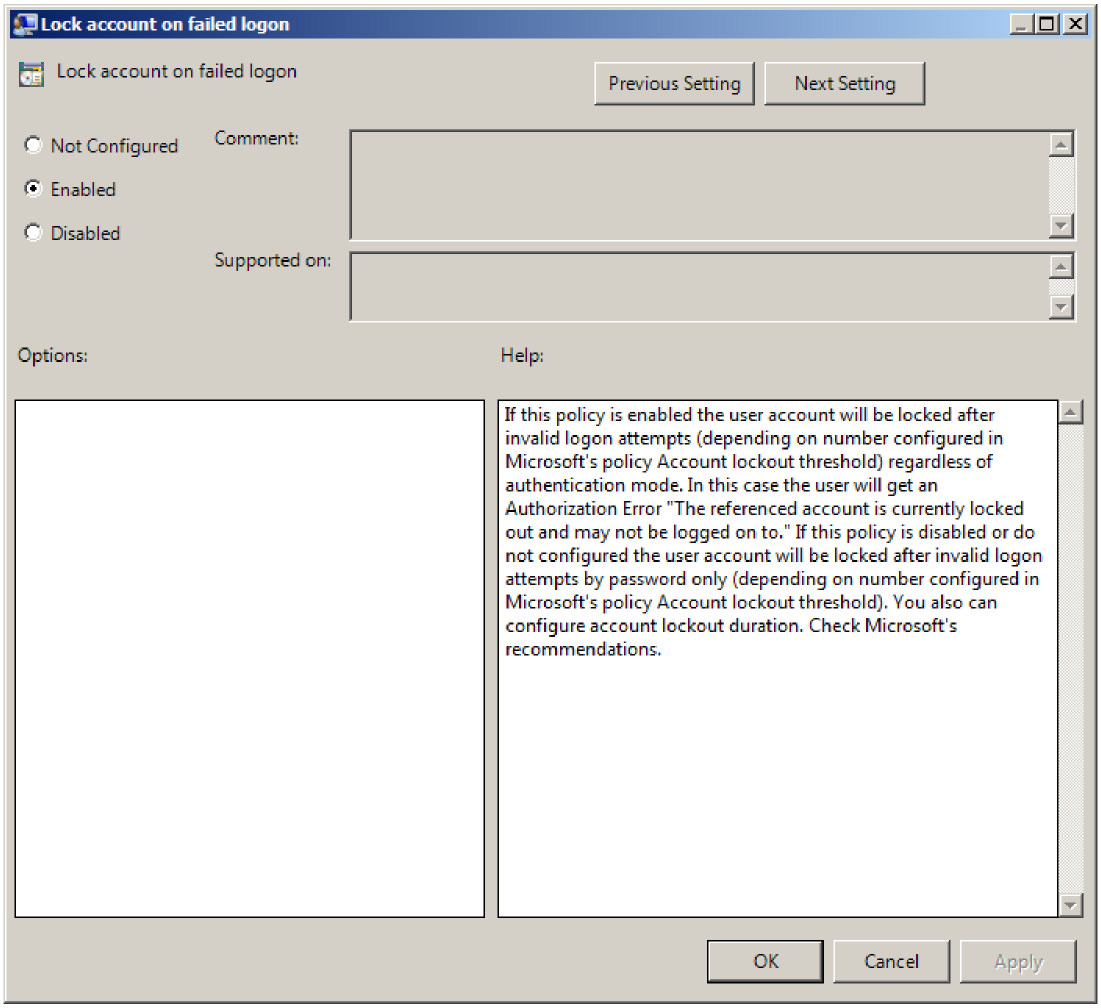
Ensure that all users of workstation on which you want to enable this policy have at least one enrolled authenticator. Otherwise, you will have problems with user logon.

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 the 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 the Account lockout threshold policy).

You also can configure Account lockout duration.



Lock account on failed logon

○ Not Configured
● Enabled
○ Disabled

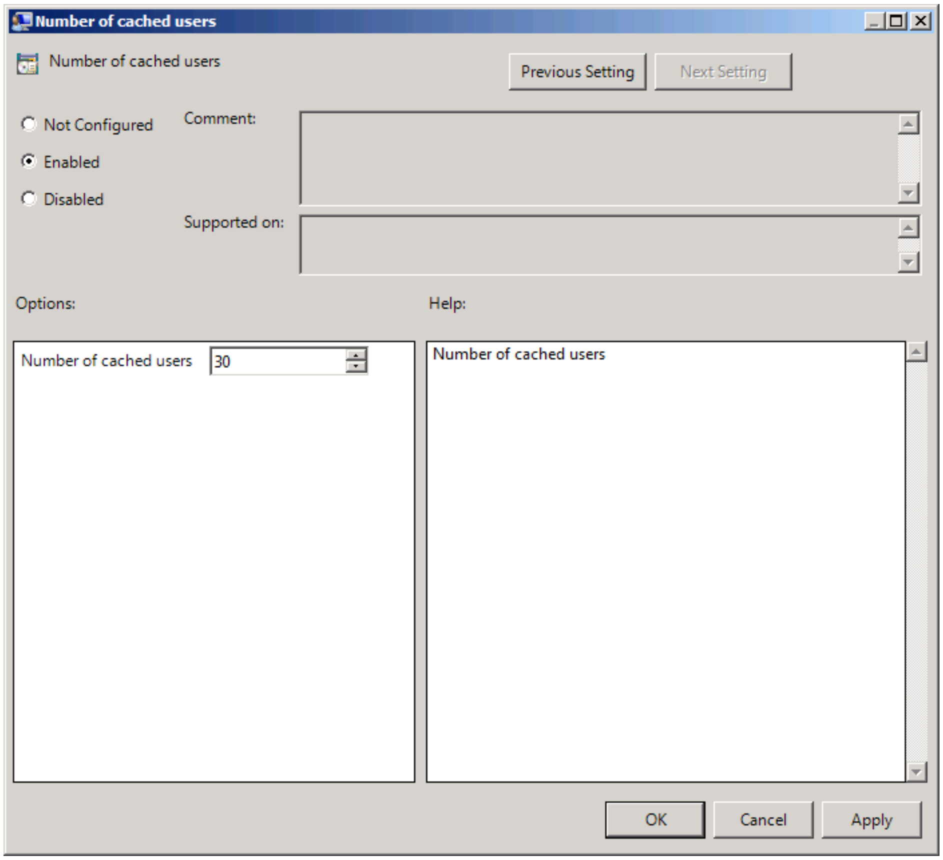
If this policy is enabled the user account will be locked after invalid logon attempts (depending on number configured in Microsoft's policy Account lockout threshold) regardless of authentication mode. In this case the user will get an Authorization Error "The referenced account is currently locked out and may not be logged on to." If this policy is disabled or do not configured the user account will be locked after invalid logon attempts by password only (depending on number configured in Microsoft's policy Account lockout threshold). You also can configure account lockout duration. Check Microsoft's recommendations.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
LockAccountOnFailedLogon:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.


Number of cached users

Number of cached users

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Number of cached users 30

Help:

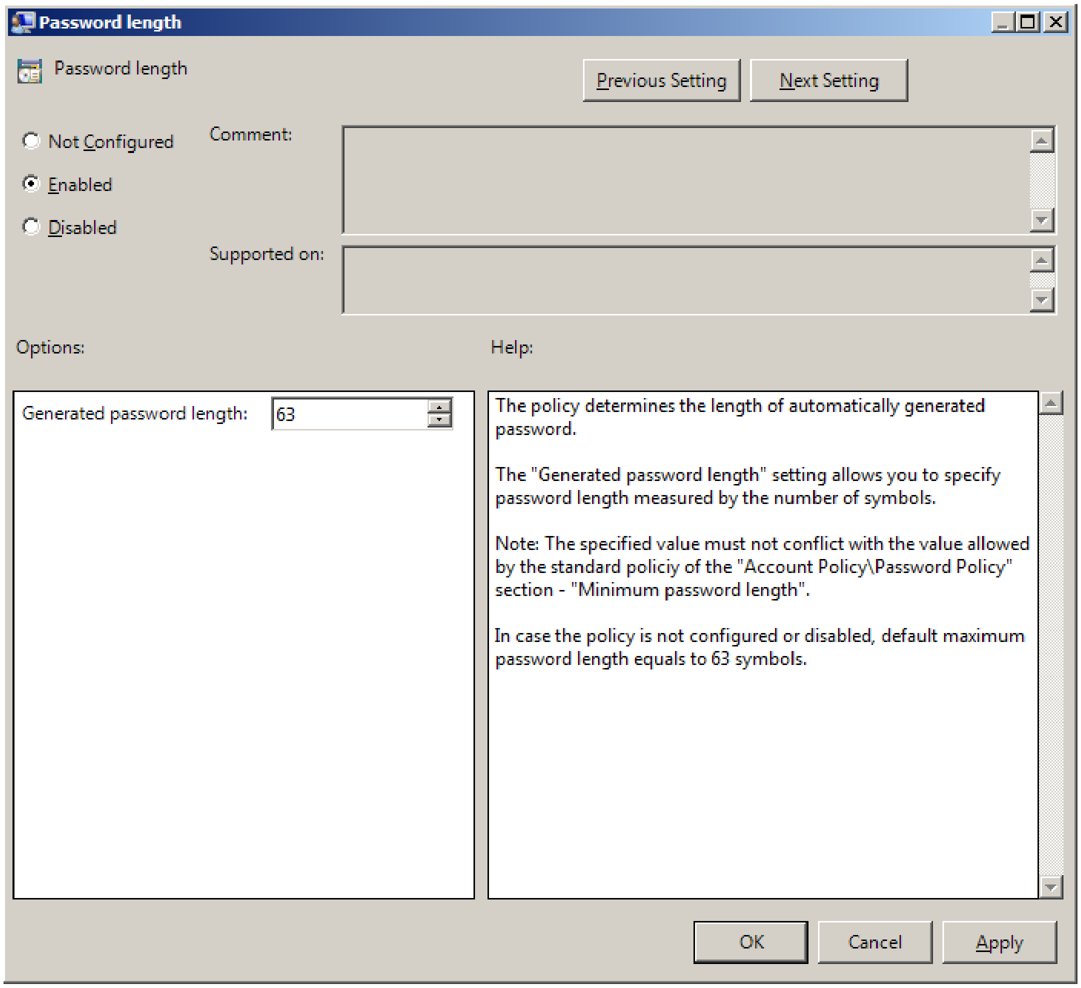
Number of cached users

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
NumberOfCachedUsers:

- type: REG_DWORD
- value: 0x0000001e (30)
- description: 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.



Password length

○ Not Configured

● Enabled

○ Disabled

Generated password length: 63

The policy determines the length of automatically generated password.

The "Generated password length" setting allows you to specify password length measured by the number of symbols.

Note: The specified value must not conflict with the value allowed by the standard policiy of the "Account Policy\Password Policy" section - "Minimum password length".

In case the policy is not configured or disabled, default maximum password length equals to 63 symbols.

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
GeneratePasswordLength:

- type: REG_DWORD
- value: 0x0000003f (63)
- description: 63 displays the generated password length

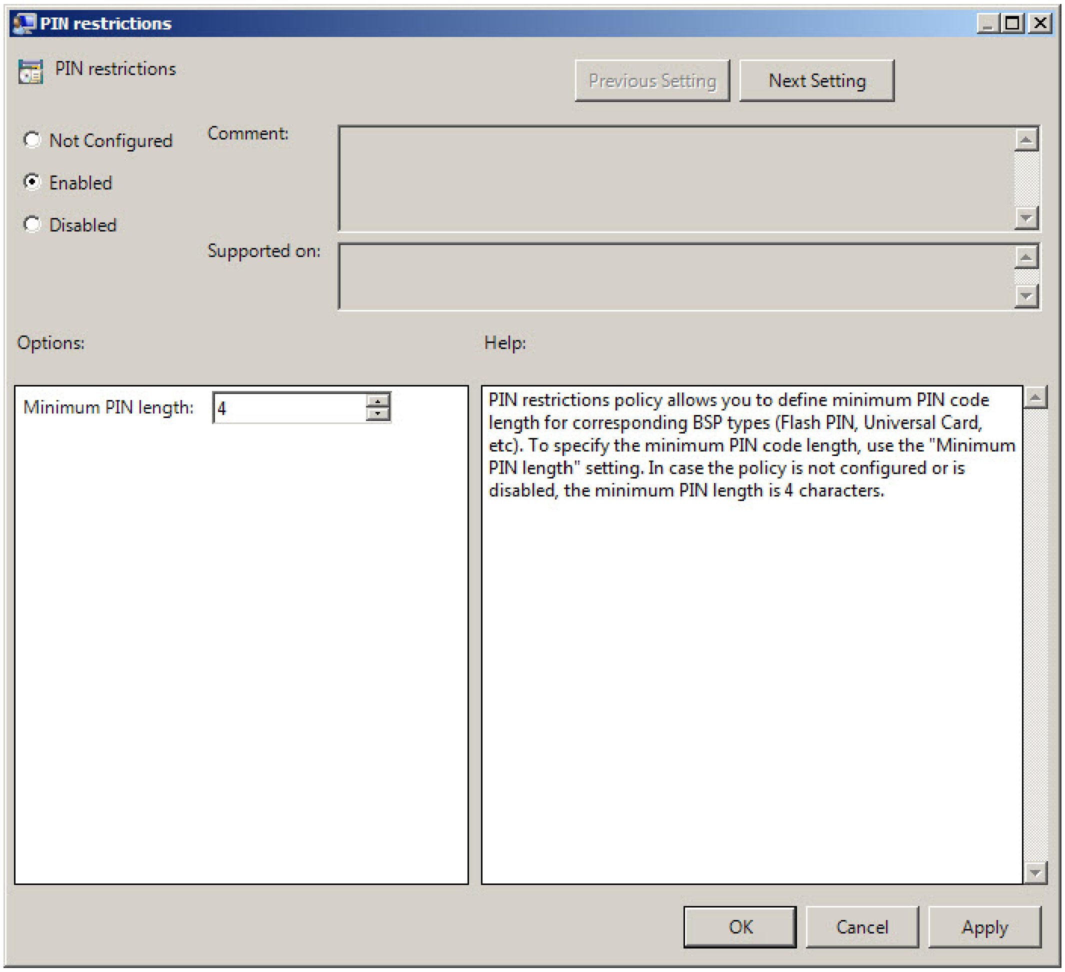
The specified value and the frequency of passwords change must not conflict with the values defined by the standard policies of the Account Policy/Password Policy section:

- 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).



PIN restrictions

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Minimum PIN length: 4

Help:

PIN restrictions policy allows you to define minimum PIN code length for corresponding BSP types (Flash PIN, Universal Card, etc). To specify the minimum PIN code length, use the "Minimum PIN length" setting. In case the policy is not configured or is disabled, the minimum PIN length is 4 characters.

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

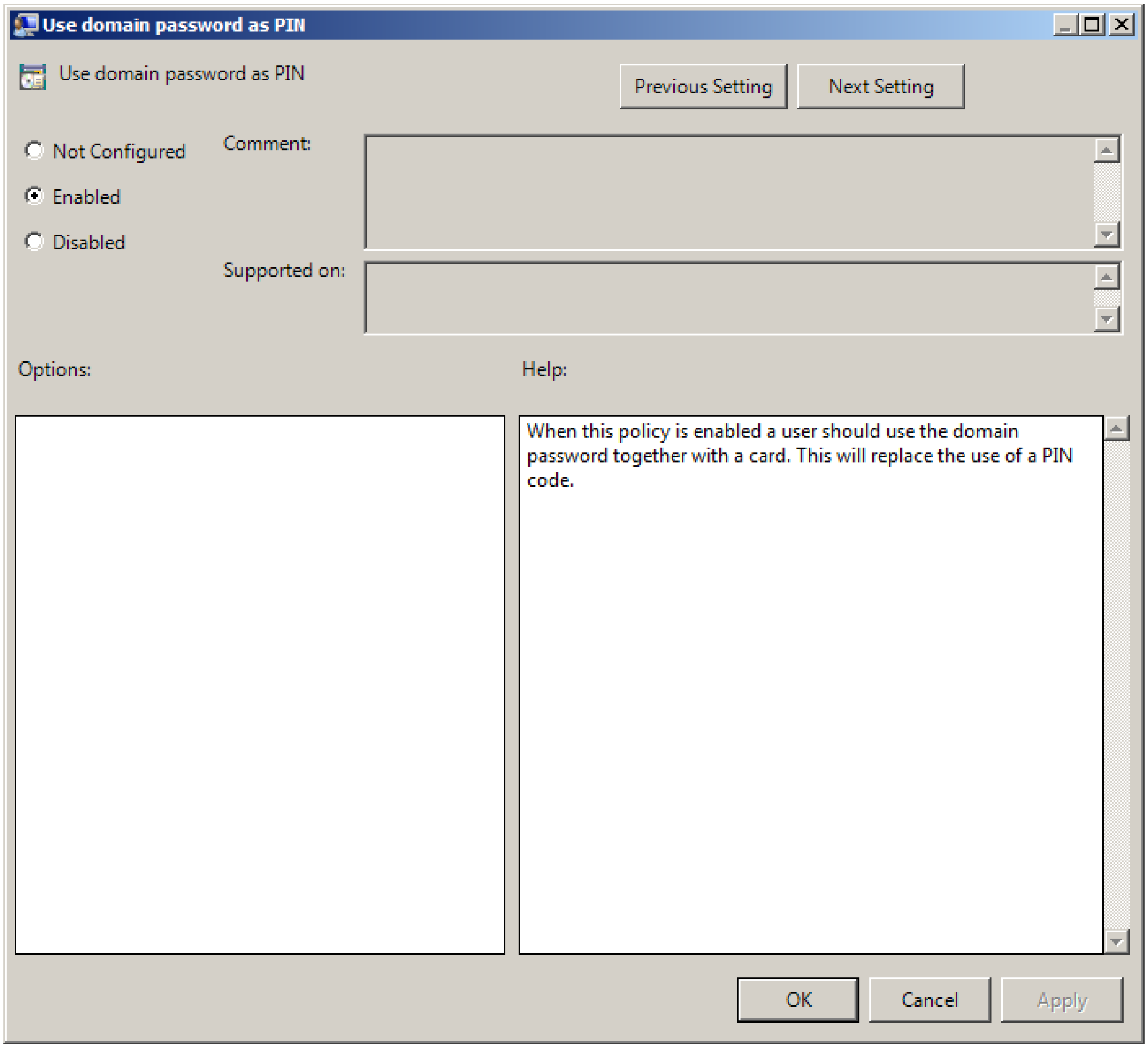
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\BSP\PINRestrictions
MinLength:

- type: REG_DWORD
- value: 0x00000004 (4)
- description: 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.



Use domain password as PIN

○ Not Configured
● Enabled
○ Disabled

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.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
DomainPasswordAsPin:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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

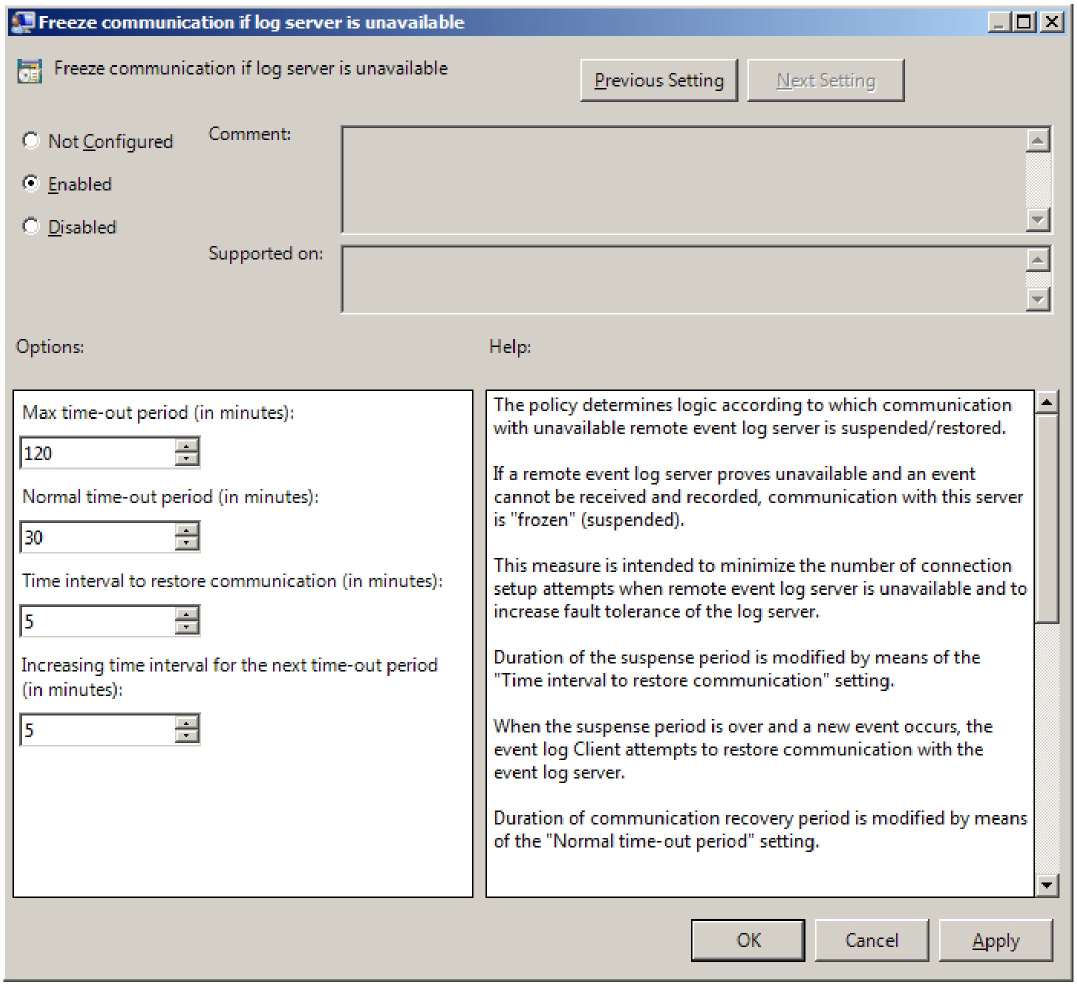
The **Event Log** section includes policies allowing you to determine logging settings.

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.



Freeze communication if log server is unavailable
Freeze communication if log server is unavailable
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Max time-out period (in minutes): 120

Normal time-out period (in minutes): 30

Time interval to restore communication (in minutes): 5

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

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

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

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

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

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

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

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
MaxTimeoutPeriod:

- type: REG_DWORD
- value: 0x00000078 (120)
- description: 120 displays the max time-out period (in minutes)

ReconnectPause:

- type: REG_DWORD
- value: 0x00000005 (5)
- description: 5 displays time interval to restore communication (in minutes)

ReconnectPauseIncrement:

- type: REG_DWORD
- value: 0x00000005 (5)
- description: 5 displays increasing time interval for the next time-out period (in minutes)

TimeoutPeriod:

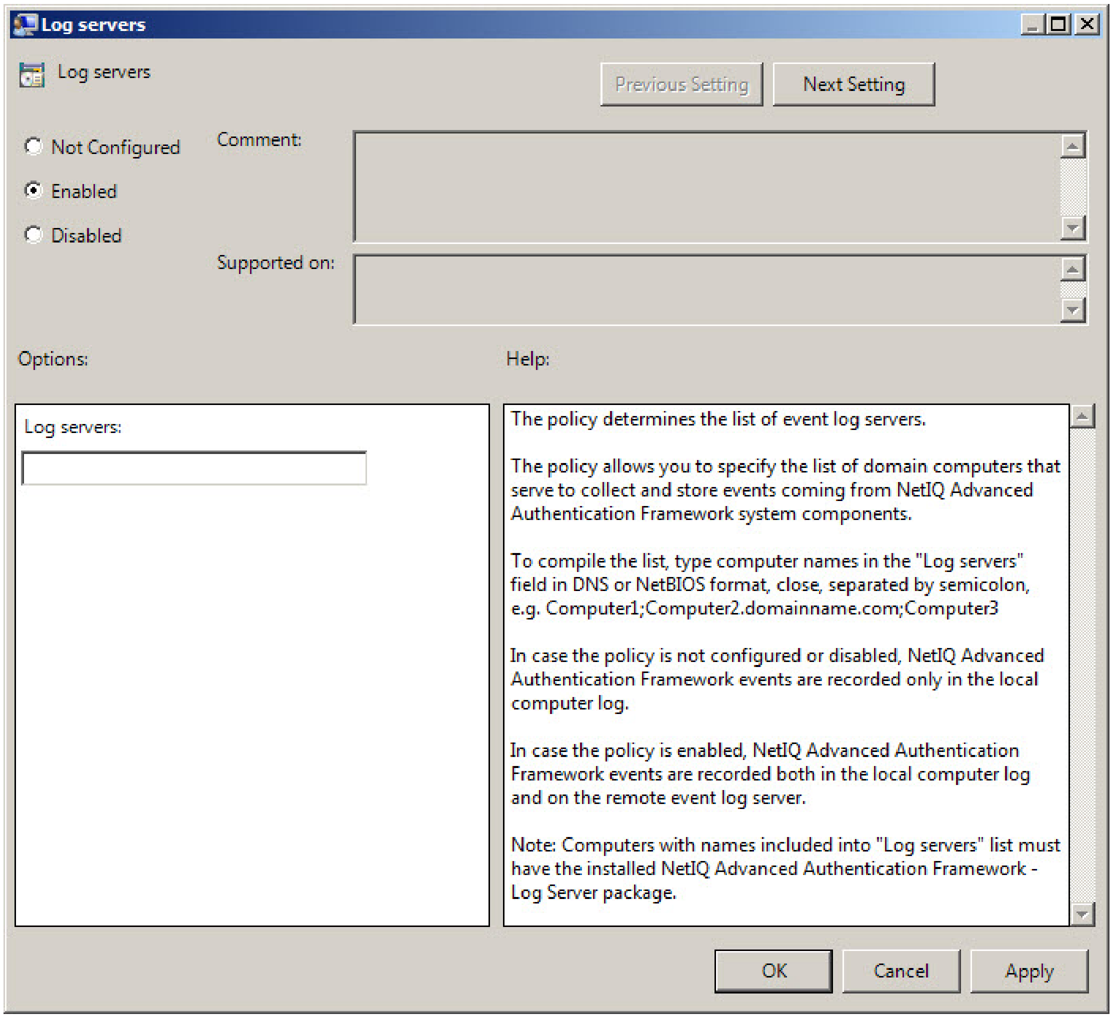
- type: REG_DWORD
- value: 0x0000001e (30)
- description: 30 displays normal time-out period (in minutes)

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.



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Log servers:

Help:

The policy determines the list of event log servers.

The policy allows you to specify the list of domain computers that serve to collect and store events coming from NetIQ Advanced Authentication Framework system components.

To compile the list, type computer names in the "Log servers" field in DNS or NetBIOS format, close, separated by semicolon, e.g. Computer1;Computer2.domainname.com;Computer3

In case the policy is not configured or disabled, NetIQ Advanced Authentication Framework events are recorded only in the local computer log.

In case the policy is enabled, NetIQ Advanced Authentication Framework events are recorded both in the local computer log and on the remote event log server.

Note: Computers with names included into "Log servers" list must have the installed NetIQ Advanced Authentication Framework - Log Server package.

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
Logging Servers:

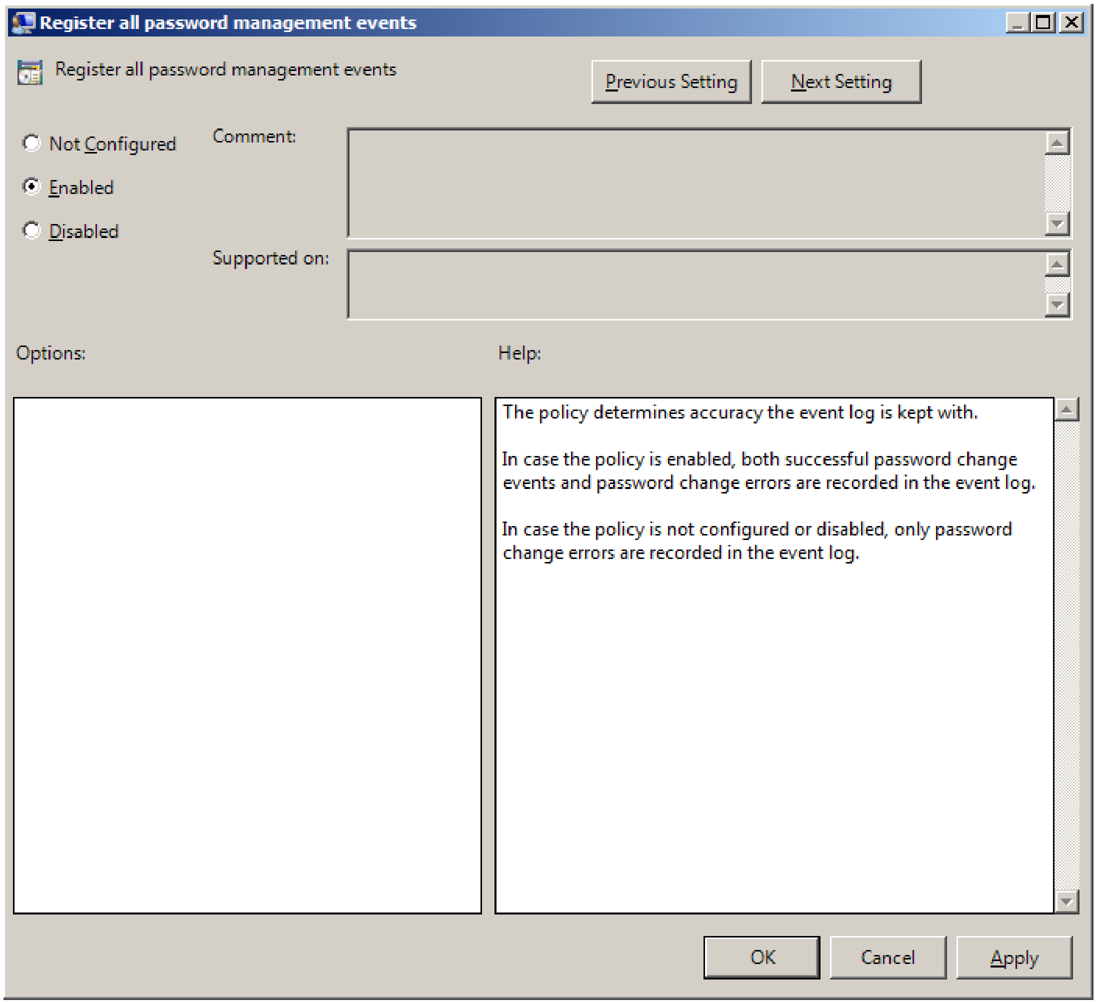
- type: REG_SZ
- value: Computer1, Computer2, Computer3
- description: Computer1, Computer2, Computer3 is the list of the defined log servers

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.



Register all password management events

Register all password management events

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Help:

The policy determines accuracy the event log is kept with.

In case the policy is enabled, both successful password change events and password change errors are recorded in the event log.

In case the policy is not configured or disabled, only password change errors are recorded in the event log.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
PasswordManagement_AllEvents:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

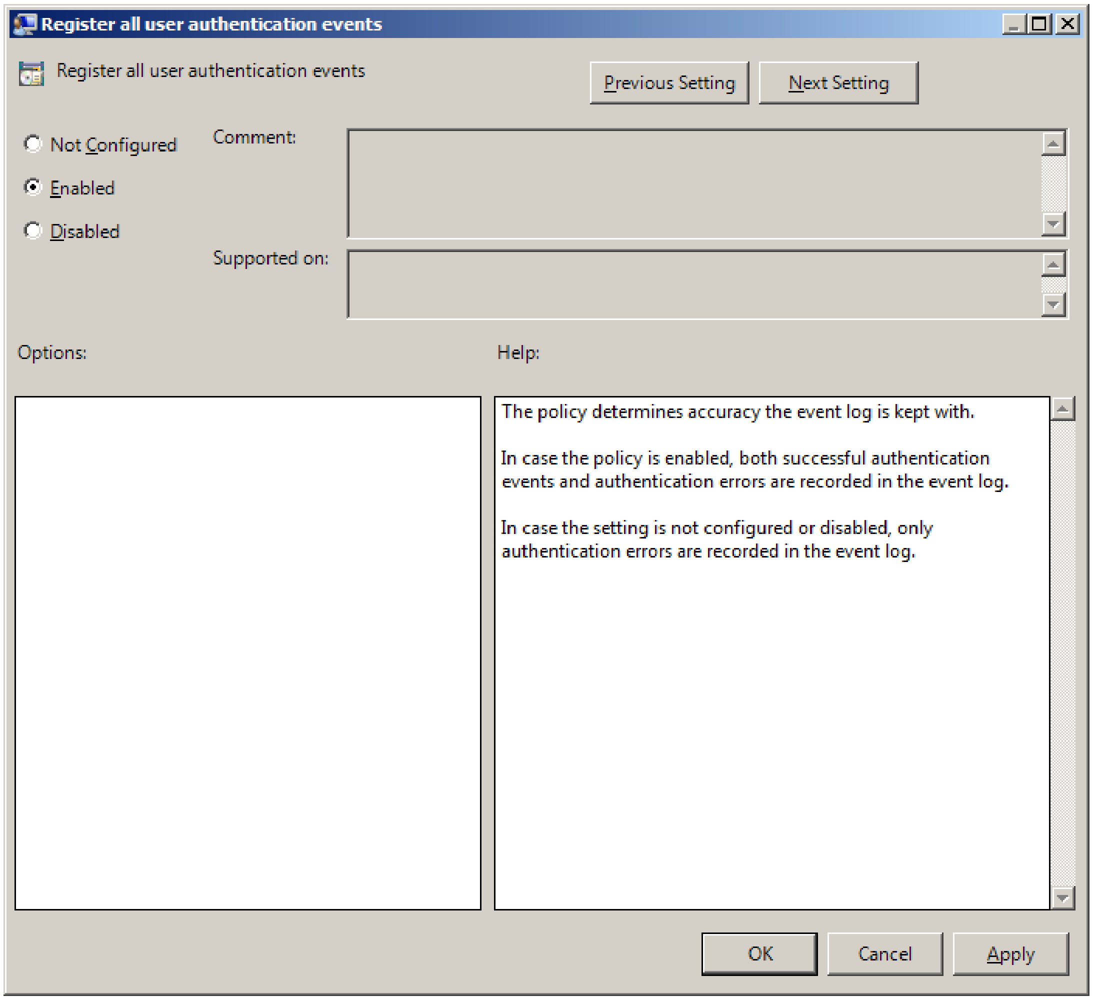
The policy requires the pre-installed Password Filter. Otherwise the policy will not work.

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.



Register all user authentication events

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

The policy determines accuracy the event log is kept with.

In case the policy is enabled, both successful authentication events and authentication errors are recorded in the event log.

In case the setting is not configured or disabled, only authentication errors are recorded in the event log.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
UserAuthentication_AllEvents:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.

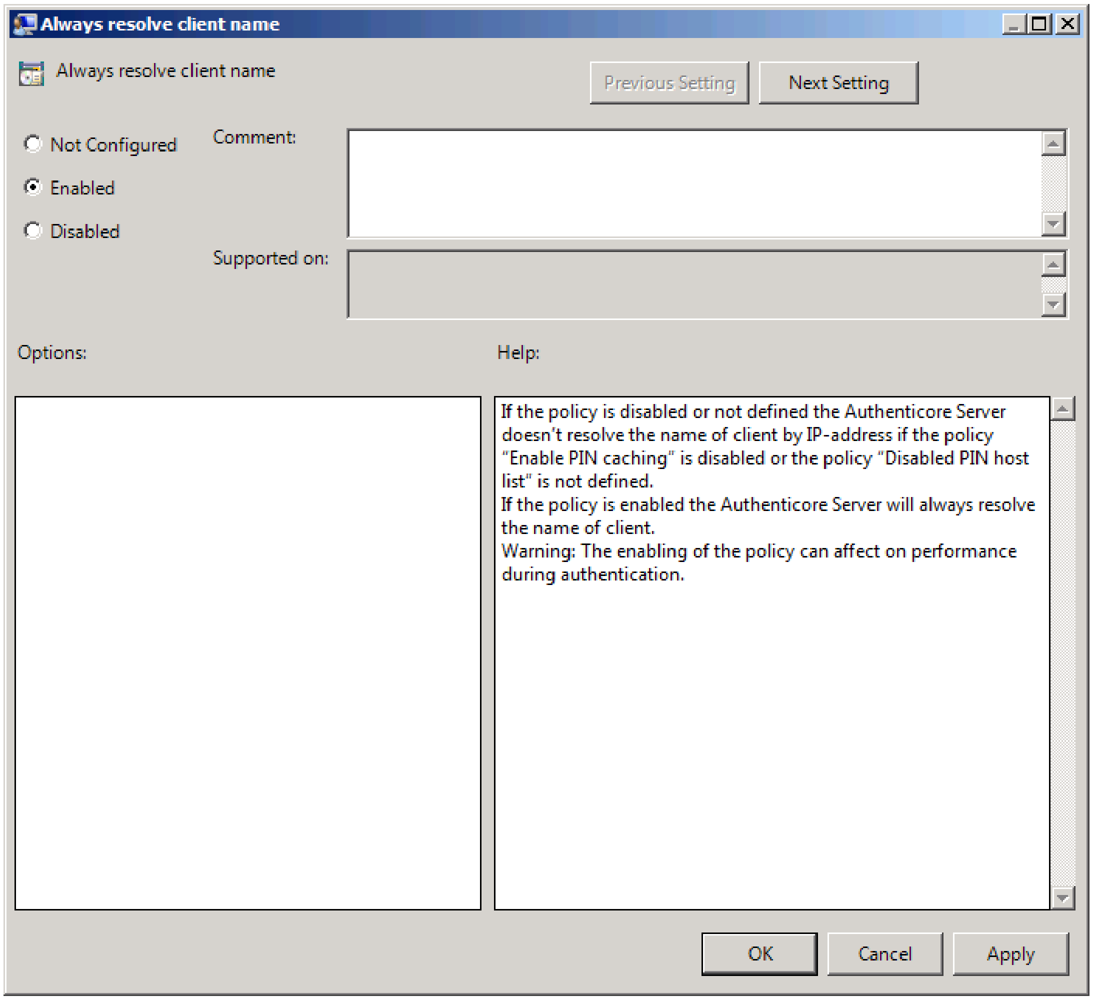
It includes:

- Always resolve client name
- Enable 802.11 pre logon authentication
- 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.



Always resolve client name

○ Not Configured

● Enabled

○ Disabled

If the policy is disabled or not defined the Authenticore Server doesn't resolve the name of client by IP-address if the policy "Enable PIN caching" is disabled or the policy "Disabled PIN host list" is not defined.
If the policy is enabled the Authenticore Server will always resolve the name of client.
Warning: The enabling of the policy can affect on performance during authentication.

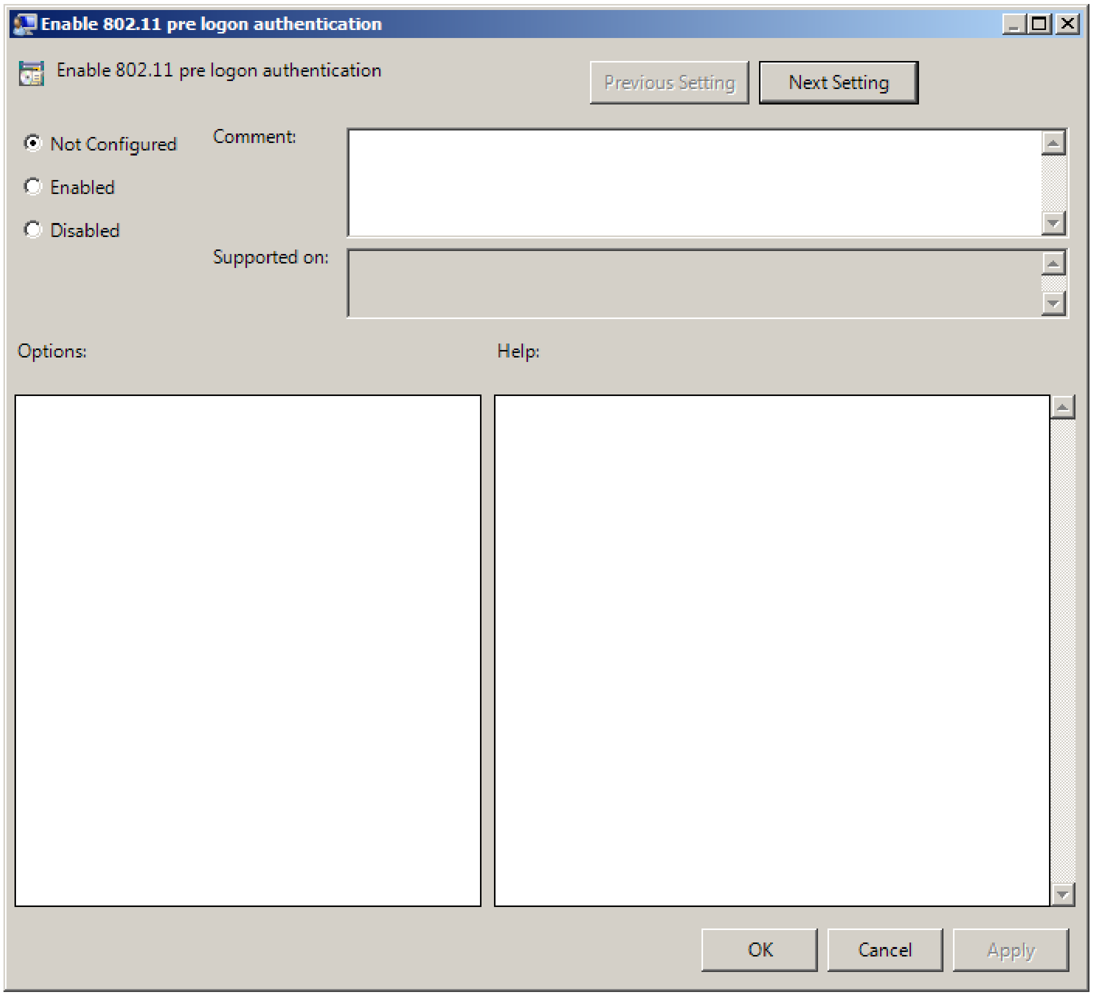
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
AlwaysResolveClientName:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

⚠ Enabling of the policy can affect the performance during authentication.

Enable 802.11 pre logon authentication

The **Enable 802.11 pre logon authentication** policy allows you to enable the detection of network connections during logon. It should be enabled in case EAP is used during logon.



Enable 802.11 pre logon authentication

● Not Configured

○ Enabled

○ Disabled

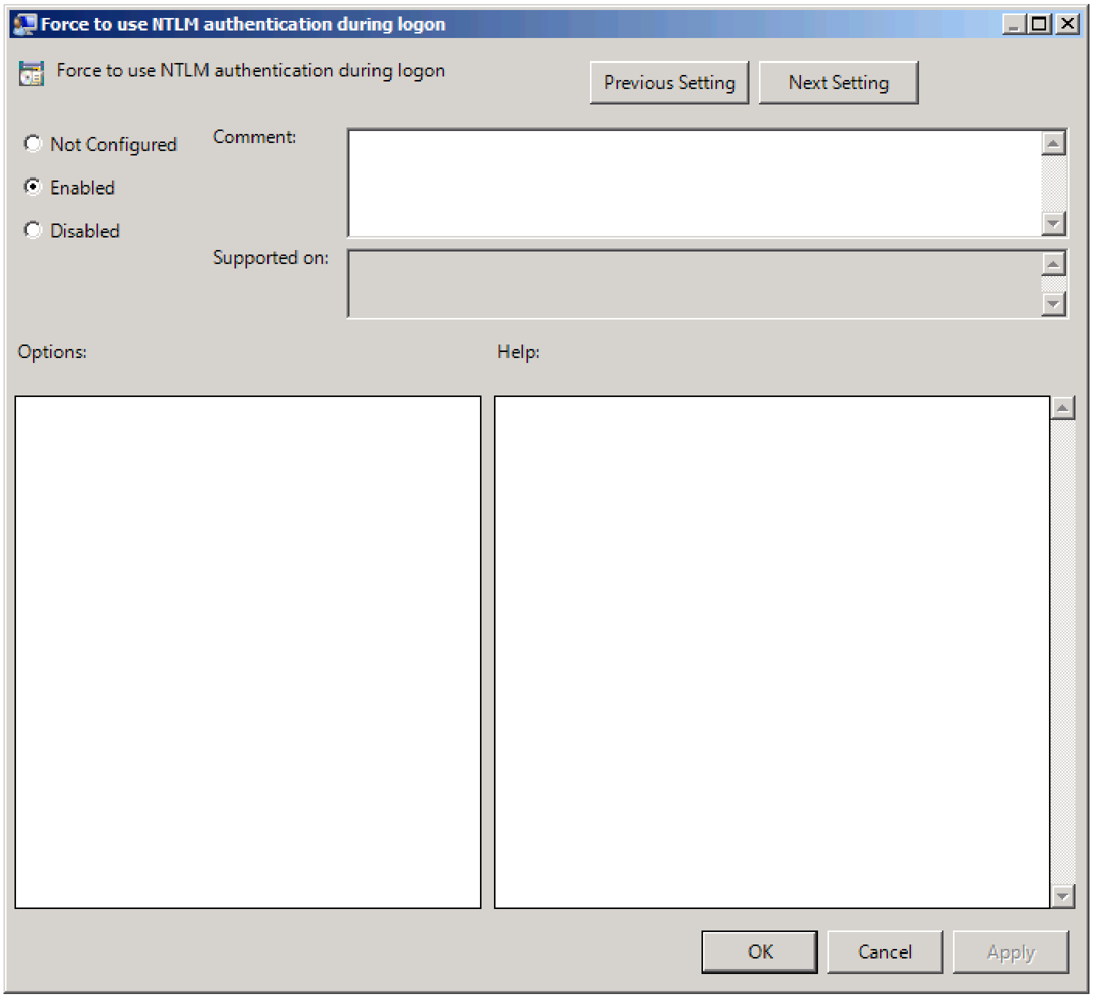
HKEY_ LOCAL_ MACHINE\SOFTWARE\ (Wow6432Node\) Policies\ NetIQ \ NetIQ Advanced Authentication Framework

802X1Enabled:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

Force to use NTLM authentication during logon

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



Force to use NTLM authentication during logon

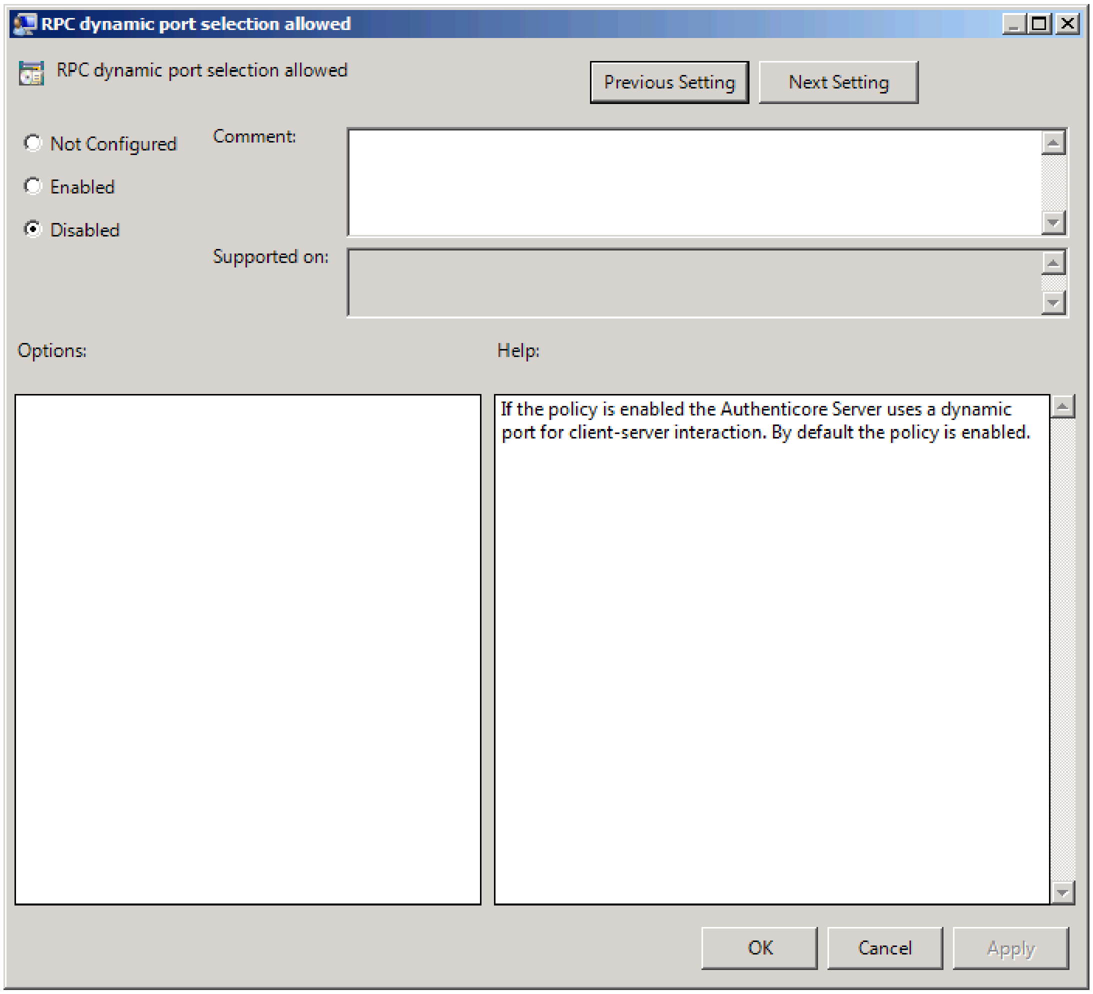
○ Not Configured
● Enabled
○ Disabled

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
RpcForceNtlmAtLogon:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.



○ Not Configured
○ Enabled
● Disabled

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

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
RpcDynamicPortAllowed:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

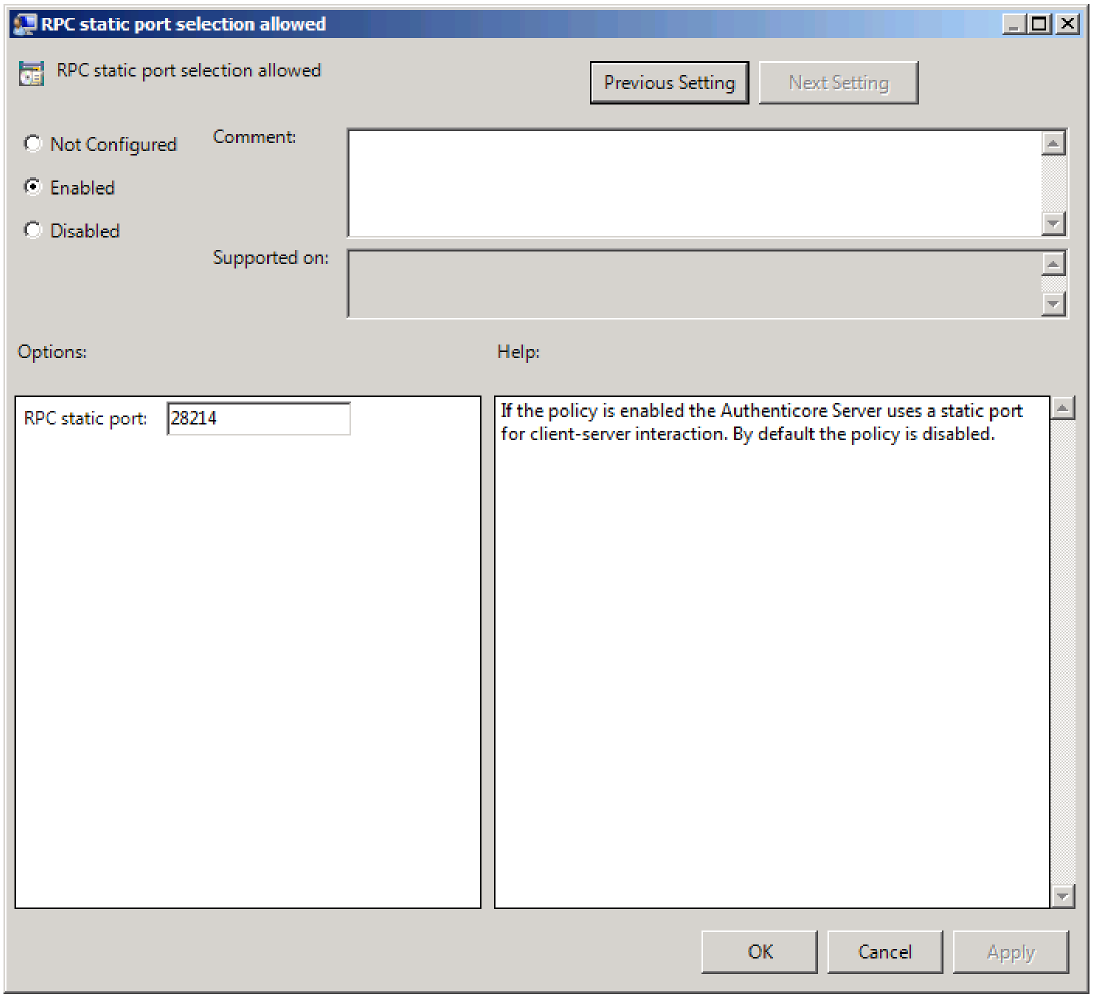
If both **RPC dynamic port selection allowed** and **RPC static port selection allowed** policies are enabled then:

- 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.



RPC static port selection allowed

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

RPC static port: 28214

Help:

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

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
RpcStaticPort:

- type: REG_DWORD
- value: 0x00006e36 (28214)

- description: 28214 is the port number in case of using static port for client-server interaction (the default port number is 28214)

RpcStaticPortAllowed:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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

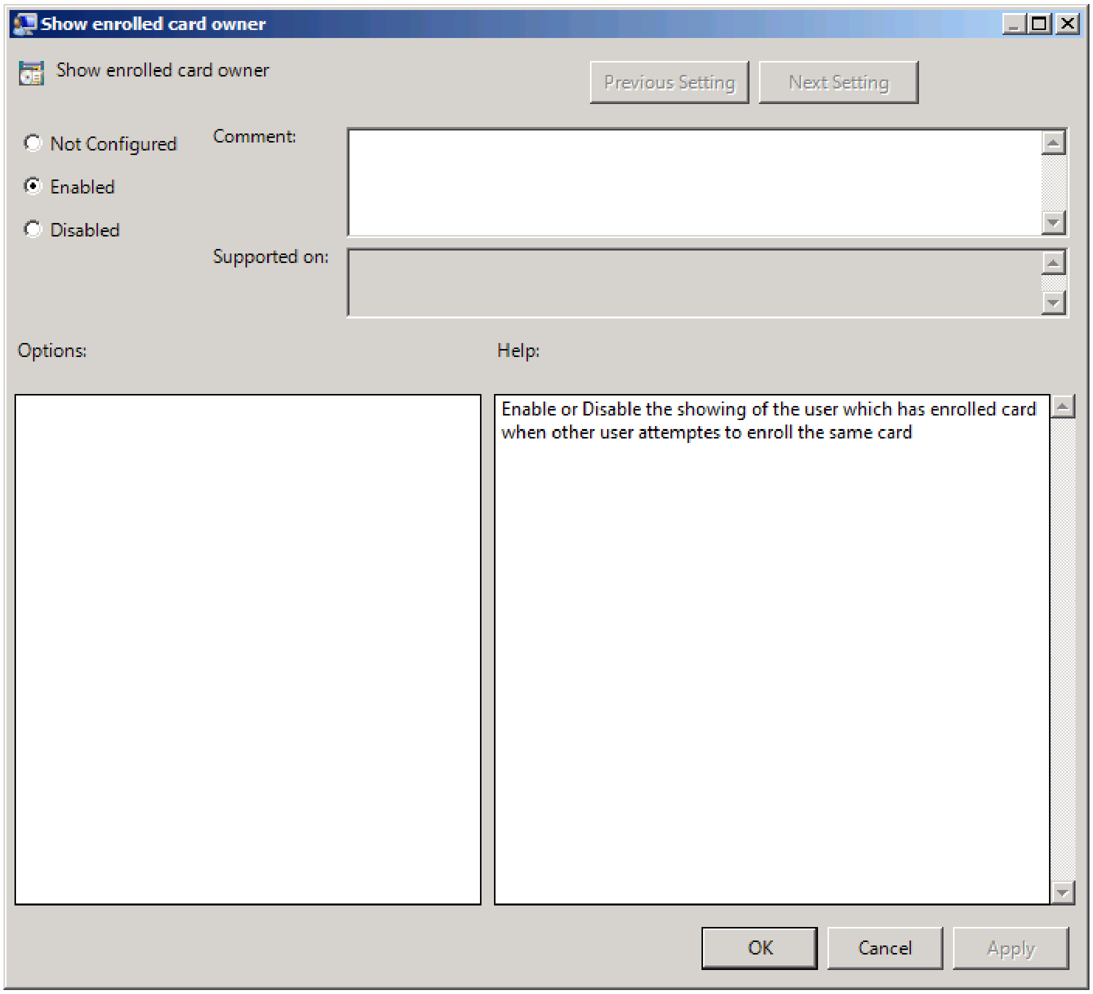
The **Runtime Environment** section includes a policy allowing to enable or disable showing of the user who has enrolled card.

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.



○ Not Configured
● Enabled
○ Disabled

Enable or Disable the showing of the user which has enrolled card when other user attemptes to enroll the same card

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

RTEShowEnrolledCardOwner:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

Users and Groups

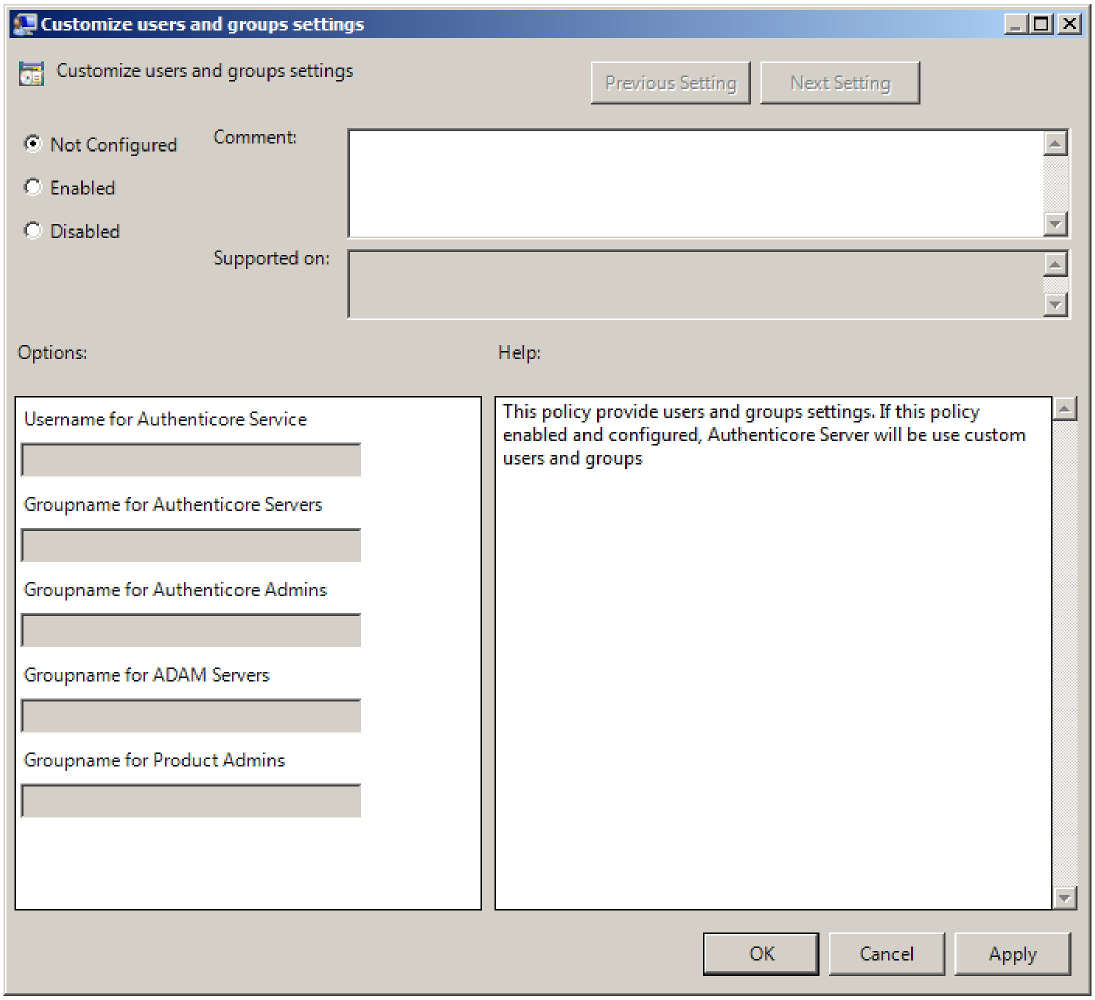
The **Users and Groups** section includes a policy allowing to specify users and groups settings manually.

It includes:

- Customize users and groups settings

Customize Users and Group Settings

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



Customize users and groups settings
Customize users and groups settings
Previous Setting
Next Setting
● Not Configured
○ Enabled
○ Disabled
Comment:
Supported on:
Options:
Help:
Username for Authenticore Service
Groupname for Authenticore Servers
Groupname for Authenticore Admins
Groupname for ADAM Servers
Groupname for Product Admins
OK
Cancel
Apply

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

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

ADAMServersGroups:

- type: REG_SZ
- value: NetIQ Advanced Authentication Framework ADAM Servers
- description: NetIQ Advanced Authentication Framework ADAM Servers displays the specified groupname for ADAM Servers

AuthenticoreAdminsGroup:

- type: REG_SZ
- value: Authenticore Admins
- description: Authenticore Admins displays the specified groupname for Authenticore Admins

AuthenticoreServersGroup:

- type: REG_SZ
- value: Authenticore Servers
- description: Authenticore Servers displays the specified groupname for Authenticore Servers

AuthenticoreServiceUser:

- type: REG_SZ
- value: AuthenticoreService
- description: AuthenticoreService displays the specified username for Authenticore Service

ProductAdminsGroup:

- type: REG_SZ
- value: NetIQ Advanced Authentication Framework Admins
- description: NetIQ Advanced Authentication Framework Admins displays the specified groupname for Product Admins

UsersAndGroups:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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:

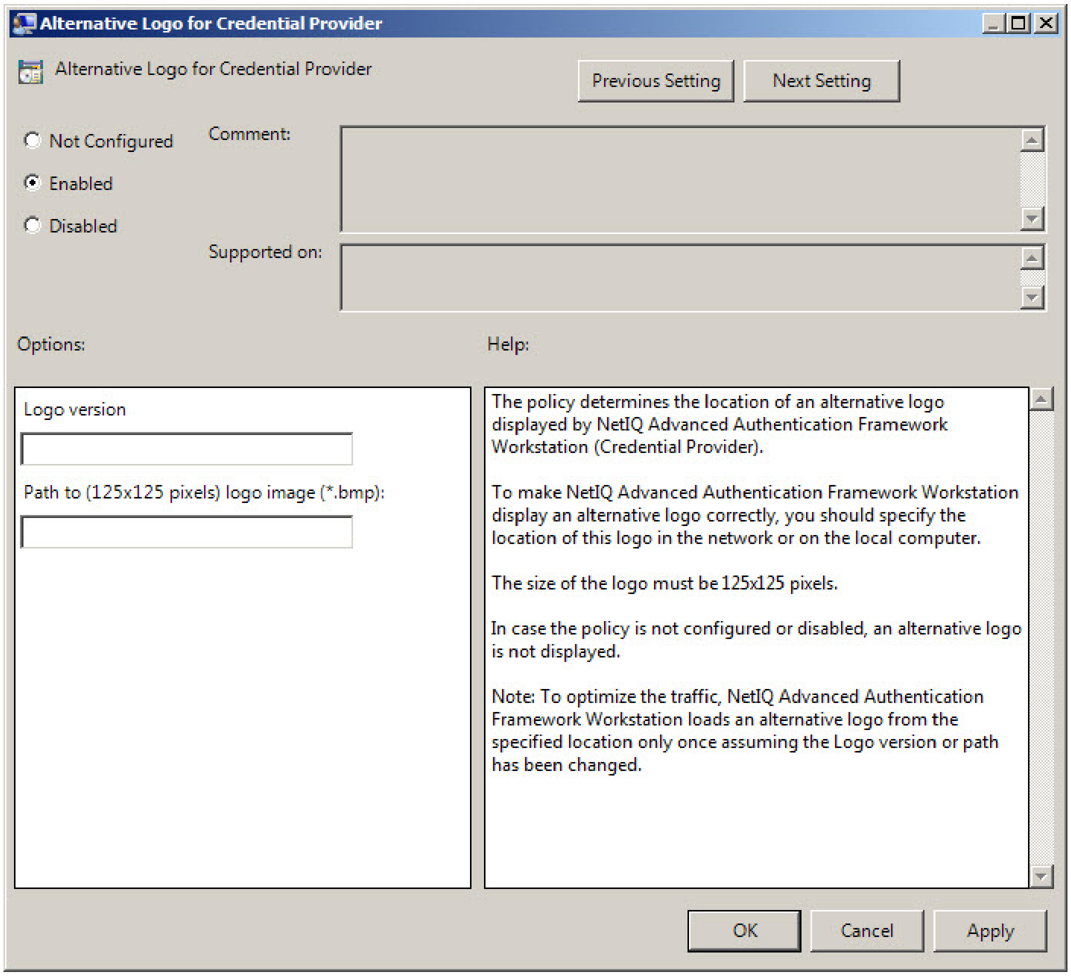
- Alternative Logo for Credential Provider
- Alternative Logo for GINA and Wizard
- Deny to specify authenticator comment at enrollment
- Deny to start Client Tray when user logs on to Windows
- Disable first logon enroll wizard
- Disable "Use Dial-up connection" option
- Do not allow to skip welcome window
- Enable device detection for all
- Enhanced reaction on device events
- Last used server timeout
- 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.

✱ Alternative logo is applied for user selection screen, UAC and all authentication methods except for fingerprint.


Alternative Logo for Credential Provider
Alternative Logo for Credential Provider
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

Logo version

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

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

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

The size of the logo must be 125x125 pixels.

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

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

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

CPLogo:

- type: REG_SZ
- value: 1
- description: 1 displays the configured logo version

CPLogoVersion:

- type: REG_SZ
- value: \\netiq\logos\cplogo.bmp
- description: \\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.

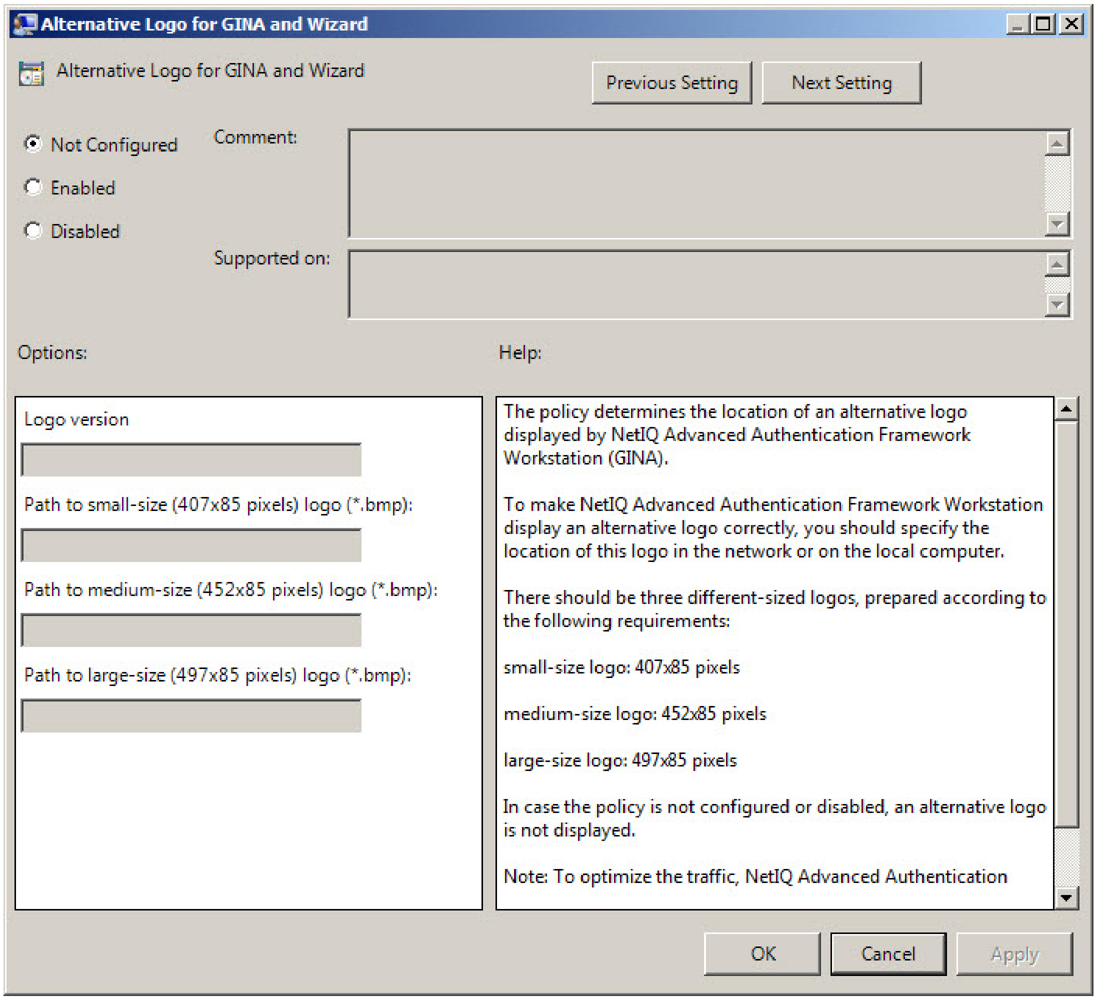
To optimize the traffic, NetIQ Advanced Authentication Framework Client loads an alternative logo from the specified location only once assuming the Logo version or any of the paths have been changed.

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.



● Not Configured
○ Enabled
○ Disabled

Logo version

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

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

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

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

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

LargeLogo:

- type: REG_SZ
- value: \\netiq\logos\cplogolarge.bmp
- description: \\netiq\logos\cplogolarge.bmp displays the path to large-size logo

LogoVersion:

- type: REG_SZ
- value: 1
- description: 1 specifies the configured logo version

MediumLogo:

- type: REG_SZ
- value: \\netiq\logos\cplogomedium.bmp
- description: \\netiq\logos\cplogomedium.bmp displays the path to medium-size logo

SmallLogo:

- type: REG_SZ
- value: \\netiq\logos\cplogosmall.bmp
- description: \\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:

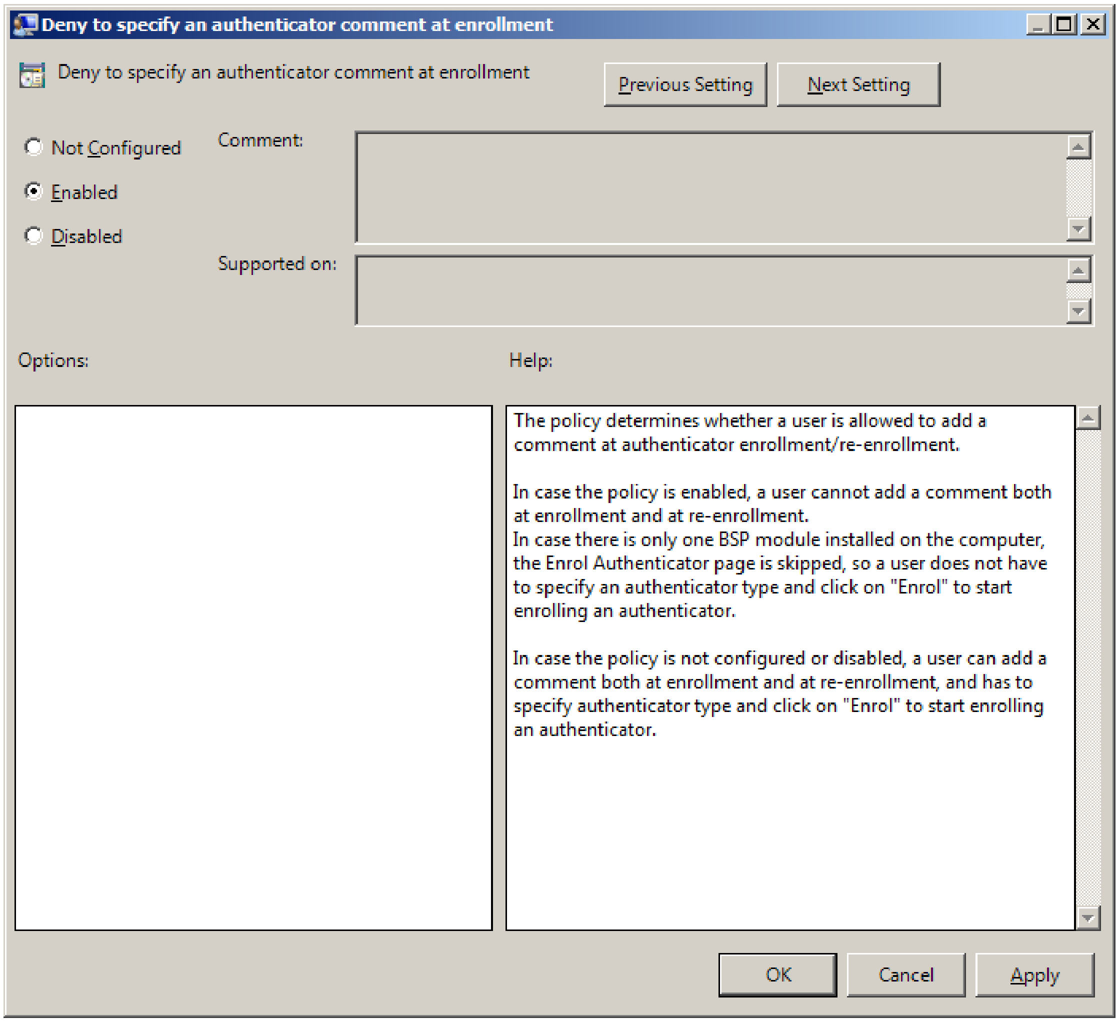
- small-size logo: 406x85 pixels;
- medium-size logo: 451x85 pixels;
- large-size logo: 495x85 pixels.

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.



The policy determines whether a user is allowed to add a comment at authenticator enrollment/re-enrollment.

In case the policy is enabled, a user cannot add a comment both at enrollment and at re-enrollment.
In case there is only one BSP module installed on the computer, the Enrol Authenticator page is skipped, so a user does not have to specify an authenticator type and click on "Enrol" to start enrolling an authenticator.

In case the policy is not configured or disabled, a user can add a comment both at enrollment and at re-enrollment, and has to specify authenticator type and click on "Enrol" to start enrolling an authenticator.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
DenyAuthenticatorComment:

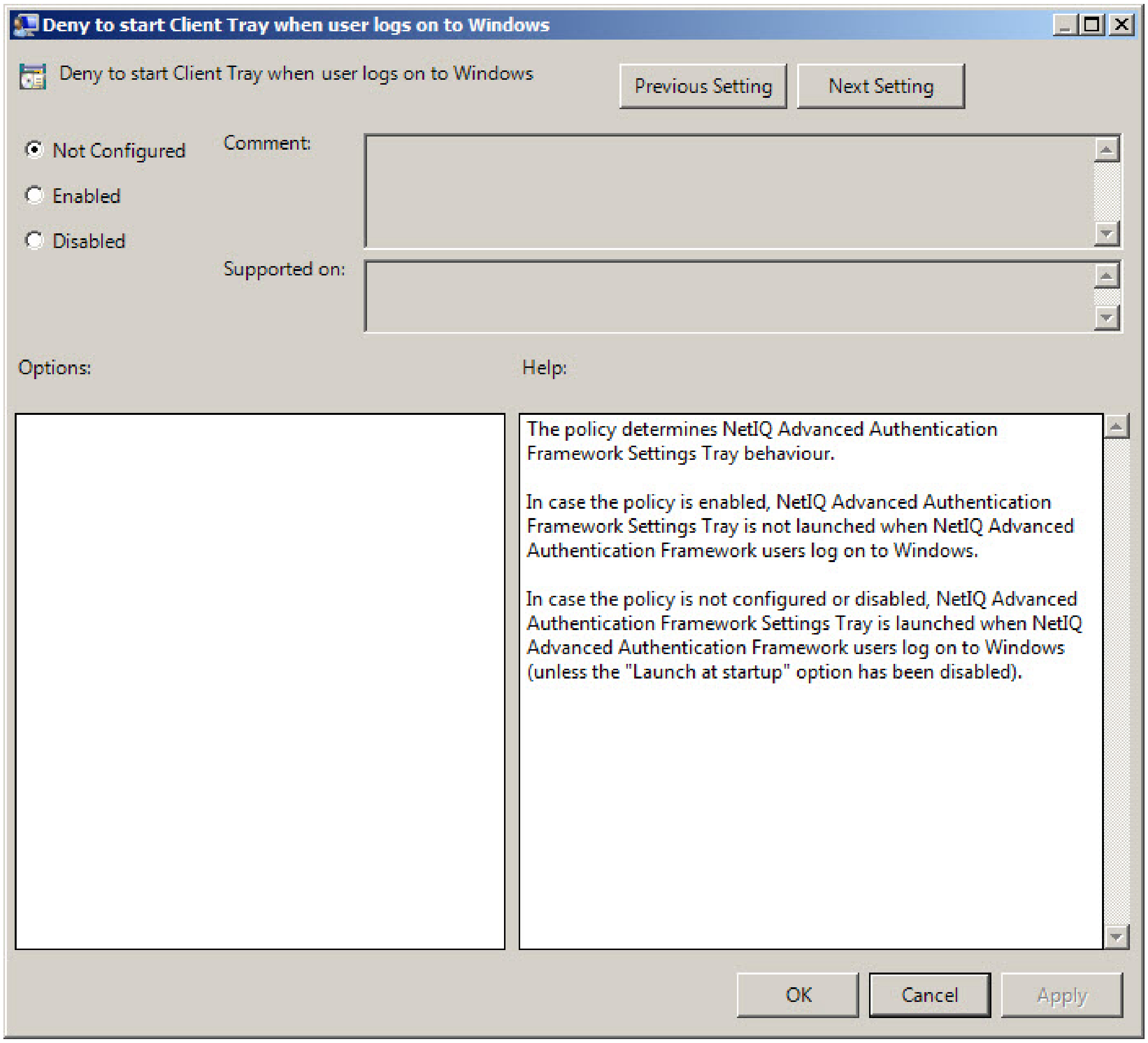
- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

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.


Deny to start Client Tray when user logs on to Windows
Deny to start Client Tray when user logs on to Windows
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

● Not Configured
○ Enabled
○ Disabled

The policy determines NetIQ Advanced Authentication Framework Settings Tray behaviour.

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

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

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
DenyClientTrayAutoStart:

- type: REG_DWORD
- value: 0x00000001 (1)

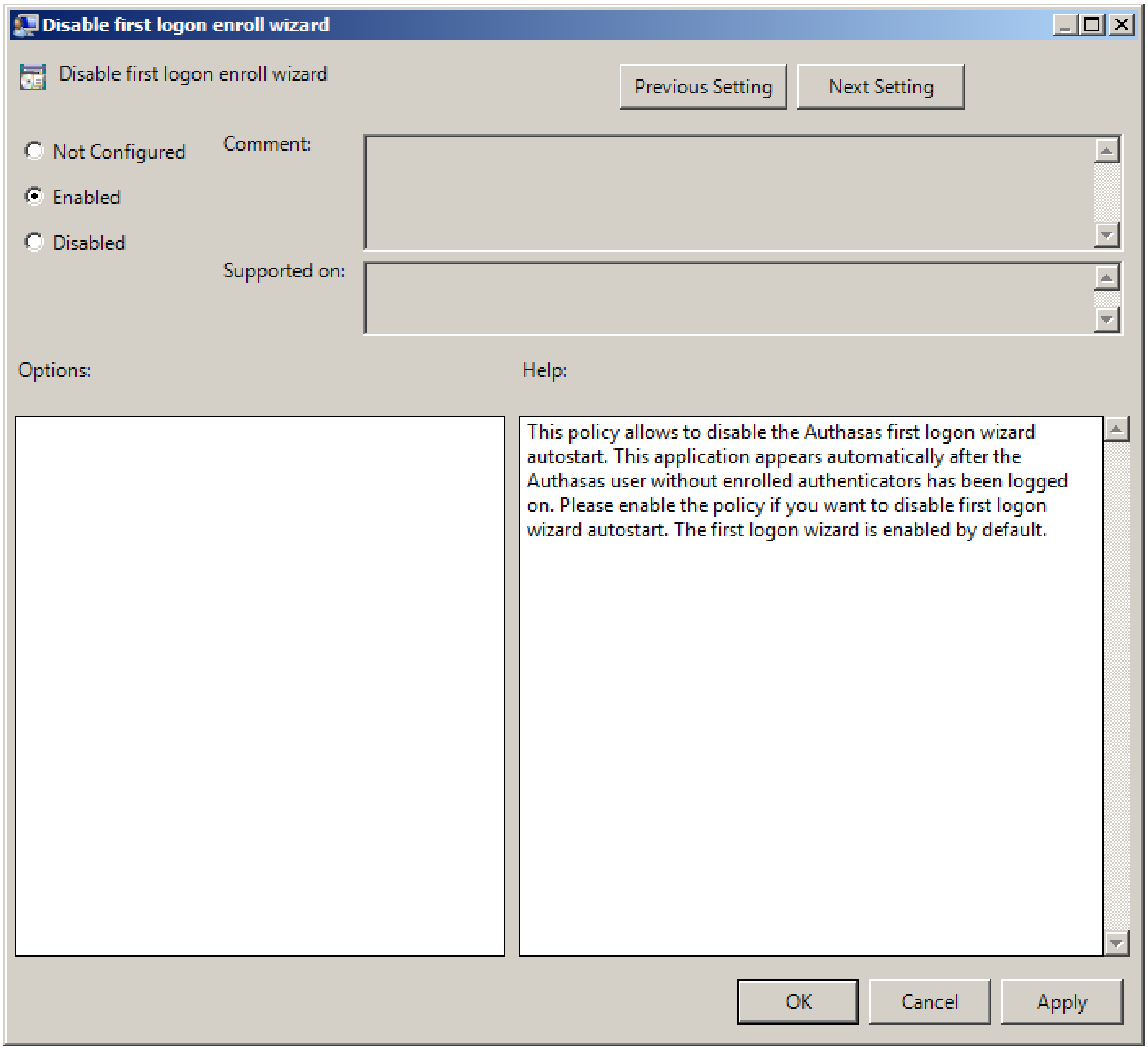
- description: 1 means that the policy is enabled

✱ 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.



This policy allows to disable the Authasas first logon wizard autostart. This application appears automatically after the Authasas 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.

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
DisableFirstLogonEnrollWizard:

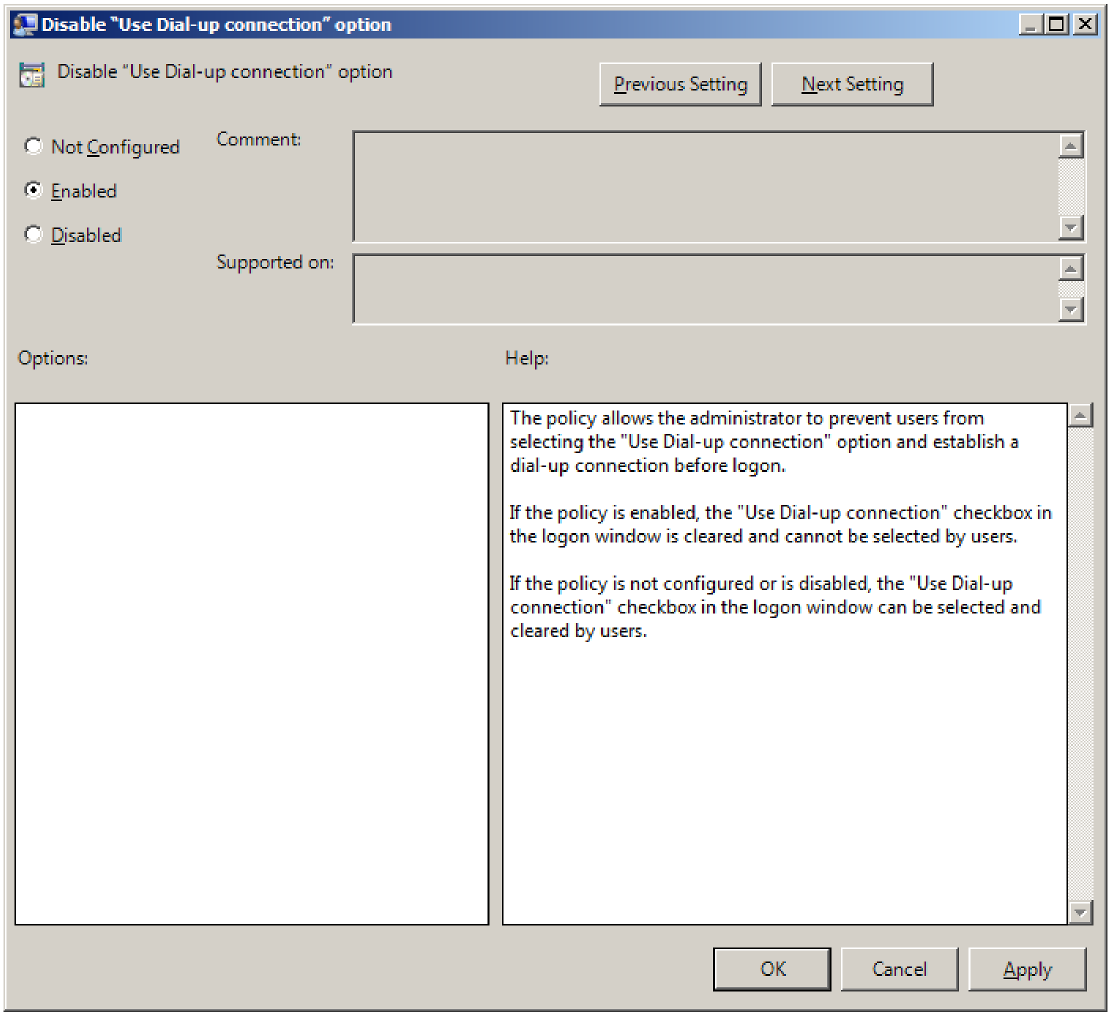
- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

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.



Disable "Use Dial-up connection" option

○ Not Configured
● Enabled
○ Disabled

The policy allows the administrator to prevent users from selecting the "Use Dial-up connection" option and establish a dial-up connection before logon.

If the policy is enabled, the "Use Dial-up connection" checkbox in the logon window is cleared and cannot be selected by users.

If the policy is not configured or is disabled, the "Use Dial-up connection" checkbox in the logon window can be selected and cleared by users.

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

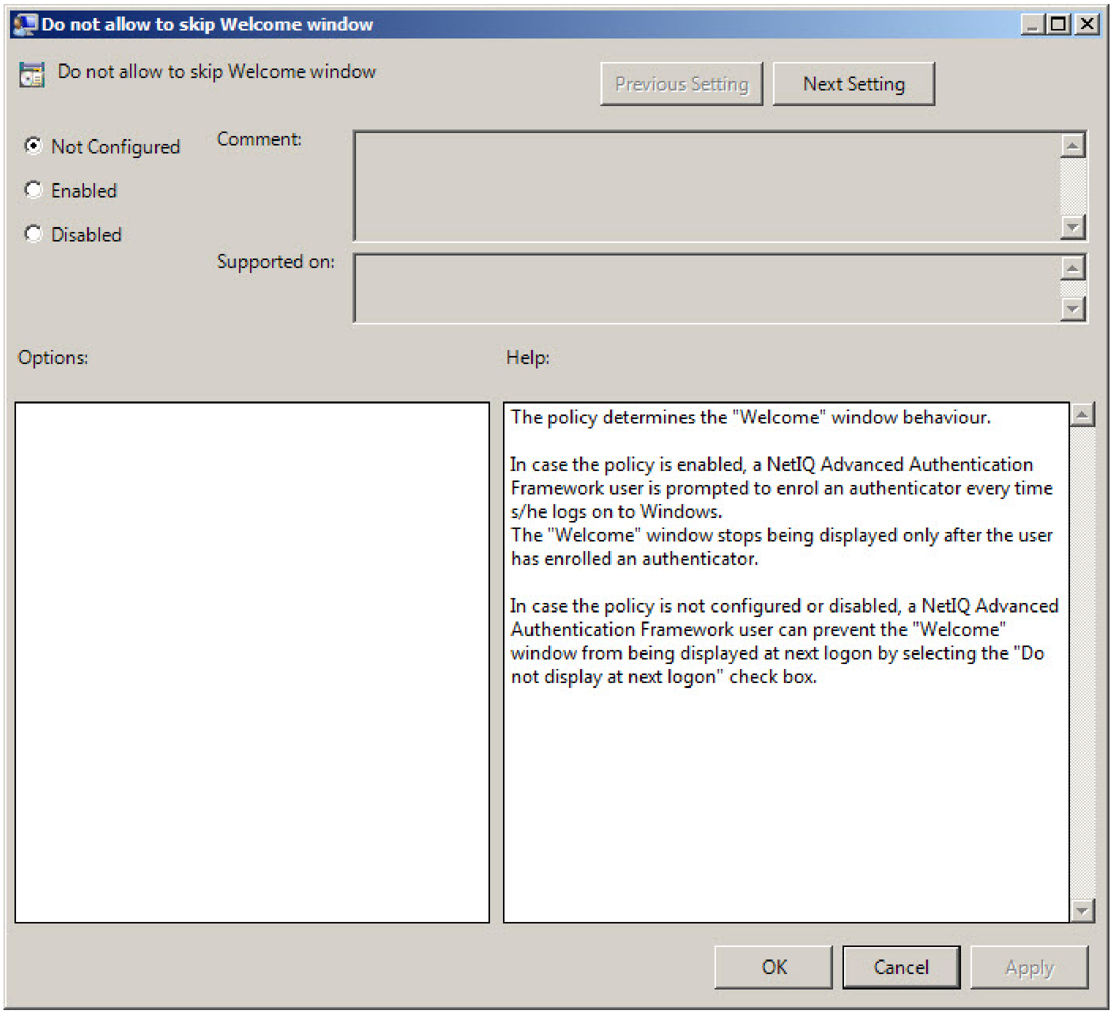
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
GinaDisableDialUp:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.



● Not Configured
○ Enabled
○ Disabled

The policy determines the "Welcome" window behaviour.

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

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

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
ShowFirstLogonWizardAlways:

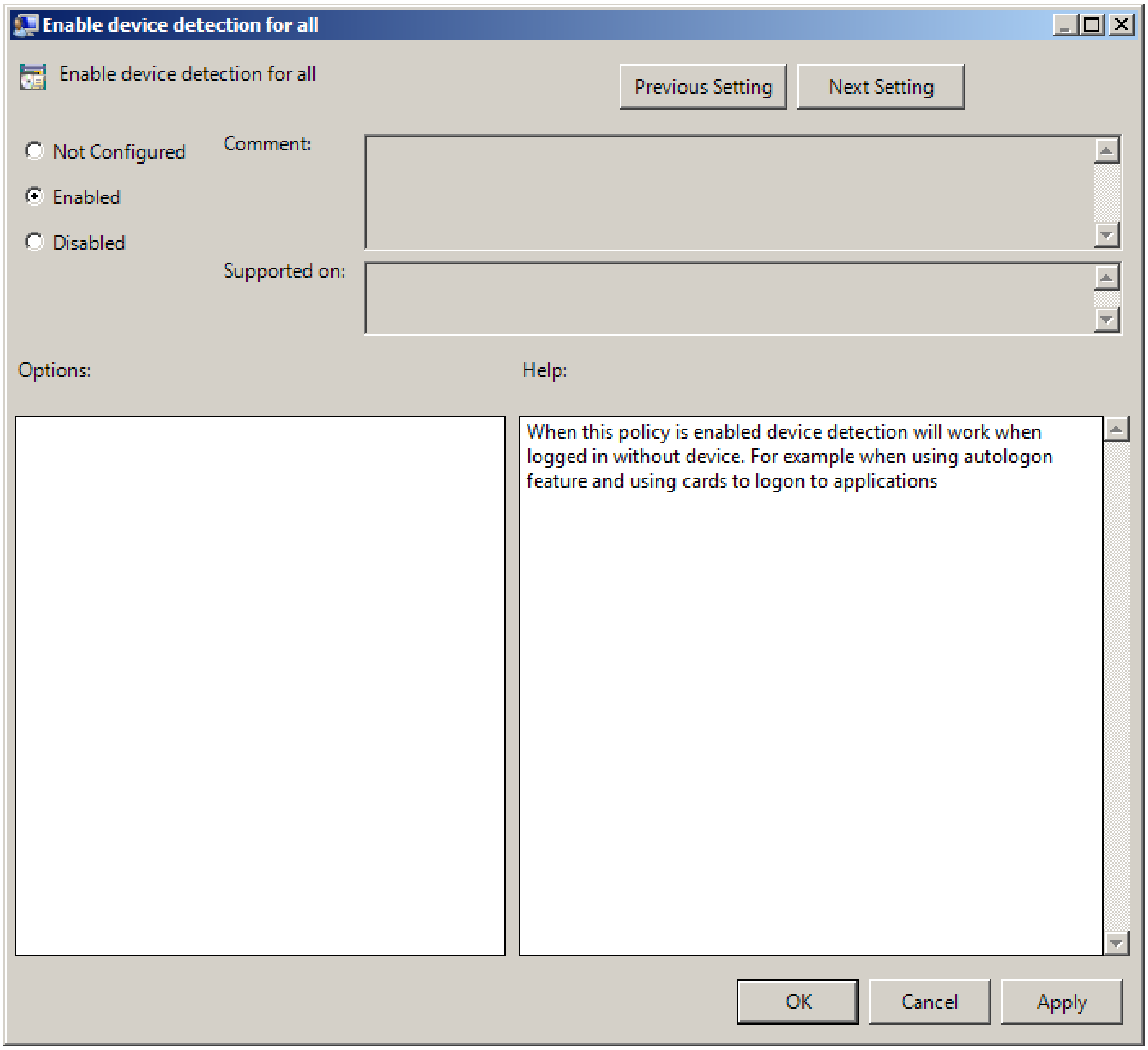
- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

✱ 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.



○ Not Configured
● Enabled
○ Disabled

When this policy is enabled device detection will work when logged in without device. For example when using autologon feature and using cards to logon to applications

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
IsDeviceDetectionForAllEnabled:

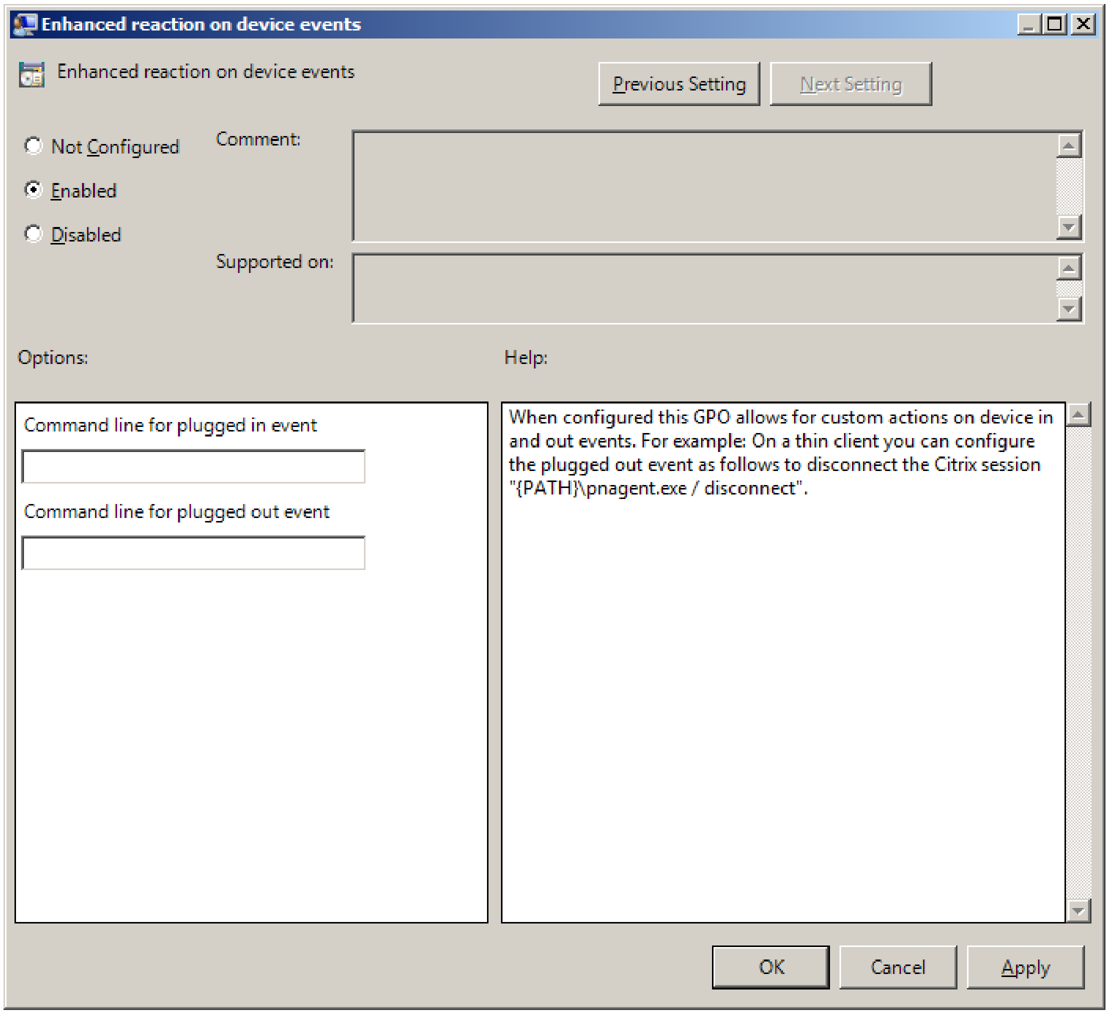
- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

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

○ Not Configured
● Enabled
○ Disabled

Command line for plugged in event

Command line for plugged out event

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

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
PluggedInCommand:

- type: REG_SZ
- value: cmd /c C:\!\OnStart.cmd
- description: cmd /c C:\!\OnStart.cmd displays the command line for plugged in event

PluggedOutCommand:

- type: RED_SZ
- value: cmd /c C:\!\OnEnd.cmd
- description: 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.

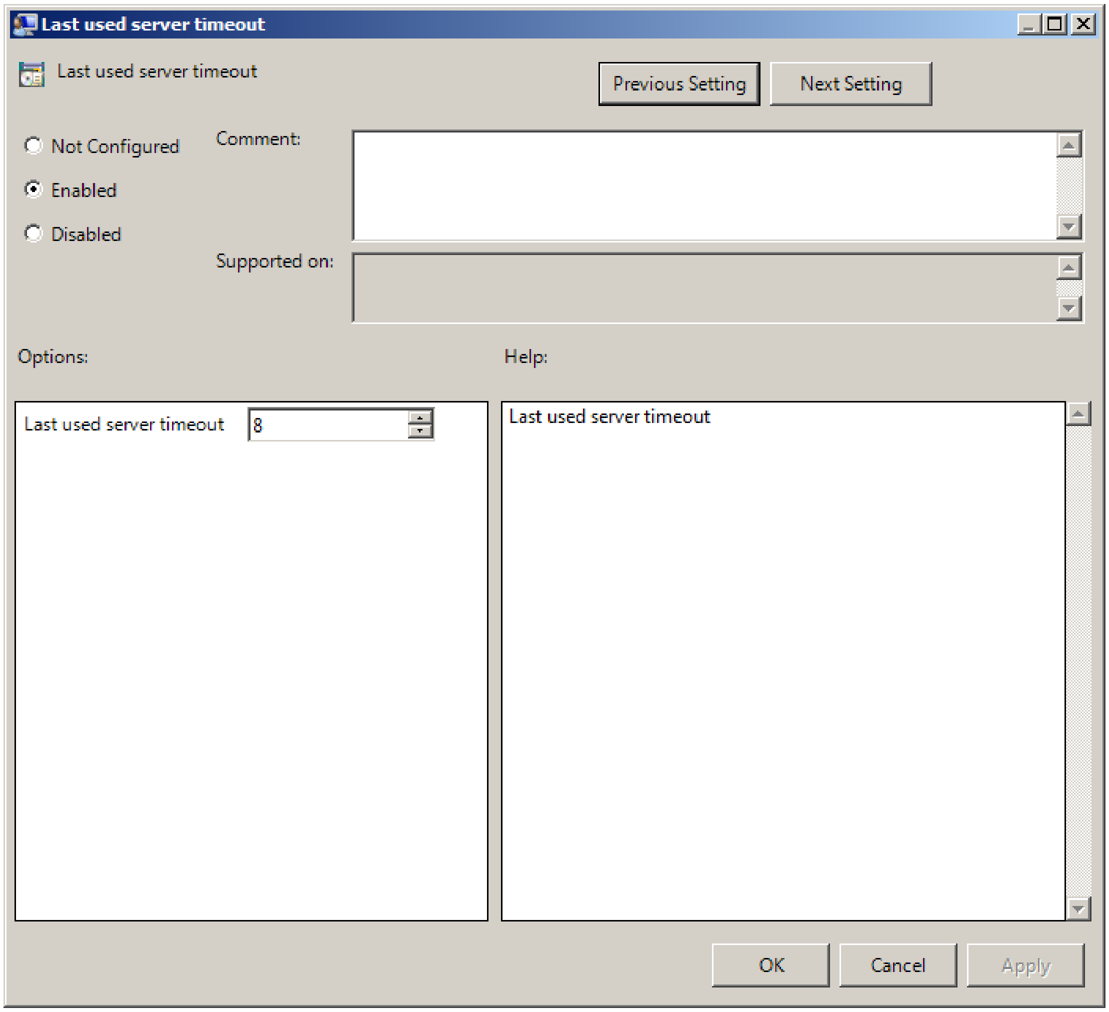
If the **Enable device detection for all** policy is enabled, then the **Enhanced reaction on device events** policy works also when the user was logged on by password or by other device.

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.

Last Used Server Timeout

The **Last used server timeout** policy allows you to specify time (in hours) during which a last used Authenticore Server will be always used on Client. After the specified time, search for another Authenticore Server will be started.



Last used server timeout

Last used server timeout

○ Not Configured
● Enabled
○ Disabled

Last used server timeout 8

Last used server timeout

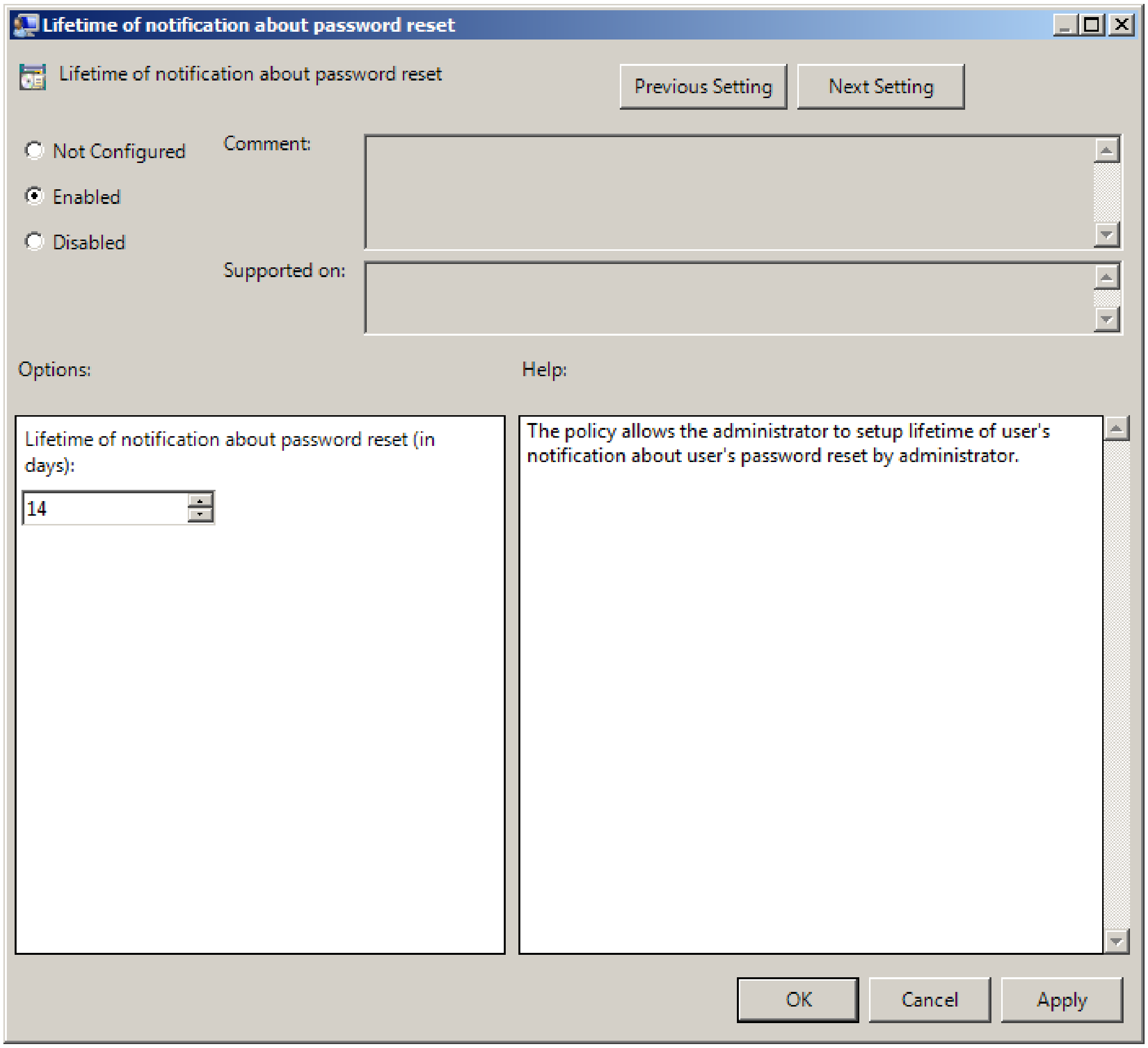
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework

LastUsedServerTimeout:

- type: REG_DWORD
- value: 0x00000008 (8)
- description: 8 displays time during which the last Authenticore Server can be used (in hours)

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.



Lifetime of notification about password reset

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on:

Options:

Lifetime of notification about password reset (in days): 14

Help:

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

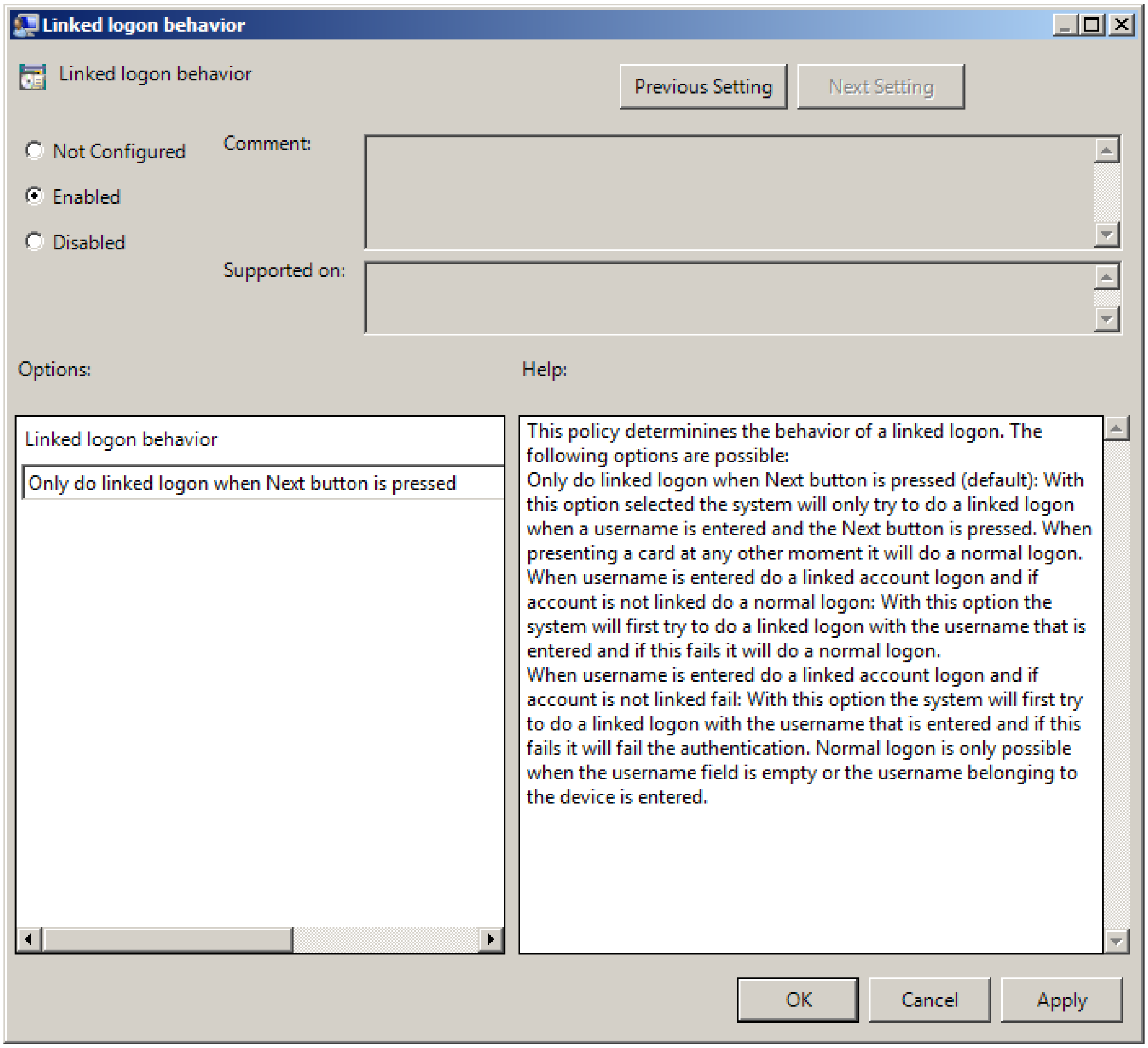
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
ResetPasswordNotificationLifeTime:

- type: REG_DWORD
- value: 0x0000000e (14)
- description: 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.



○ Not Configured

● Enabled

○ Disabled

Linked logon behavior

Only do linked logon when Next button is pressed

This policy determinines the behavior of a linked logon. The following options are possible:
Only do linked logon when Next button is pressed (default): With this option selected the system will only try to do a linked logon when a username is entered and the Next button is pressed. When presenting 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 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 belonging to the device is entered.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
LinkedLogonBehavior:

- type: REG_DWORD
- value: 0x00000000 (0)
- description: 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.

Master Server

The **Master server** policy allows you to specify the list of Master servers to which the Client will connect if there are no Authenticore Servers in the same AD site with the Client or they are not available.

The search for Authenticore Server is preformed in the following way:

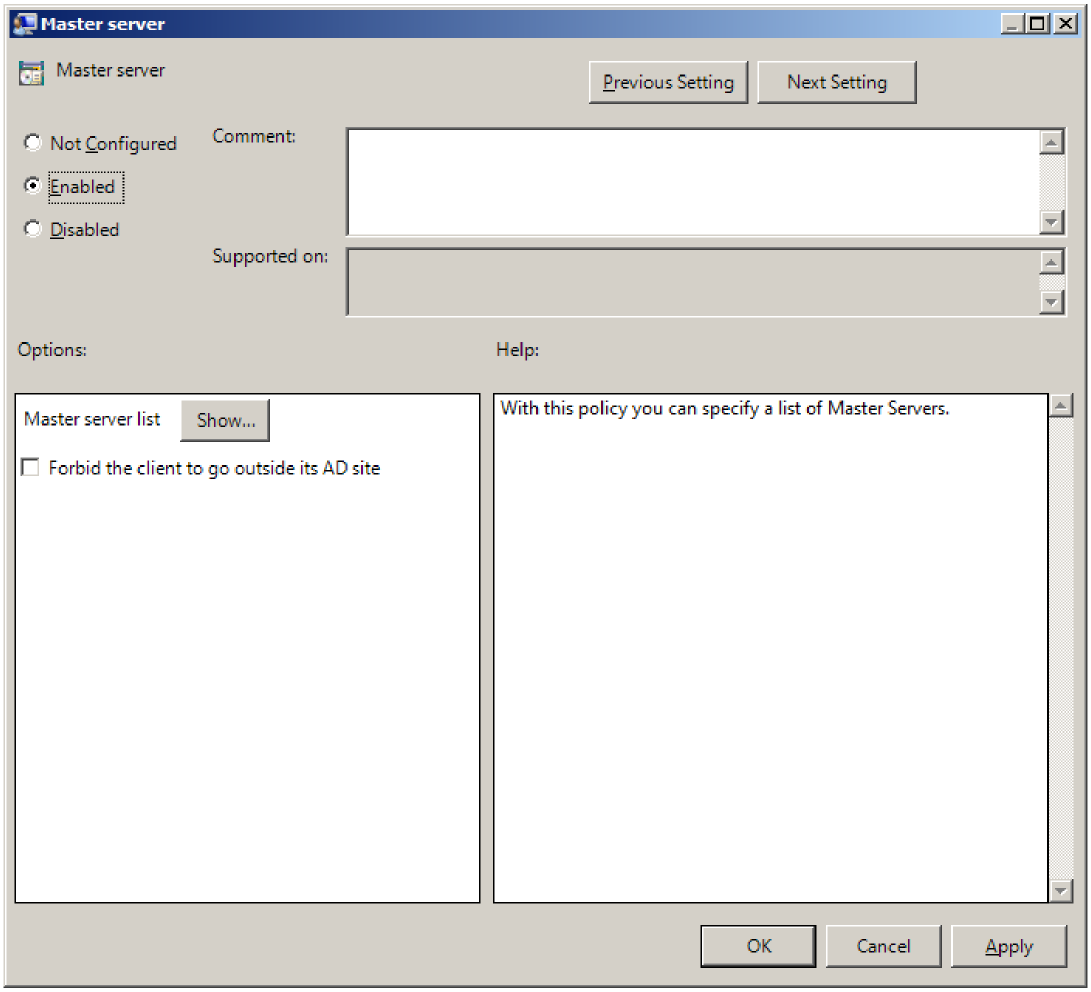
1. Client goes to the last Authenticore Server, if:
    - Client is in the same AD site as the Authenticore Server
    - Client has authenticated not less than 8 hours ago (it is configured using the **Last used server timeout** policy)
2. Otherwise Client connects to the random Authenticore Server from its AD site.
3. If there are no Authenticore Servers in the Client's AD Site or they are not available, Client goes to the Authenticore Server from the Master server list (if the **Master server** is enabled and Authenticore Servers are added to the **Master server list**). Master servers can used no matter in which AD site they are located.
4. If Master servers are not available, Client goes to other servers outside its AD site (if the **Forbid the client to go outside its AD site checkbox** is not selected).

It is recommended to configure the policy only for the AD sites with the installed NetIQ Client, but without available Authenticore Servers. Otherwise the Client will try to connect to the random Authenticore Server which can be located geographically far from the Client (in another country, on another continent). It may cause long authentication delay.

The **Forbid the client to go outside its AD site** checkbox can be selected when Master servers are not specified in the policy or are not available:

- If the checkbox is selected, the Client will not try to connect to any other random server.
- If the checkbox is cleared, the Client will go to a random server.

This option can prevent the delays when there is no cache and no connection to any server.



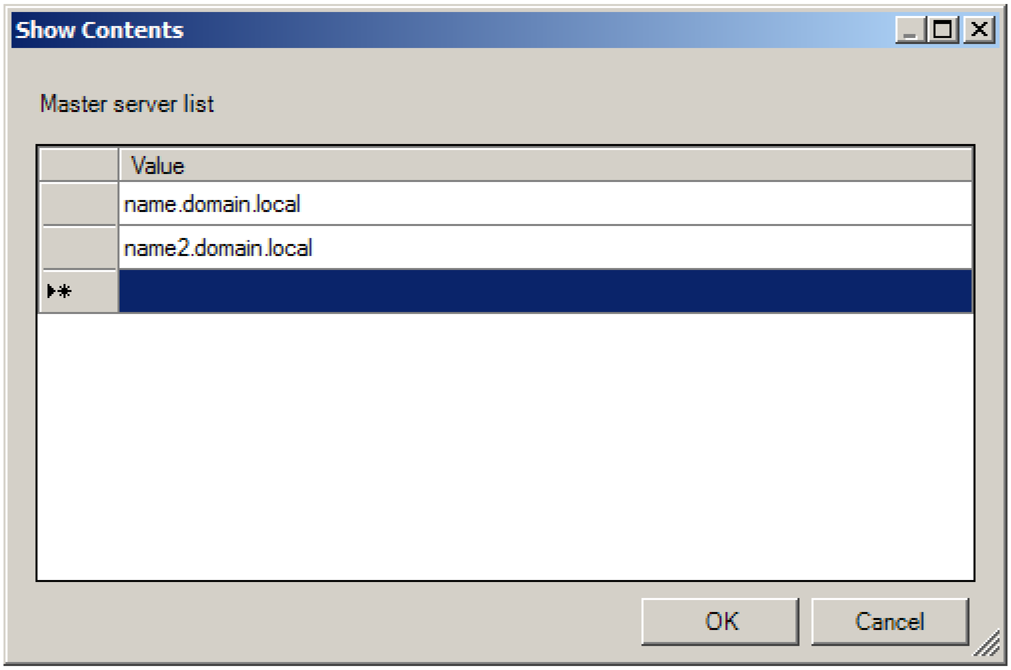
○ Not Configured
● Enabled
○ Disabled

Master server list

□ Forbid the client to go outside its AD site

With this policy you can specify a list of Master Servers.

To add an applicable Master server, click the **Show** button. Specify its name and click **OK** to save changes.



Master server list

	Value
	name.domain.local
	name2.domain.local
▸*	

It is required to specify the DNS name of an applicable server, not its IP address.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
MasterServers:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\MasterServerList
1:

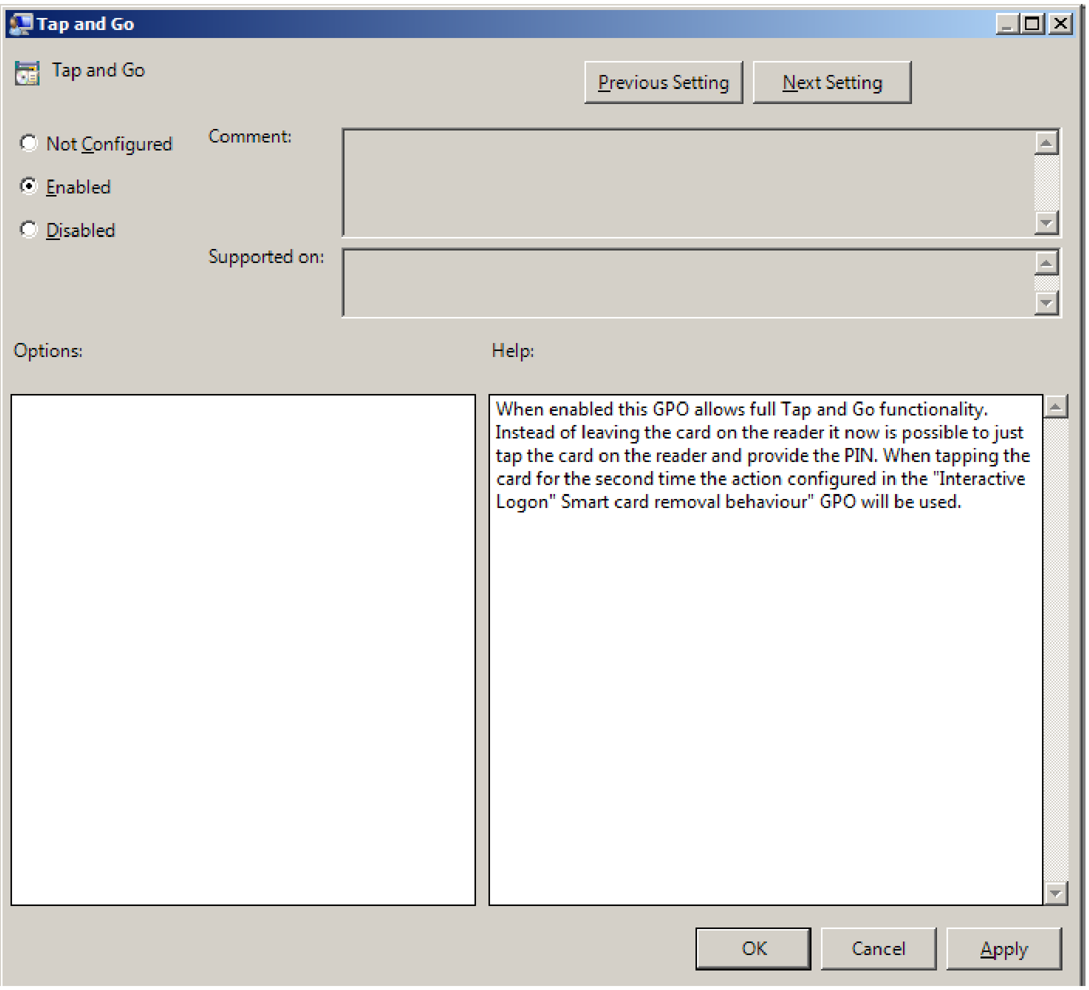
- type: REG_SZ
- value: name.domain.local
- description: name.domain.local displays the name of the first Master server on the list

2:

- type: REG_SZ
- value: name2.domain.local
- description: name.domain.local displays the name of the second Master server on the list

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.



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

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
TapAndGo:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

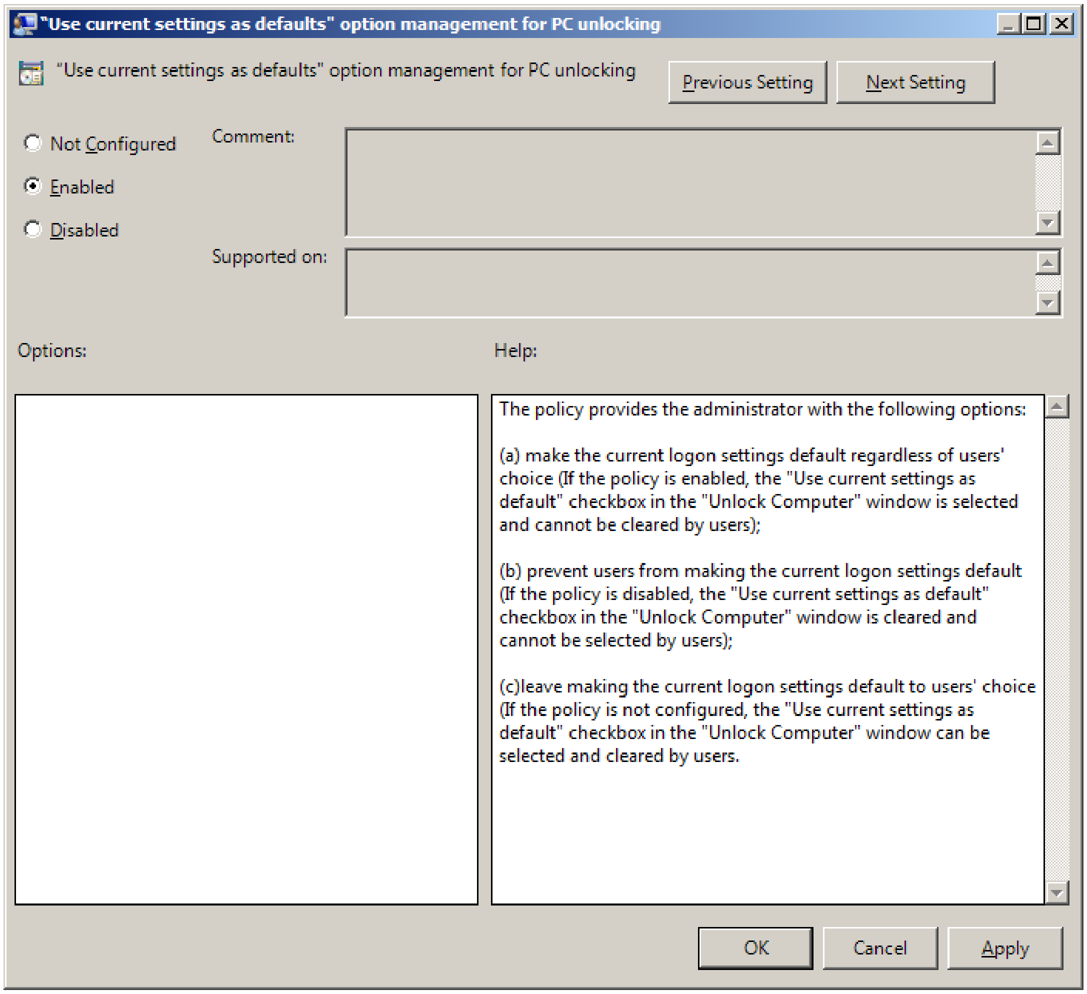
If the policy is not configured or is disabled, user cannot take the card from the reader until the Logon process is finished.

“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:

a. force current logon settings as defaults regardless of users’ wishes;
b. disable the **Use current settings as defaults** option regardless of users’ wishes;
c. let users set the current logon settings as defaults if they wish to.



"Use current settings as defaults" option management for PC unlocking

○ Not Configured
● Enabled
○ Disabled

The policy provides the administrator with the following options:

(a) make the current logon settings default regardless of users' choice (If the policy is enabled, the "Use current settings as default" checkbox in the "Unlock Computer" window is selected and cannot be cleared by users);

(b) prevent users from making the current logon settings default (If the policy is disabled, the "Use current settings as default" checkbox in the "Unlock Computer" window is cleared and cannot be selected by users);

(c)leave making the current logon settings default to users' choice (If the policy is not configured, the "Use current settings as default" checkbox in the "Unlock Computer" window can be selected and cleared by users.

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
GinaCurrentAsDefaultUnlock:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.

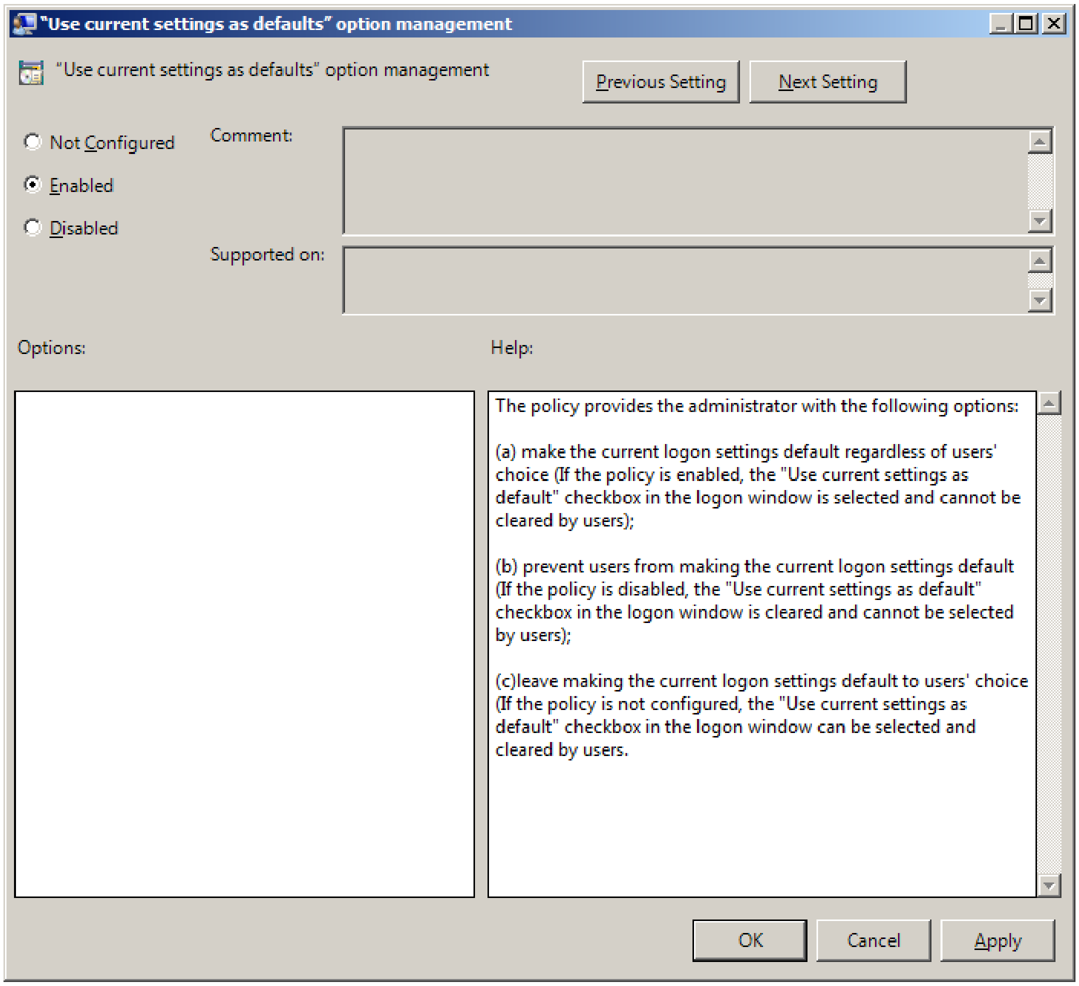
If the policy is not configured, the **Use current settings as defaults** option is enabled and can be selected or canceled by users.

“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:

a. force current logon settings as defaults regardless of users’ wishes
b. disable the **Use current settings as defaults** option regardless of users’ wishes
c. let users set the current logon settings as defaults if they wish to


"Use current settings as defaults" option management
"Use current settings as defaults" option management
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
● Enabled
○ Disabled

The policy provides the administrator with the following options:

(a) make the current logon settings default regardless of users' choice (If the policy is enabled, the "Use current settings as default" checkbox in the logon window is selected and cannot be cleared by users);

(b) prevent users from making the current logon settings default (If the policy is disabled, the "Use current settings as default" checkbox in the logon window is cleared and cannot be selected by users);

(c)leave making the current logon settings default to users' choice (If the policy is not configured, the "Use current settings as default" checkbox in the logon window can be selected and cleared by users.

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
GinaCurrentAsDefault:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

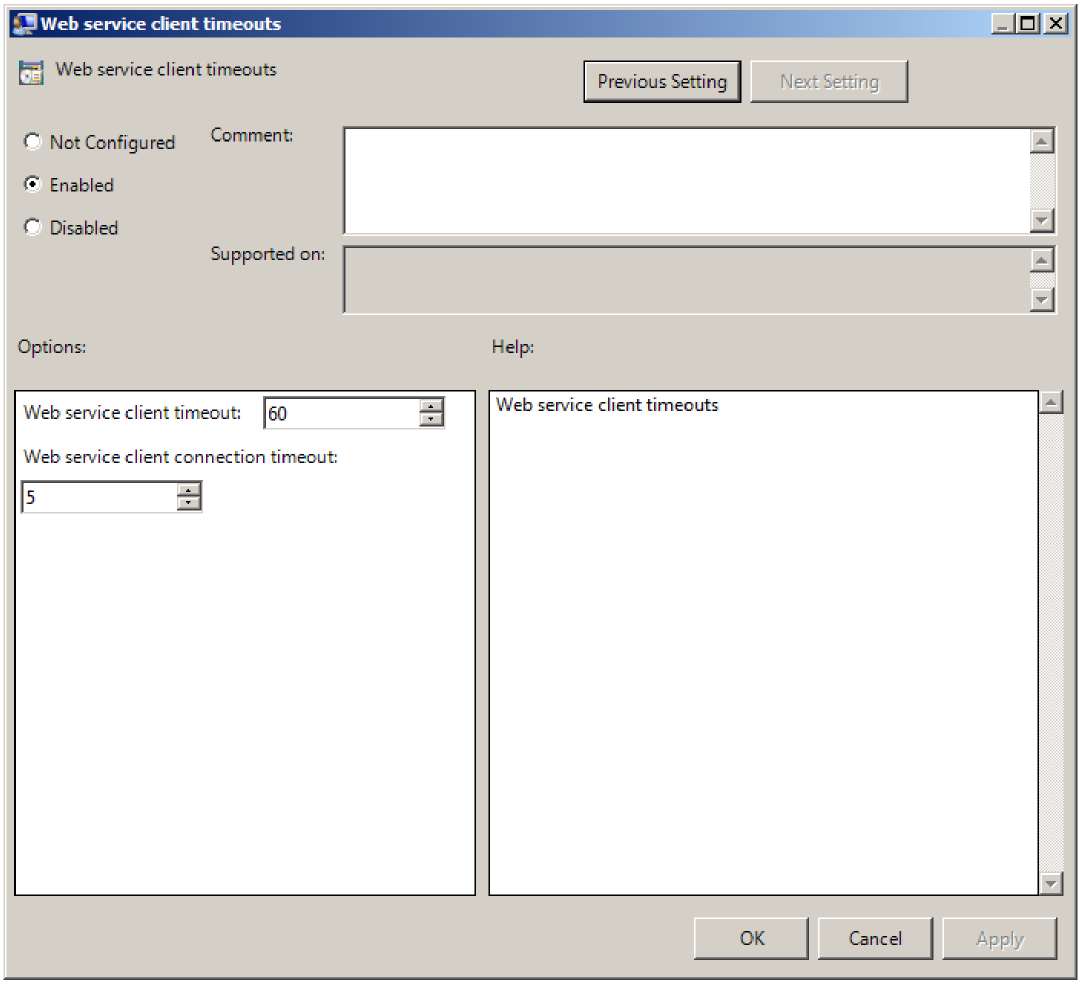
If the policy is enabled, the **Use current settings as defaults** option is always enabled and cannot be canceled by users.

✱ 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 Timeouts

The **Web service client timeouts** policy allows you to set the timeout value for Web Service(s).



Web service client timeouts

○ Not Configured

● Enabled

○ Disabled

Web service client timeout: 60

Web service client connection timeout: 5

Web service client timeouts

It is recommended to install Web Service on every Authenticore Server. If several Web Services are installed, the timeout should be set on the basis of 30 seconds of timeout per Web Service (it means that 90 seconds of timeout should be set for 3 Web Services) but not less than 60 seconds.

HKEY_ LOCAL_ MACHINE\SOFTWARE\ (WowPolicies\ NetIQ \ NetIQ Advanced Authentication Framework

WebServiceClientConnectionTimeout:

- type: REG_DWORD
- value: 0x00000005 (5)

- description: 5 displays duration of connection timeout to one Web Service (in seconds). If Web Service does not respond within 5 seconds, connection to another Web Service in the queue will be established.

WebServiceClientTimeout:

- type: REG_DWORD
- value: 0x0000003c (60)
- description: 60 displays duration of general connection timeout to Web Service(s) (in seconds).

Repository Policies

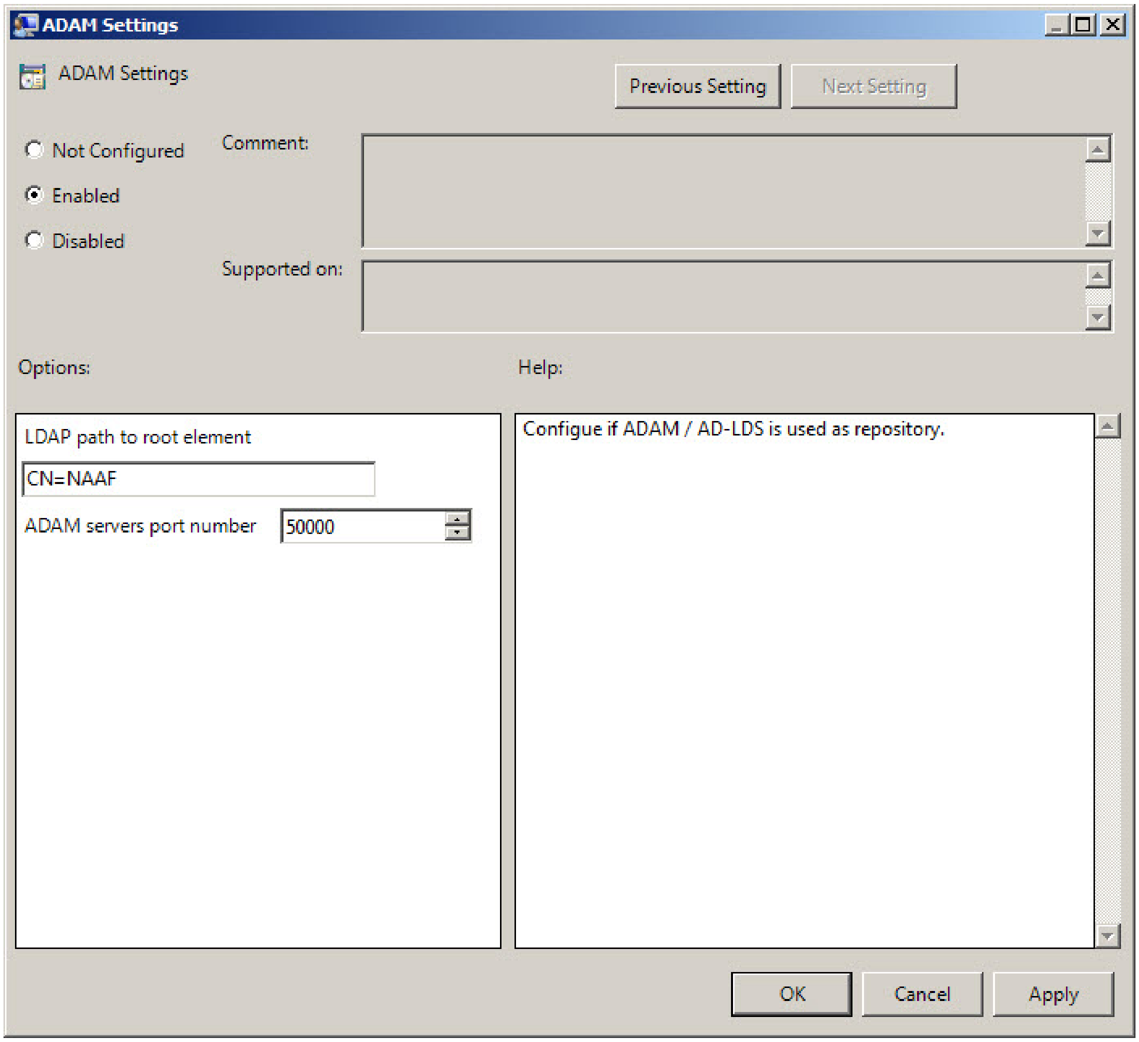
The **Repository** section includes policies that allow you not to extend Active Directory Scheme.

It includes:

- ADAM settings
- Enable Novell support
- Repository

ADAM Settings

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



○ Not Configured
● Enabled
○ Disabled

LDAP path to root element: CN=NAAF

ADAM servers port number: 50000

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

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

Port:

- type: REG_DWORD
- value: 0x0000c350 (50000)
- description: 50000 displays ADAM server port number

RootPath:

- type: REG_SZ
- value: CN=NAAF
- description: 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.

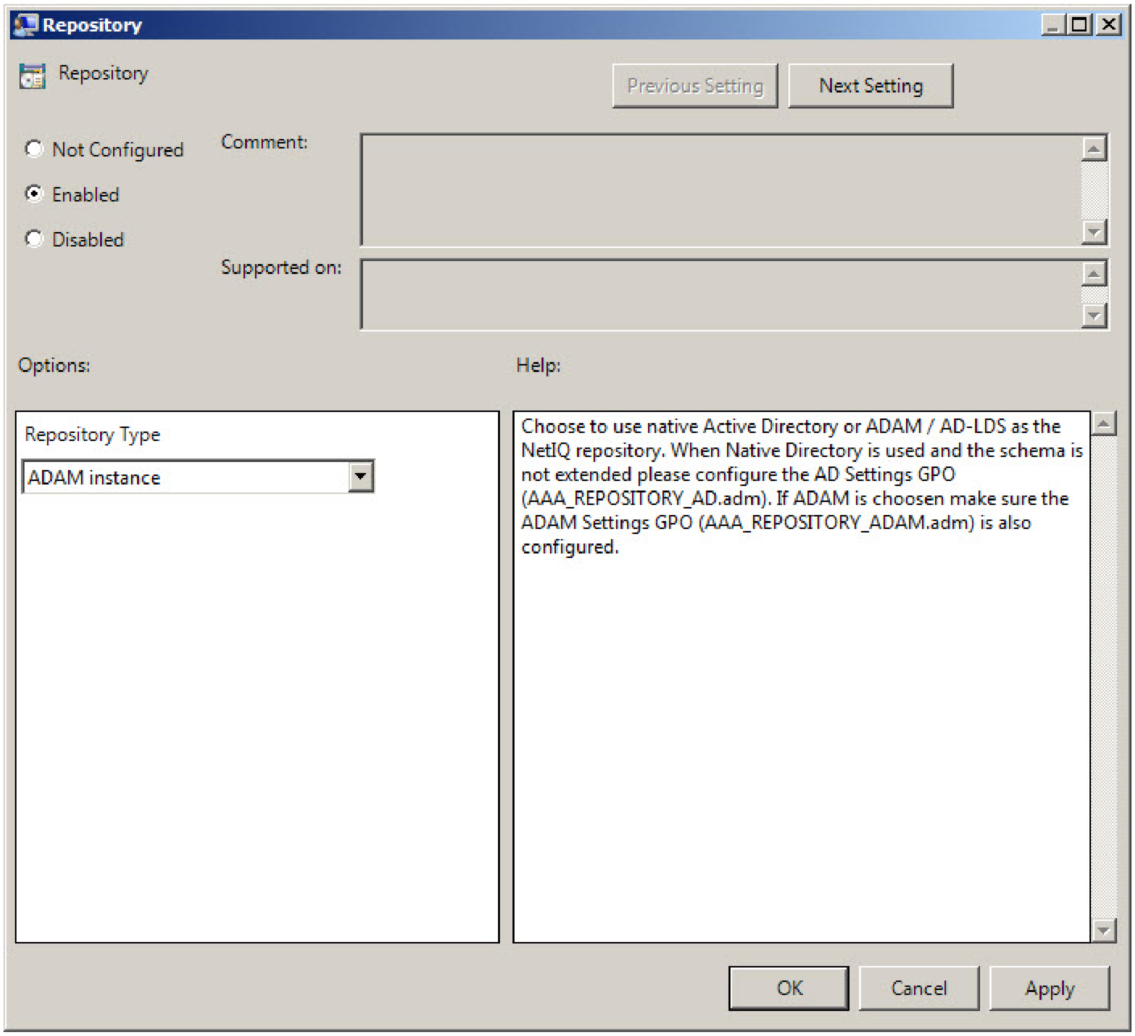
If you decide not to apply this policy, the NetIQ will not work properly, - you will have a problem with 1-N authentication.

HKEY_LOCAL_ MACHINE\SOFTWARE\Policies\ NetIQ \ NetIQ Advanced Authentication Framework\Repository
NovellSupportEnabled:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.



○ Not Configured
● Enabled
○ Disabled

Repository Type: ADAM instance

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 choosen make sure the ADAM Settings GPO (AAA_REPOSITORY_ADAM.adm) is also configured.

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.

HKEY_ LOCAL_ MACHINE\SOFTWARE\Policies\ NetIQ \ NetIQ Advanced Authentication Framework\Repository
Type:

- type: REG_DWORD
- value: 0x00000002 (2)
- description: 2 means that ADAM instance is chosen

UI Look & Feel Policies

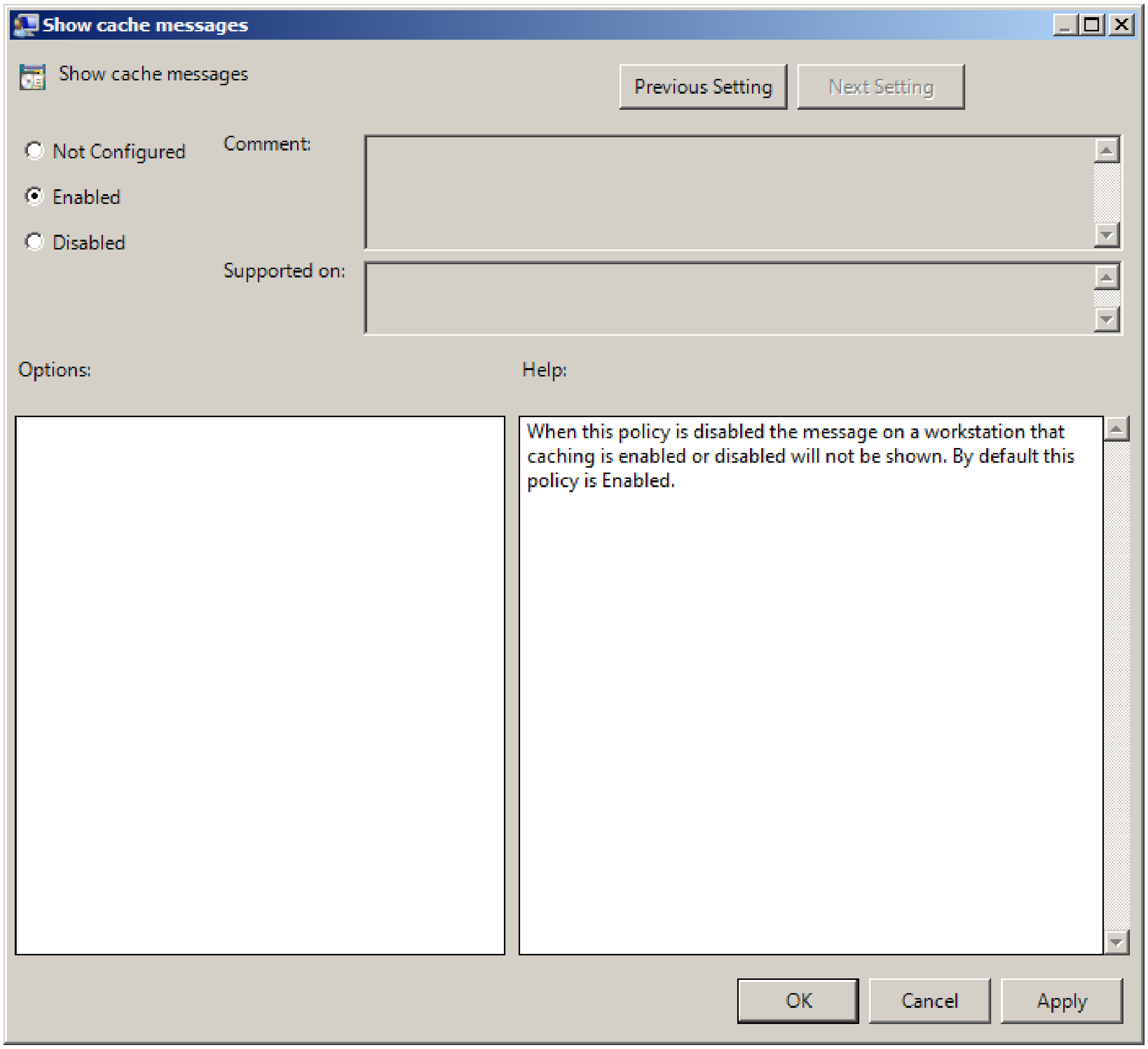
The **UI Look & Feel** section includes policies designed for terminal clients. The **UI Look & Feel** section is located in **Group Policy Management Editor** under **User Configuration -> Policies -> Administrative Templates: Policy definitions -> NetIQ Advanced Authentication Framework**.

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.



○ Not Configured
● Enabled
○ Disabled

When this policy is disabled the message on a workstation that caching is enabled or disabled will not be shown. By default this policy is Enabled.

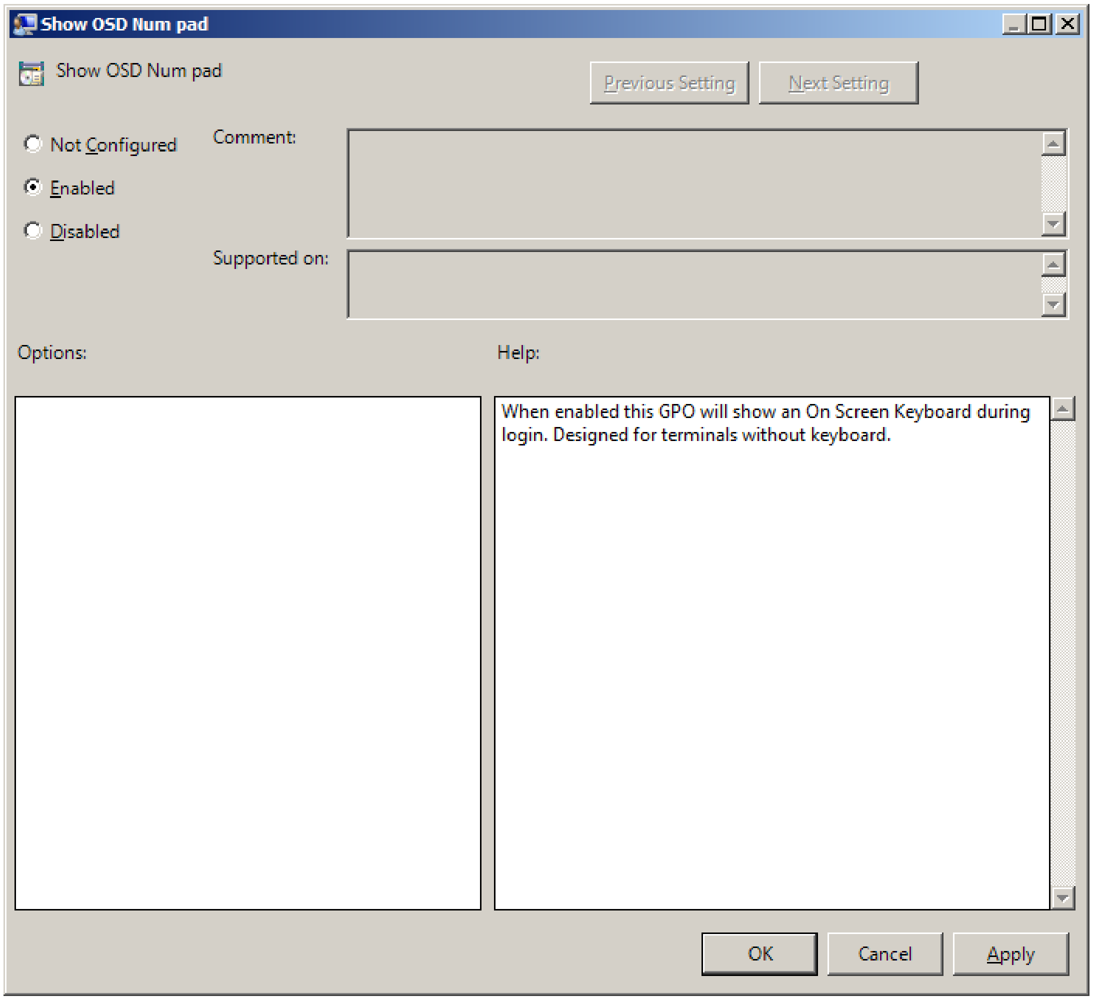
By default this policy is enabled.

HKEY_CURRENT_USER\Software\Policies\NetIQ\NetIQ Advanced Authentication
ShowCacheMessages:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 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.



○ Not Configured
● Enabled
○ Disabled

When enabled this GPO will show an On Screen Keyboard during login. Designed for terminals without keyboard.

HKEY_CURRENT_USER\Software\Policies\NetIQ\NetIQ Advanced Authentication Framework
OSDNumPadEnabled:

- type: REG_DWORD
- value: 0x00000001 (1)
- description: 1 means that the policy is enabled

Index