



NetIQ Advanced Authentication Framework - Group Policy Templates

Administrator's Guide

Version 5.1.0

Table of Contents

	1
Table of Contents	2
Introduction	4
About This Document	4
Group Policies	5
Adding Group Policies	8
Security Policies	9
Authenticator Life Period	10
Credential Providers Filter Settings	12
Default method for Other user	14
Disabled PIN Host List	15
Disable Random Password Generation by Default	17
Do not Allow Administrators to Remove User Credentials	18
Enable Caching	19
Enable PIN Caching	20
Hide password mode from logon UI	22
Lock account on failed logon	23
Number of Cached Users	25
Password Length	26
PIN Restrictions	28
Use domain password as PIN	29
Event Log Policies	31
Freeze Communication If Log Server Is Unavailable	32
Log Servers	34
Register All Password Management Events	36
Register All User Authentication Events	37
Network Policies	38
Always resolve client name	38
Force to use NTLM authentication during logon	39
RPC dynamic port selection allowed	40
RPC static port selection allowed	41
Runtime Environment	43
Show Enrolled Card Owner	43
Users and Groups	44
Customize Users and Group Settings	45
Workstation Policies	47
Alternative Logo for Credential Provider	48
Alternative Logo for GINA and Wizard	50
Deny to Specify Authenticator Comment at Enrollment	52
Deny to Start Client Tray When User Logs on to Windows	53
Disable First Logon Enroll Wizard	55
Disable "Use Dial-up Connection" Option	56
Do Not Allow to Skip Welcome Window	58

Enable Device Detection for All	60
Enhanced Reaction on Device Events	62
Lifetime of Notification about Password Reset	64
Linked Logon Behavior	65
Tap and Go	67
“Use Current Settings as Defaults” Option Management for PC Unlocking	68
“Use Current Settings as Defaults” Option Management	70
Web service client timeout	71
Repository Policies	73
ADAM Settings	74
Enable Novell Support	75
Repository	76
UI Look & Feel Policies	78
Show Cache Messages	79
Show OSD Num Pad	80
Index	81

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 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.

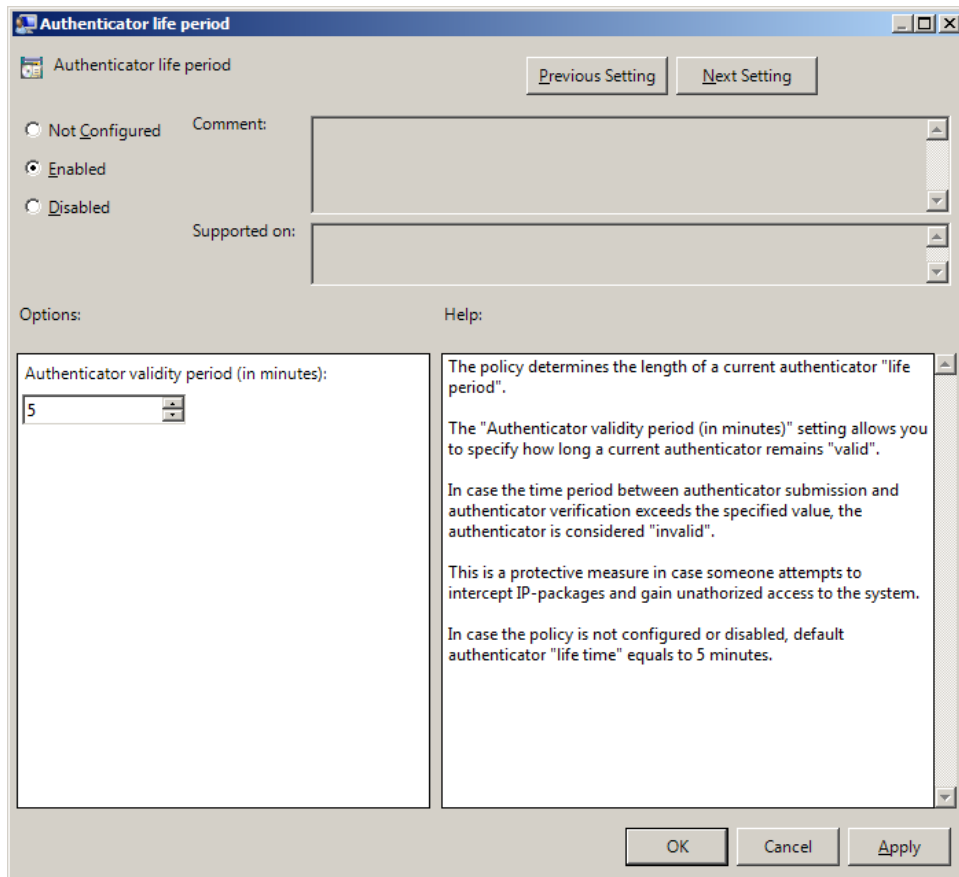
It includes:

- [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)

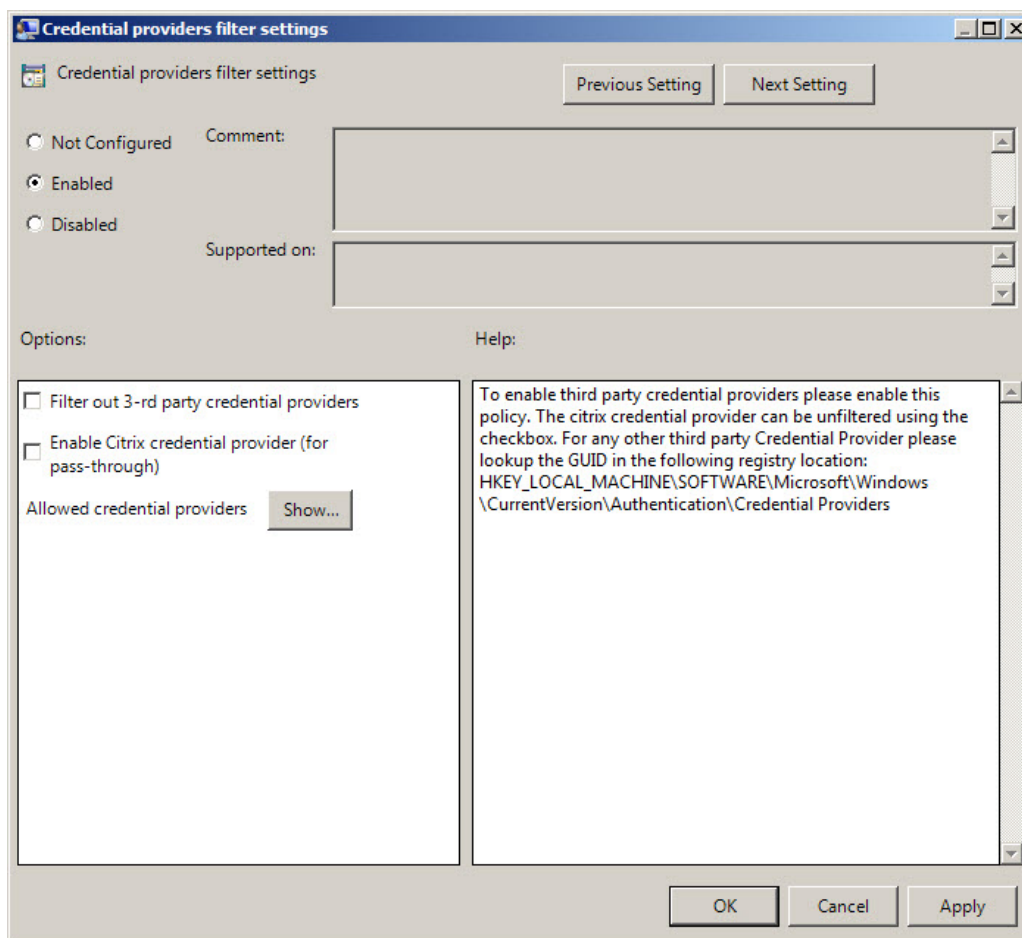
value: 0x00000005 (5)

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 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}.

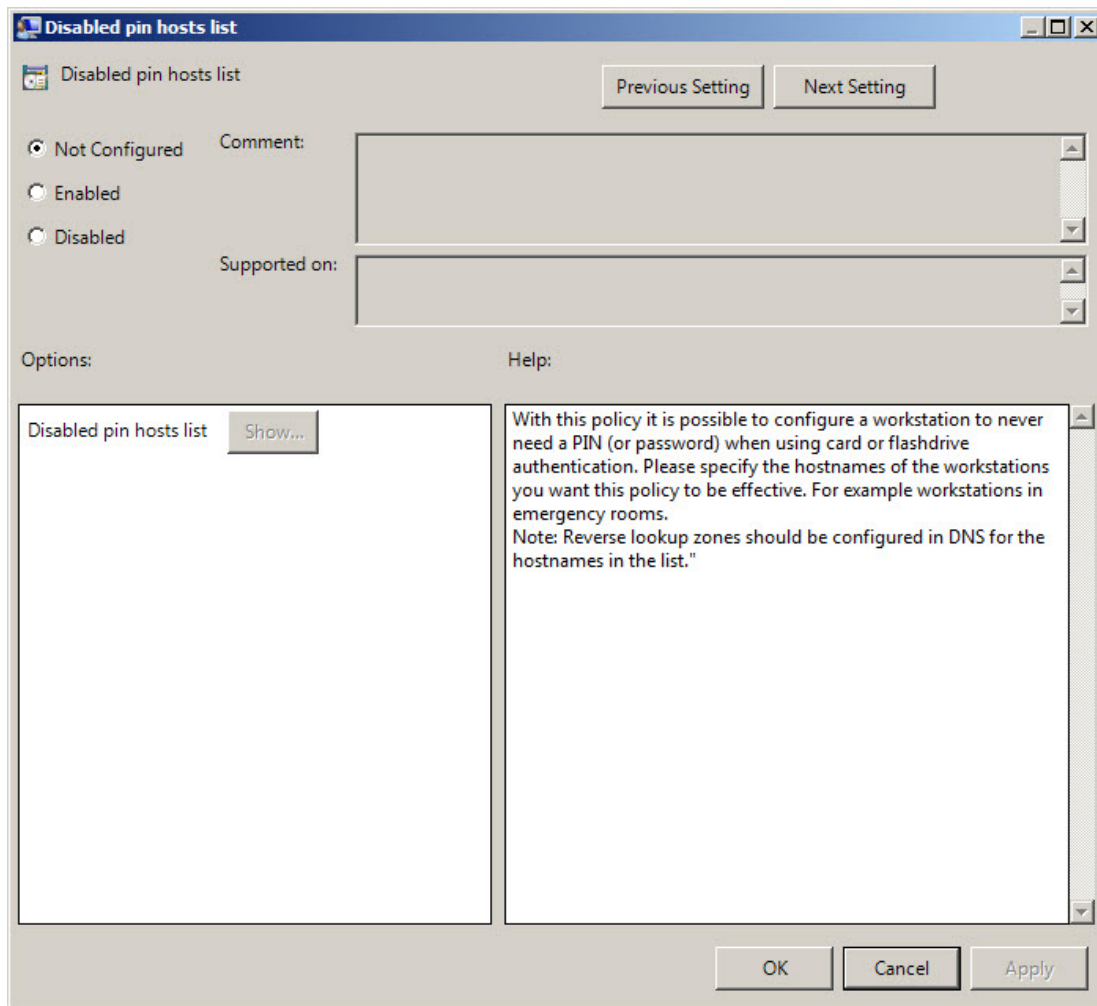
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: OtherUserDefMethod (REG_SZ)
value: {9D5D01EF-76B0-1749-838B-C1441F7E23B3}
{9D5D01EF-76B0-1749-838B-C1441F7E23B3} means that Security Questions method of authentication is used by default for the "Other user".

 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:



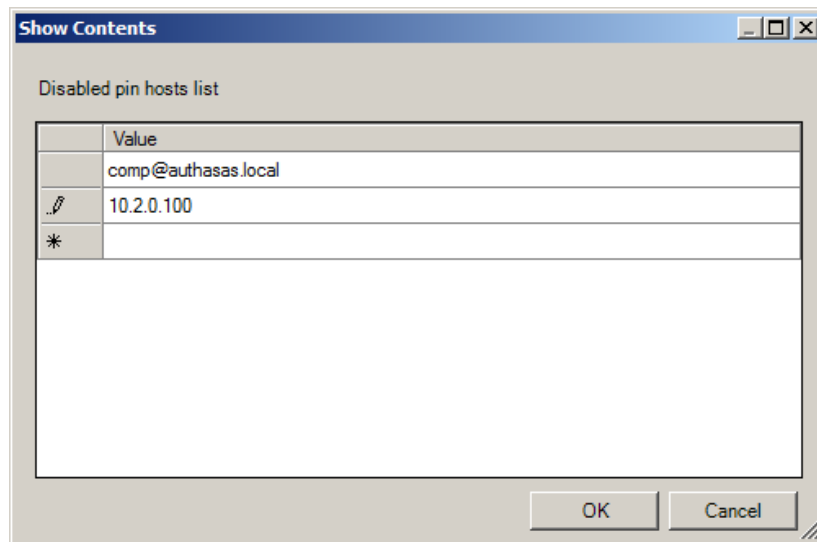
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework\DisabledPinHostList
parameter: Host1 (REG_SZ) (the specified host name is displayed in the registry parameter)
value: 1
1 displays the value that was added to the Show Contents window

* 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.

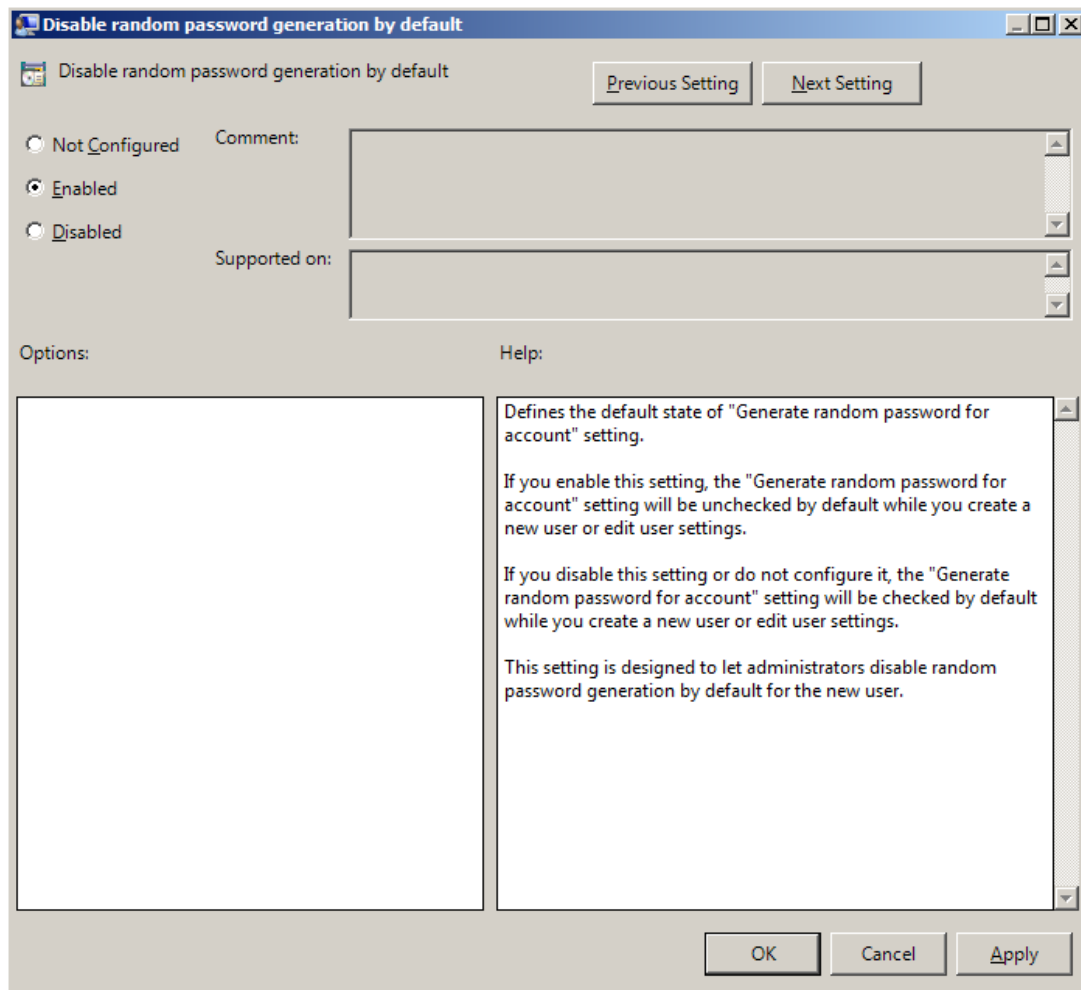


After all computers and IP addresses that will not need to enter PIN to logon are added, click the **OK** button to save changes. Then click the **Apply** button to save all the changes.

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)

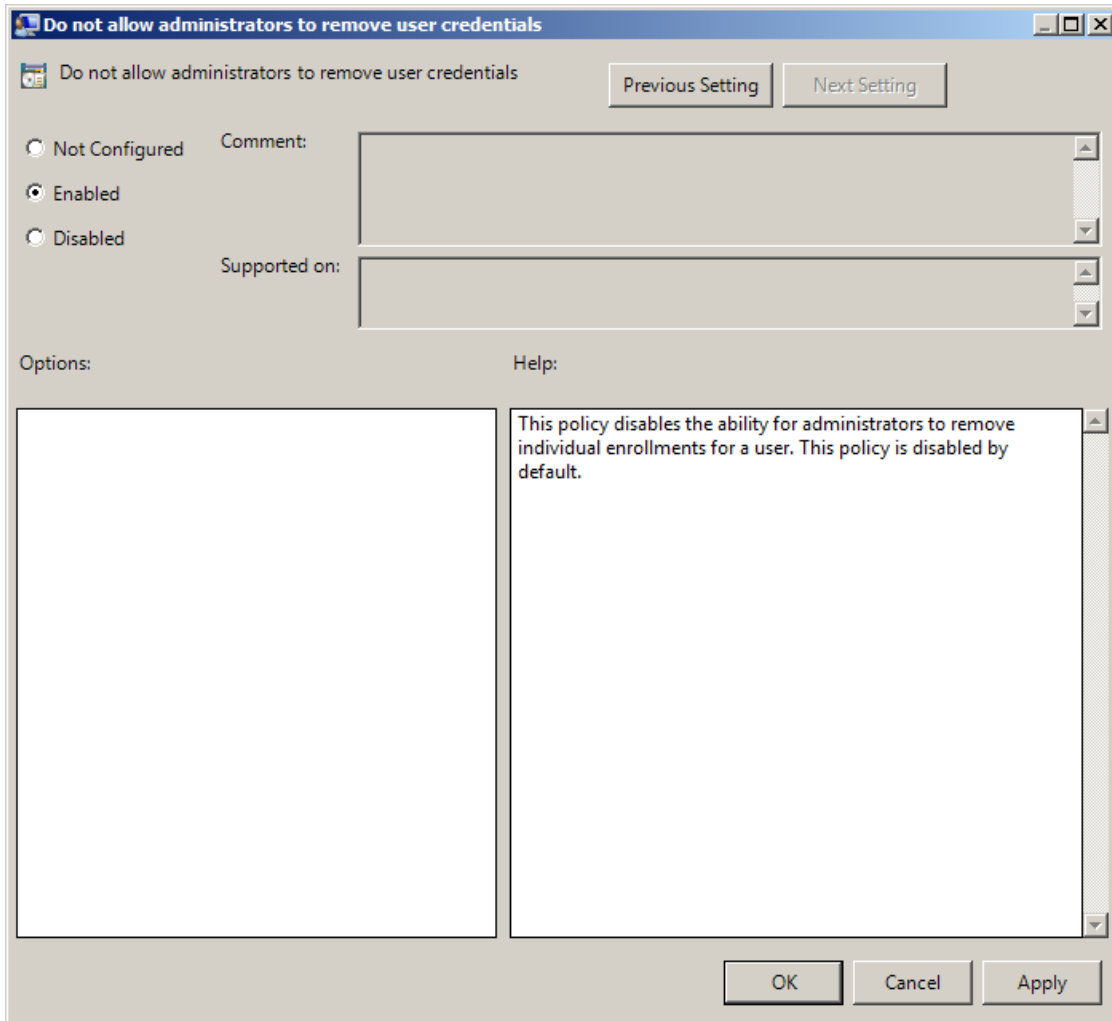
1 means that the policy is enabled.

* 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.



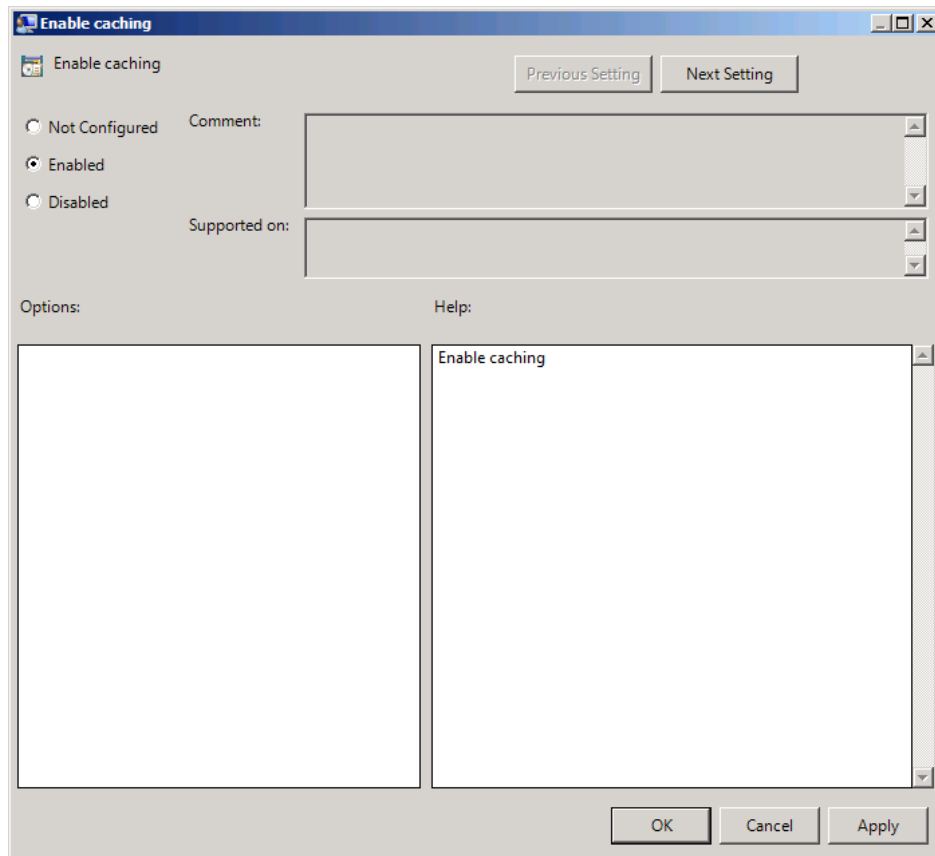
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DisableRemoveTemplatesByAdmin (REG_DWORD)

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.

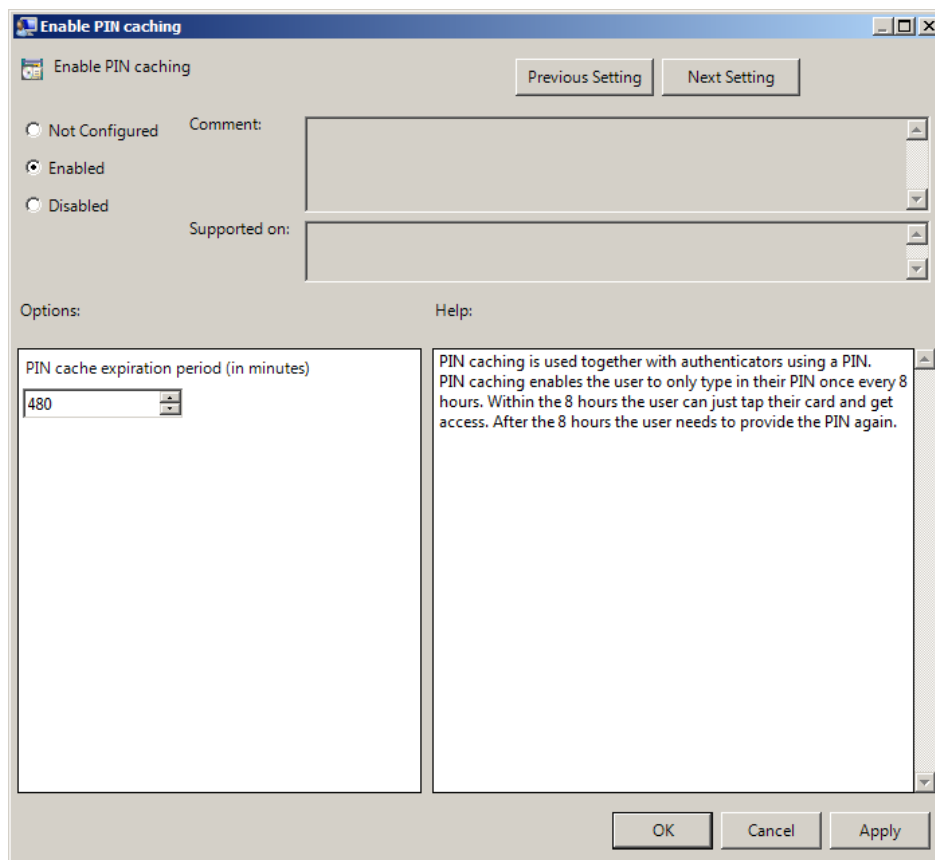
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: IsCacheEnabled (REG_DWORD)

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)

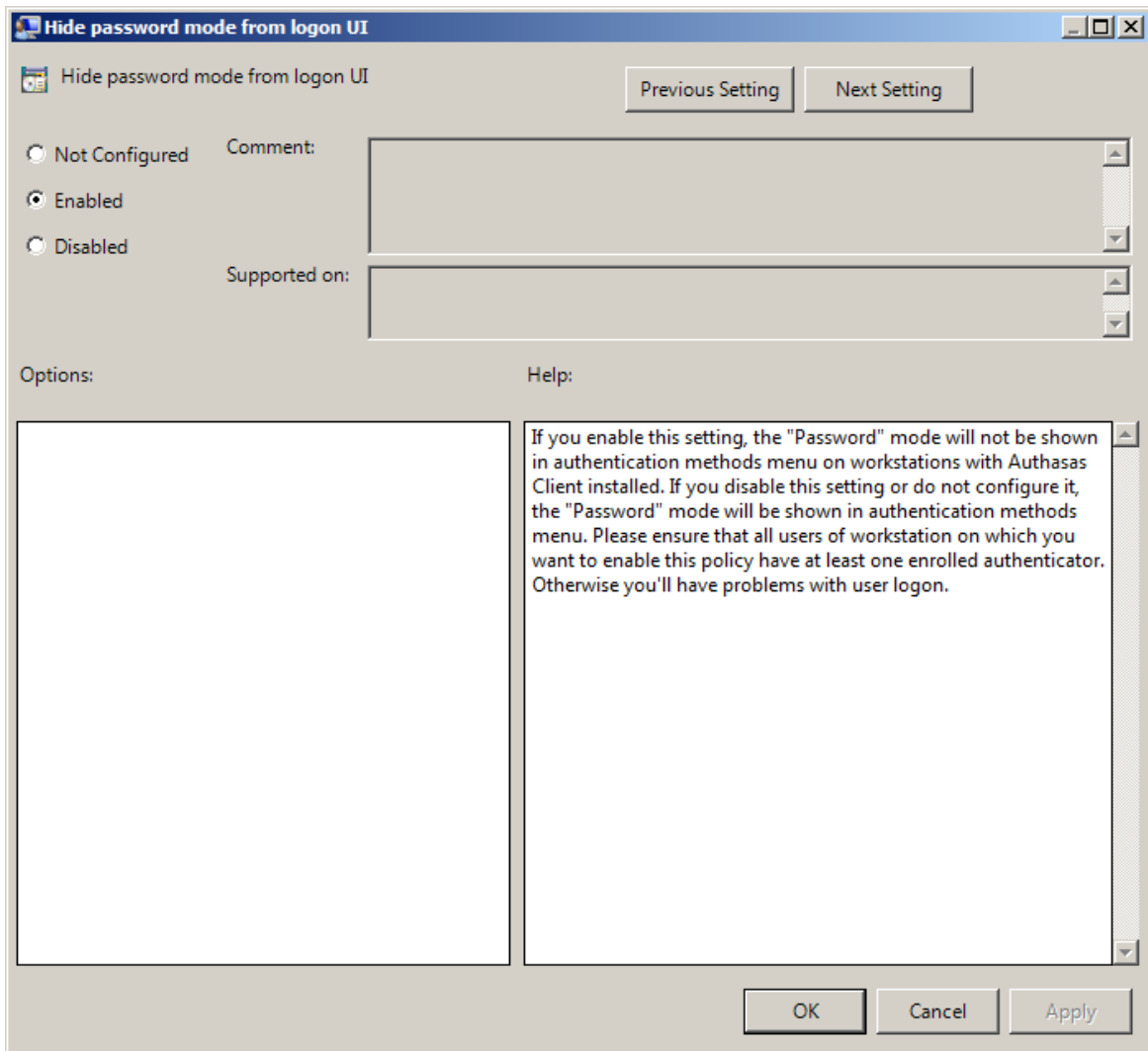
 If the policy is not defined or is disabled, the user should type in his/her PIN during every authentication process.

 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

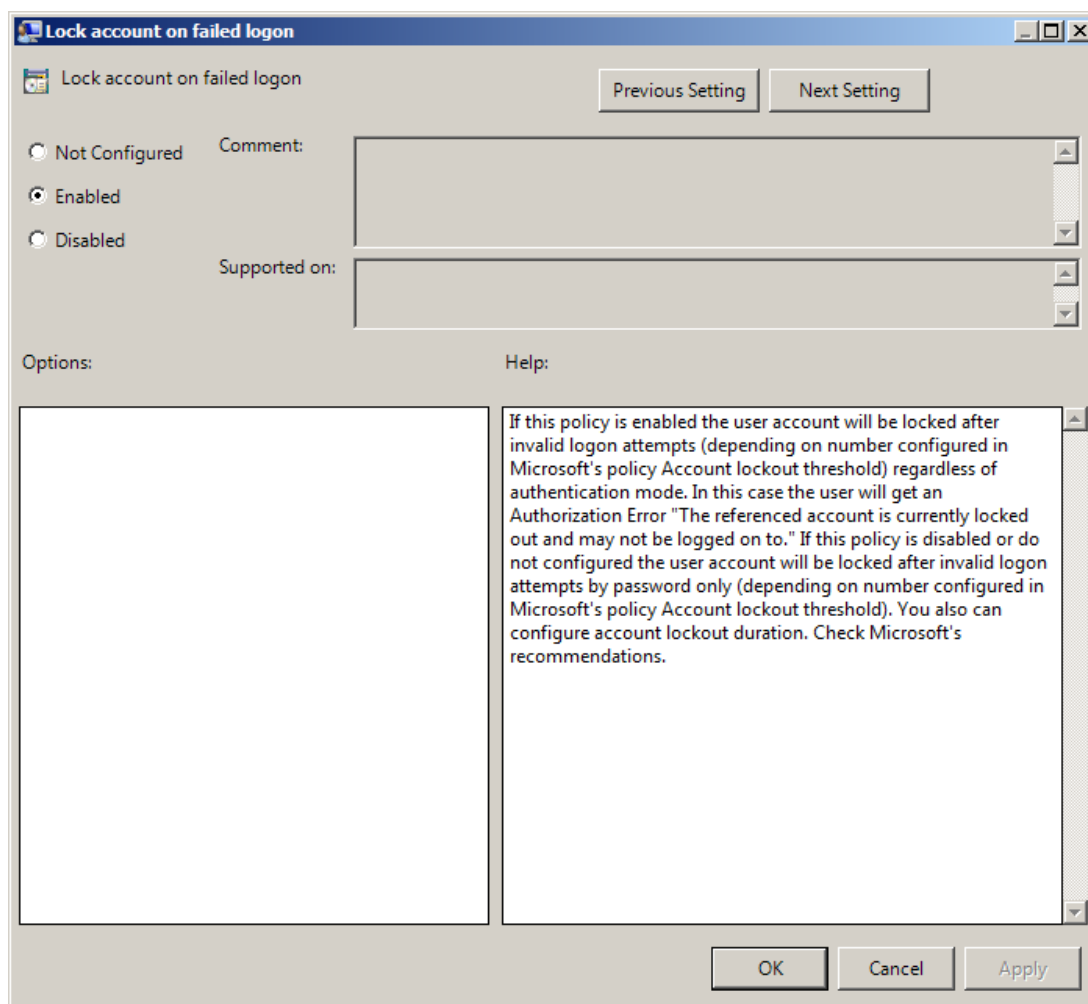
 Please ensure that all users of workstation on which you want to enable this policy have at least one enrolled authenticator. Otherwise, you will have problems with user logon.

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](#).

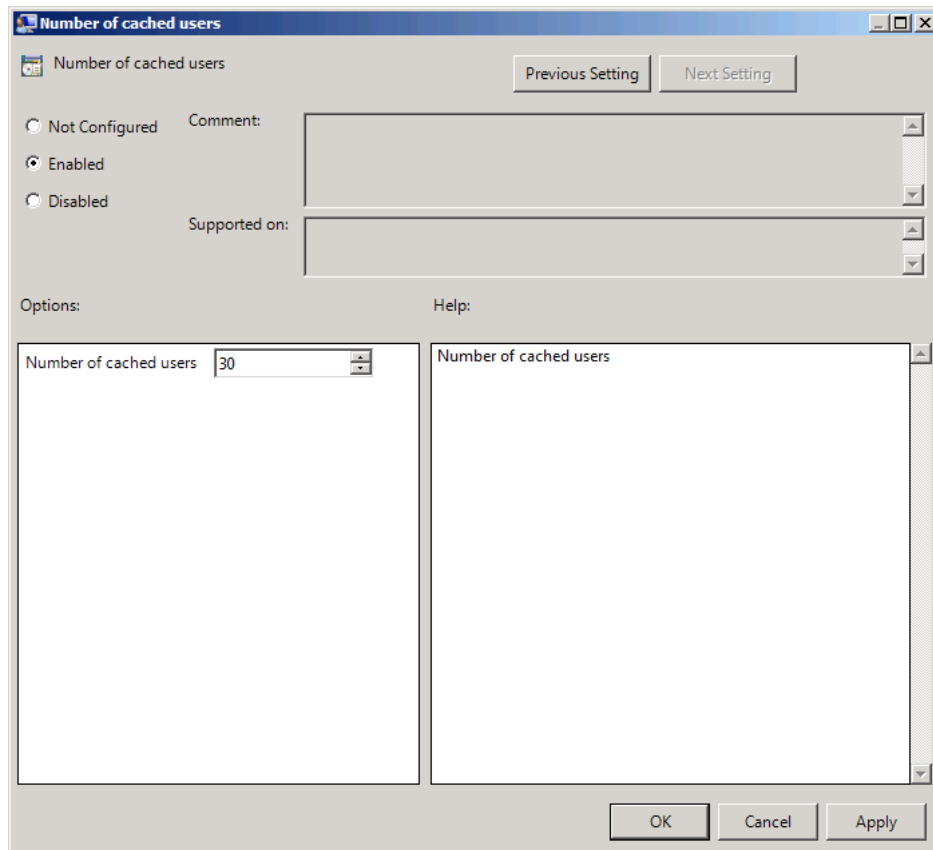


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: LockAccountOnFailedLogon (REG_DWORD)

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

Number of Cached Users

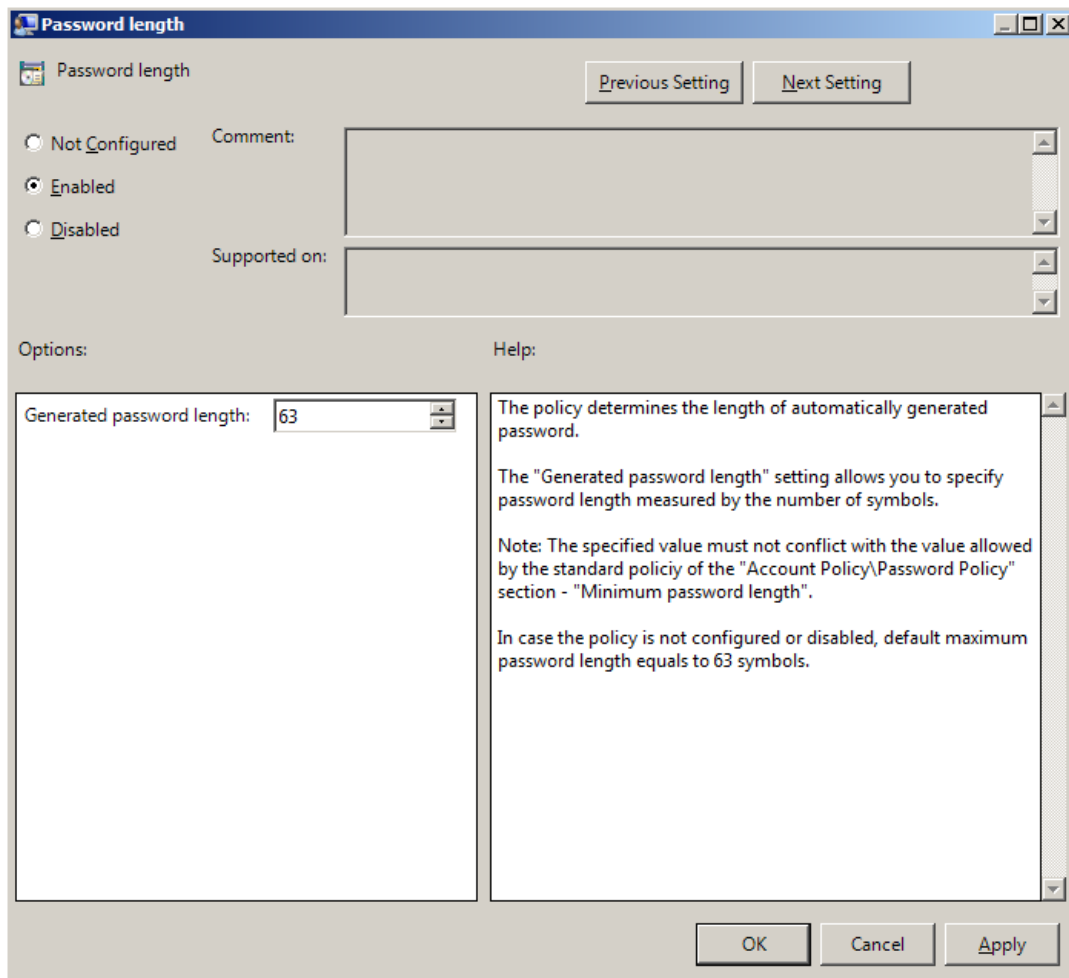
The **Number of cached users** policy allows you to define the number of user accounts that can be stored in the computer cache. When the number of cached user accounts reaches the number that is specified in the **Number of cached users** policy, then the latest user account is deleted from the computer 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 screenshot shows the 'PIN restrictions' dialog box. It has a title bar with the text 'PIN restrictions' 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:' section with two dropdown menus. At the bottom left, there is an 'Options:' section with a 'Minimum PIN length:' label and a spinner box containing the number '4'. To the right of this is a 'Help:' section with a text area containing the following text: 'PIN restrictions policy allows you to define minimum PIN code length for corresponding BSP types (Flash PIN, Universal Card, etc). To specify the minimum PIN code length, use the "Minimum PIN length" setting. In case the policy is not configured or is disabled, the minimum PIN length is 4 characters.' At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Apply'.


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 bottom right 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

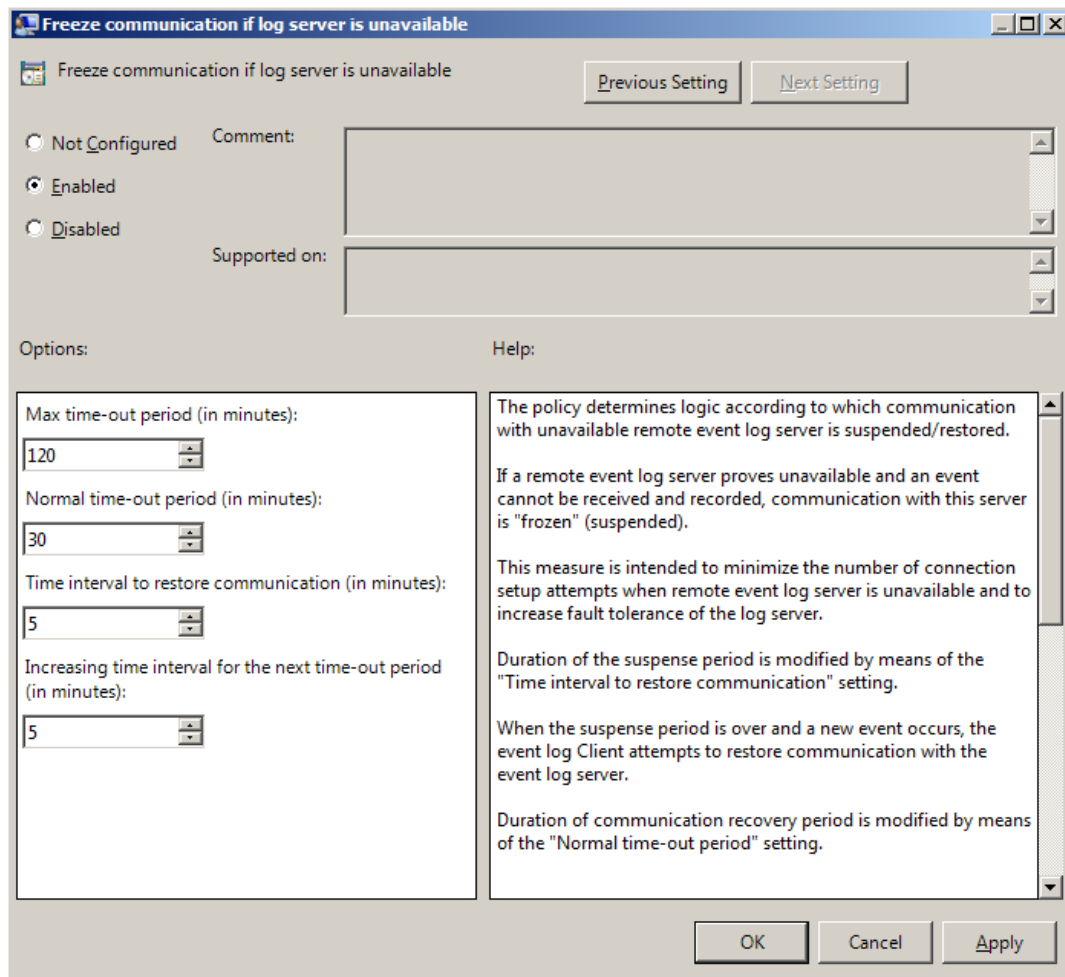
The **Event Log** section includes policies allowing you to determine logging settings.

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;

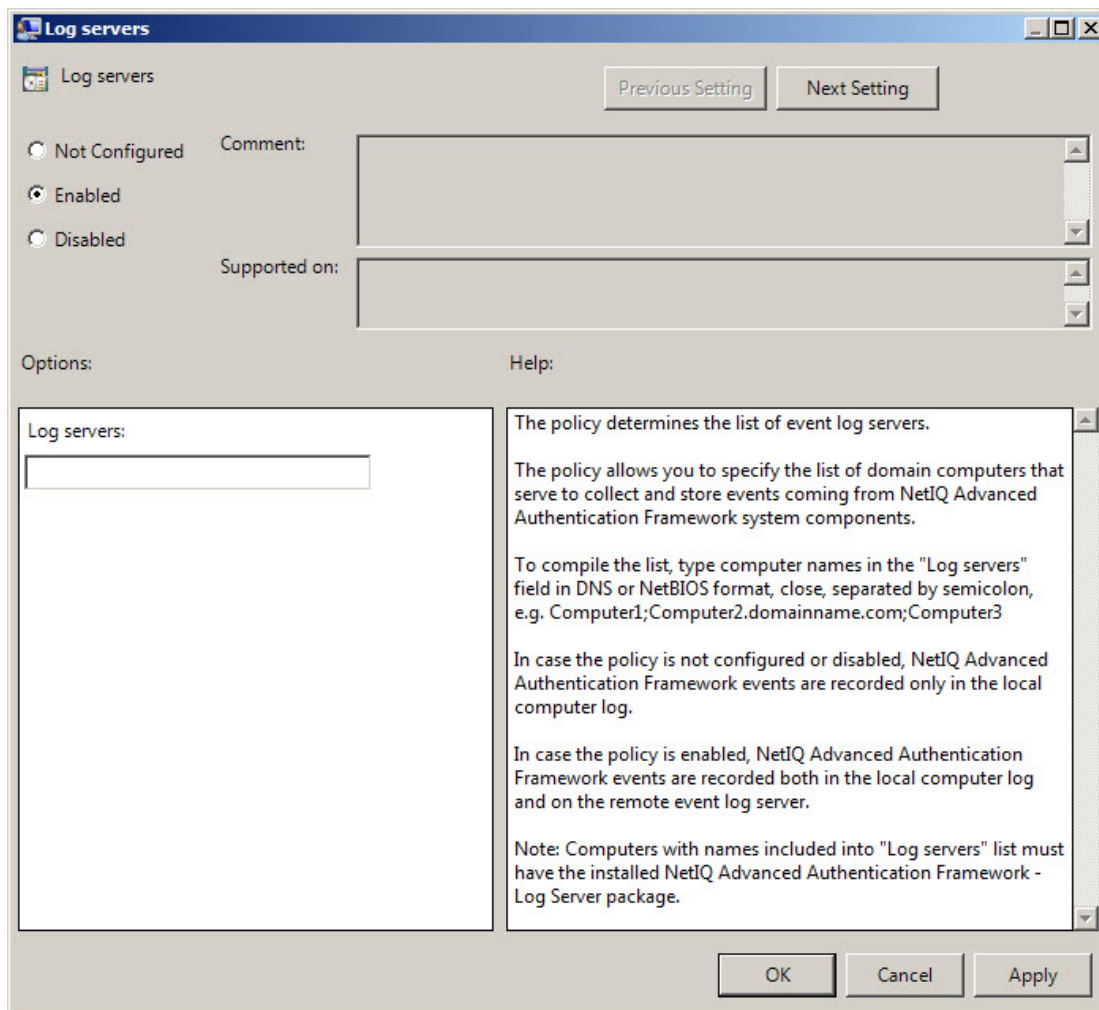
Normal time-out period (in minutes): 30;

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

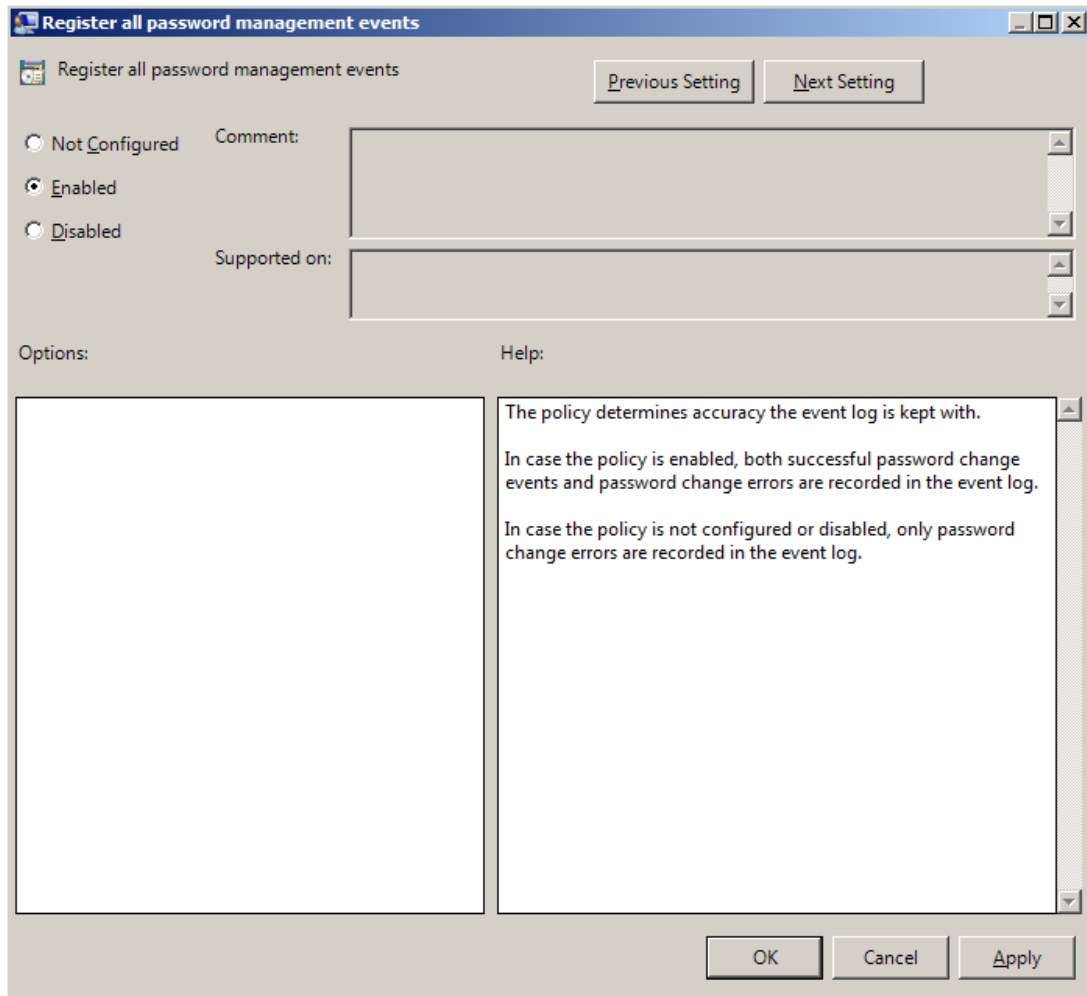
Computer1, Computer2, Computer3 is the list of the defined log servers

 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.



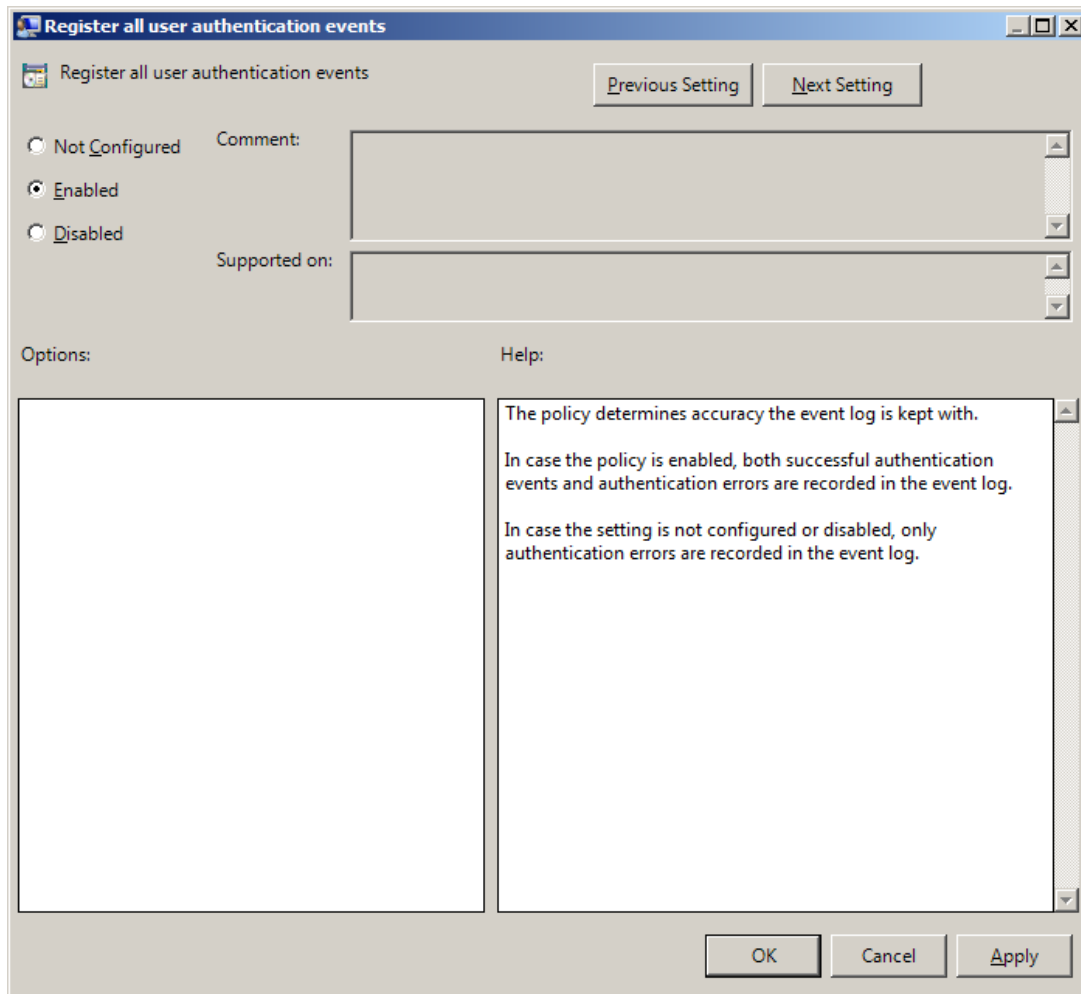
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: PasswordManagement_AllEvents (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled

 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.

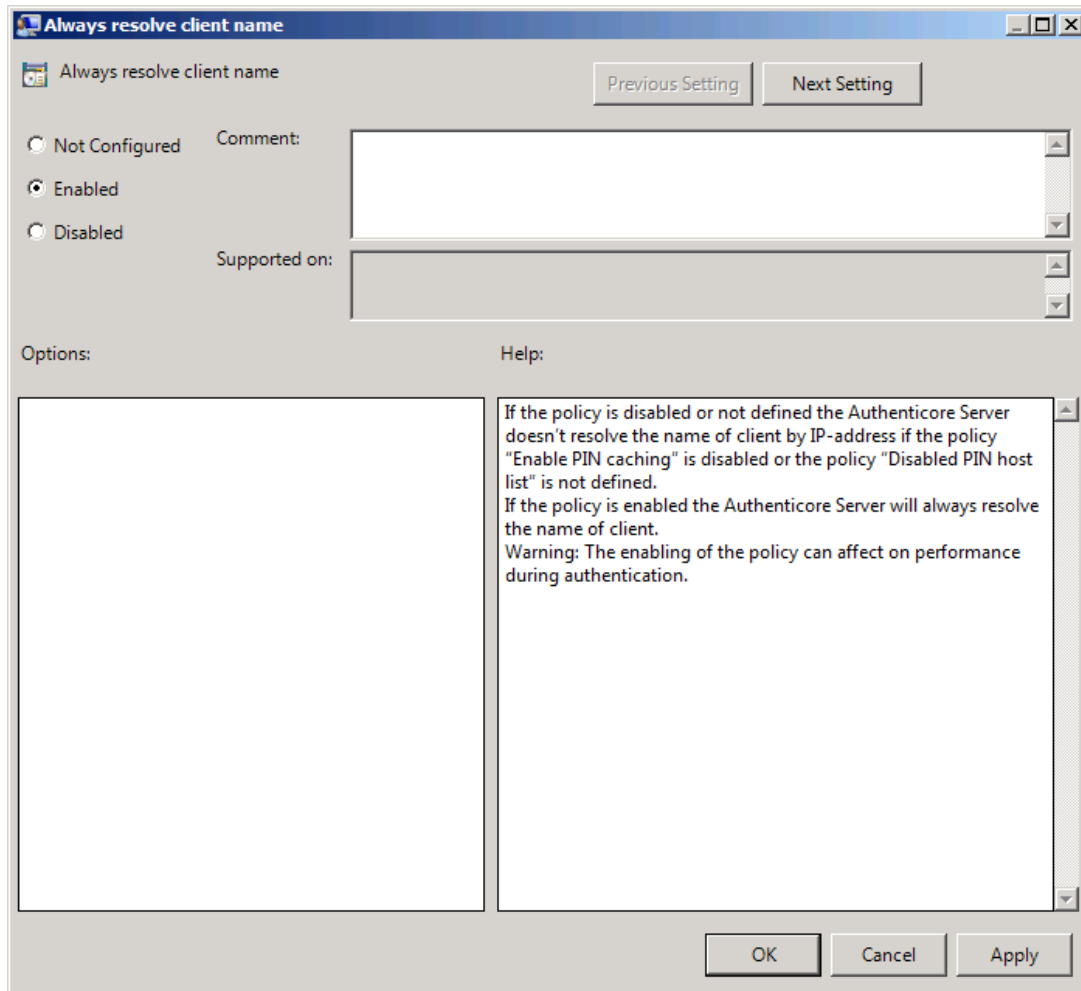
It includes:

- [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.

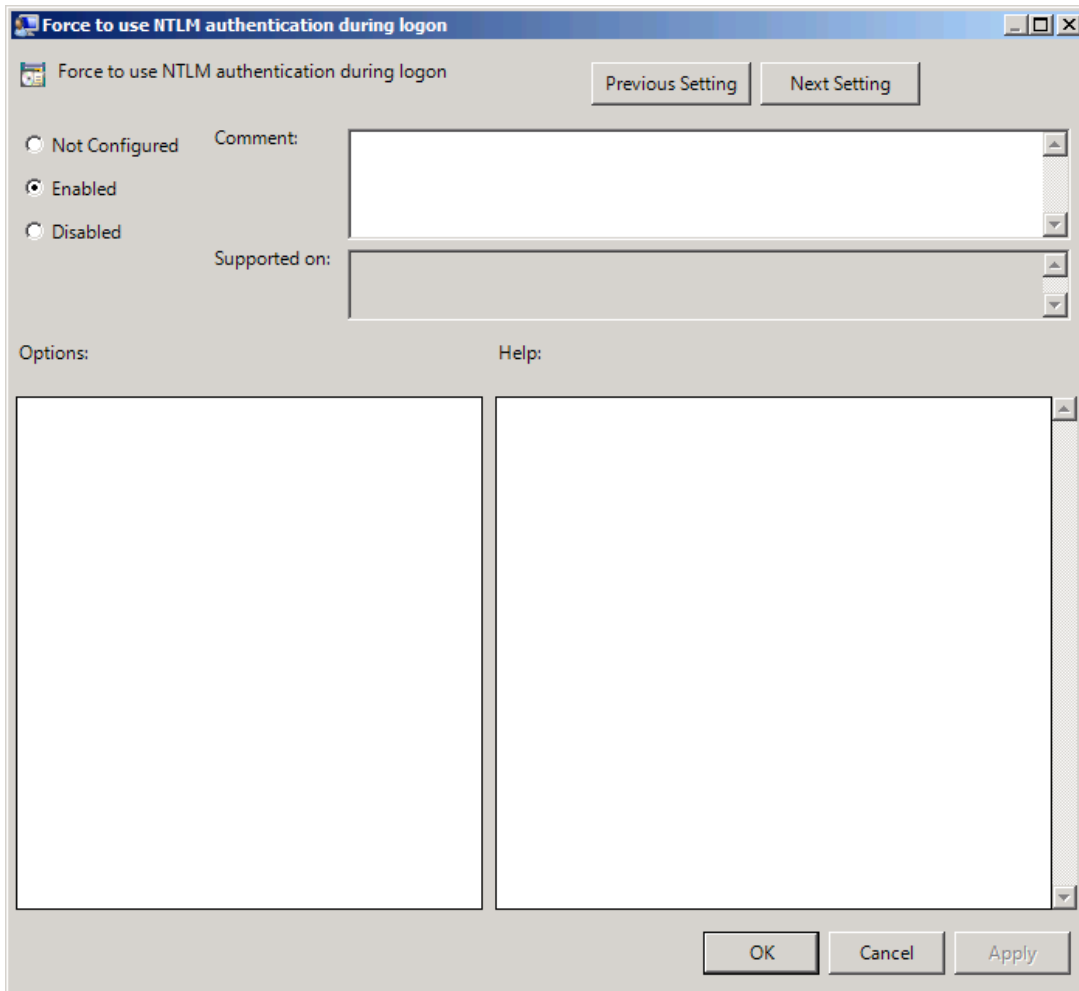


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: AlwaysResolveClientName (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled

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

Force to use NTLM authentication during logon

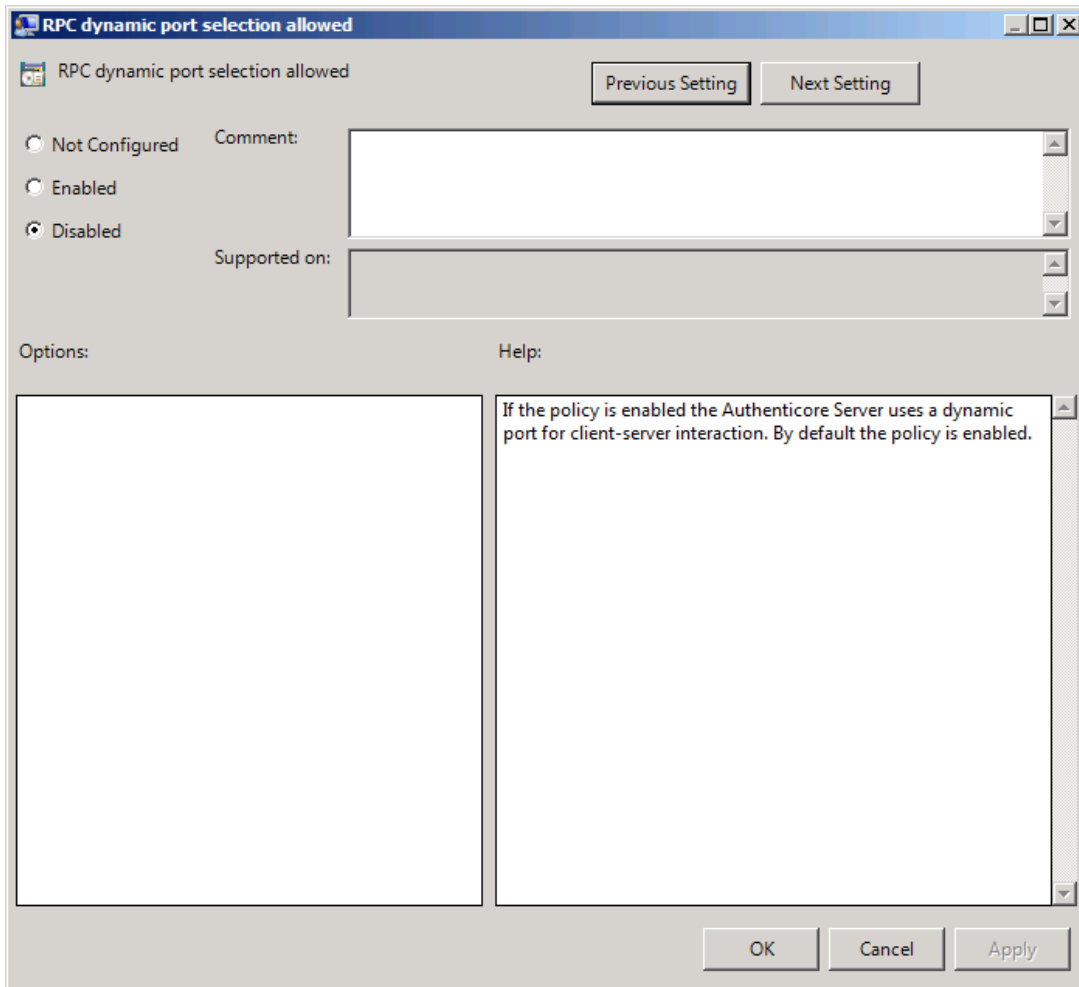
If the **Force to use NTML authentication during logon** policy is enabled, NTML authentication will be automatically used during logon.



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.

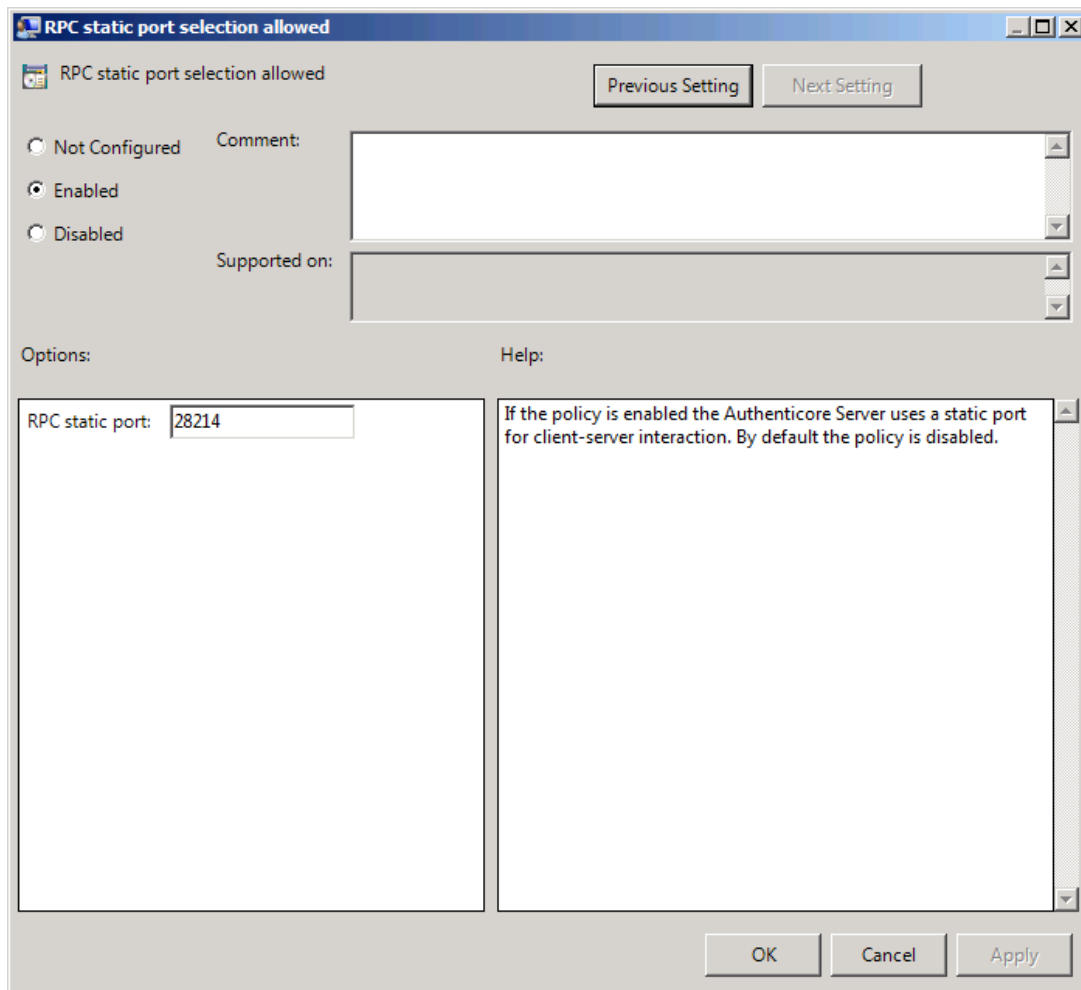


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: RpcDynamicPortAllowed (REG_DWORD)
value: 0x00000001 (1),
1 means that the policy is enabled


- ✖ 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.



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

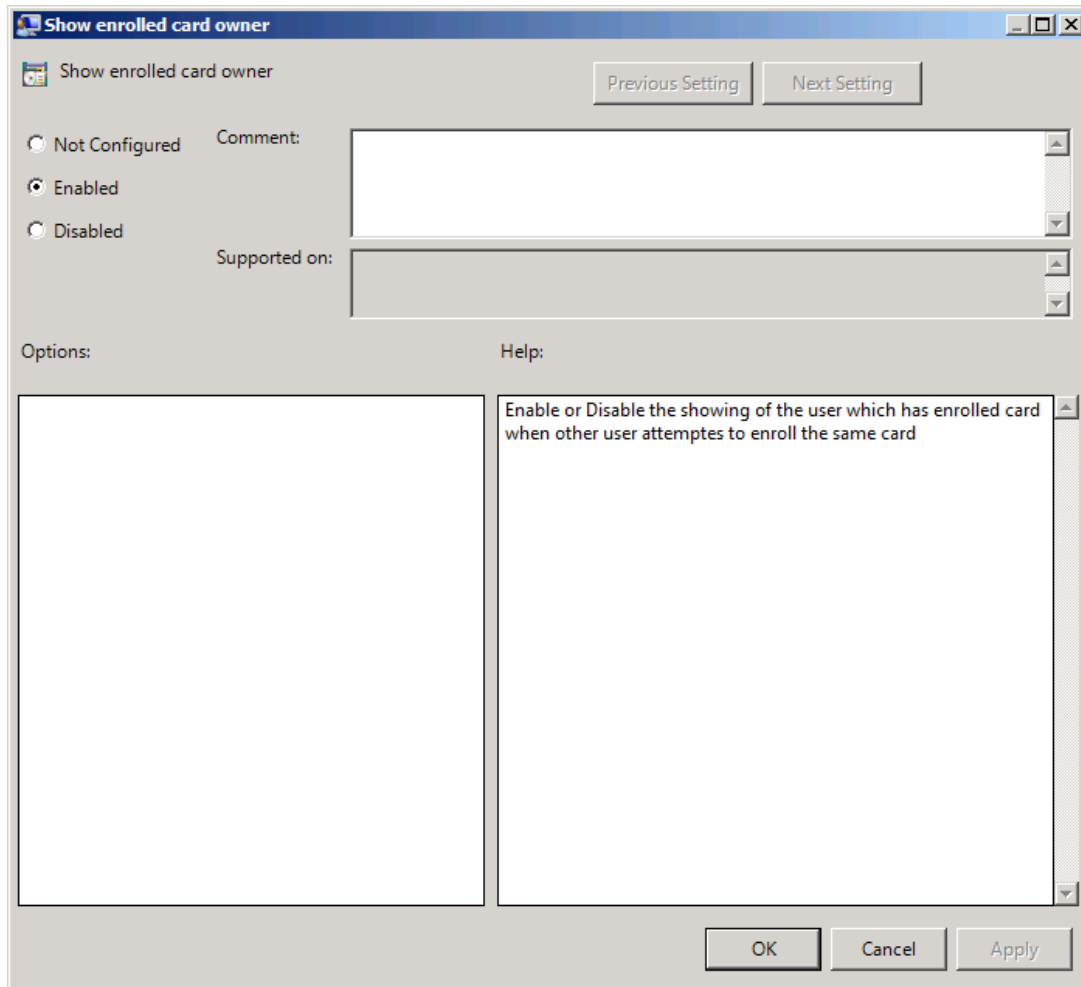
The **Runtime Environment** section includes a policy allowing to enable or disable showing of the user who has enrolled card.

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.

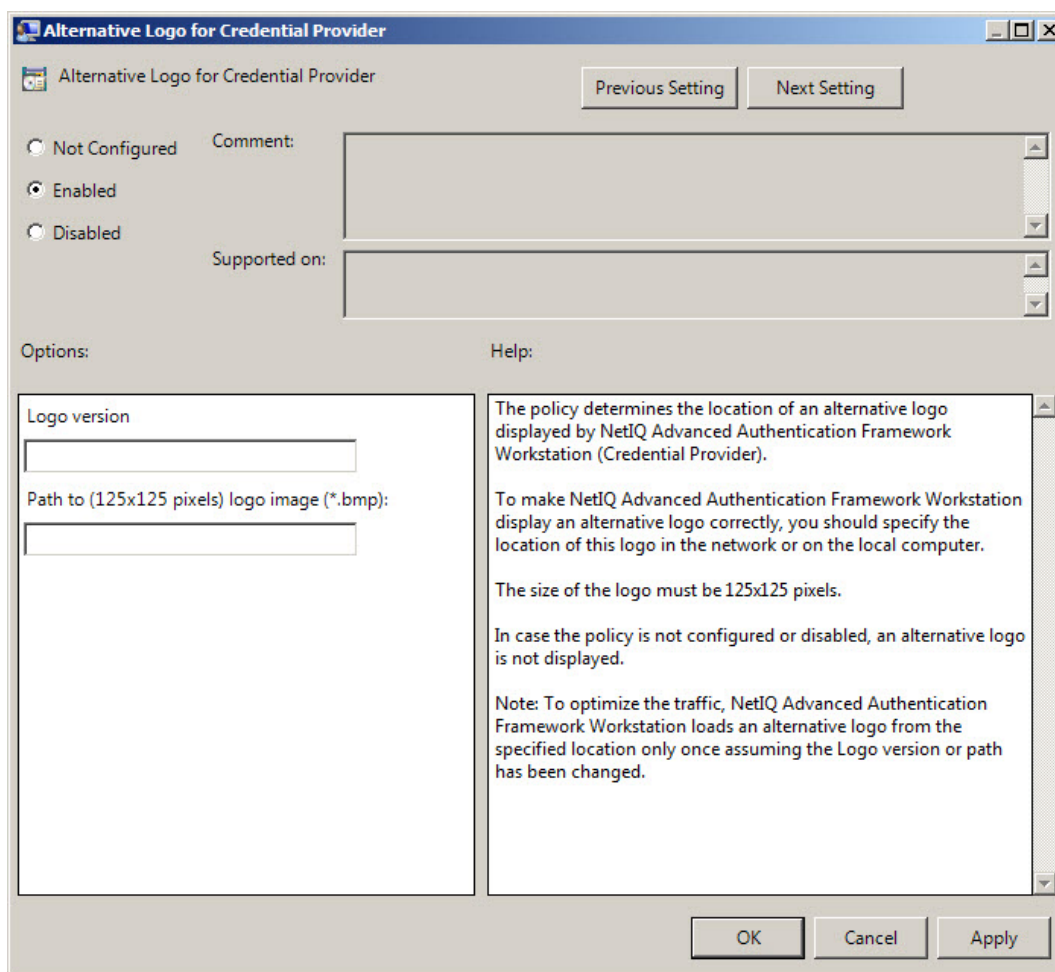
It includes:

- [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.



The screenshot shows the 'Alternative Logo for Credential Provider' dialog box. It has a title bar with the text 'Alternative Logo for Credential Provider' and standard window controls. Below the title bar are 'Previous Setting' and 'Next Setting' buttons. The main area contains three radio buttons: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. To the right of these buttons is a 'Comment:' text box and a 'Supported on:' dropdown menu. Below these are two sections: 'Options:' and 'Help:'. The 'Options:' section has two text boxes: 'Logo version' and 'Path to (125x125 pixels) logo image (*.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 (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.' At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

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: CPLogo (REG_SZ)

CPLoVersion (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:" text box. In the "Options:" section, there are 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):". To the right of the "Options:" section is a "Help:" text box containing explanatory text. At the bottom of the dialog are "OK", "Cancel", and "Apply" buttons.

Alternative Logo for GINA and Wizard

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on:

Options: Help:

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

OK Cancel Apply

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

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:

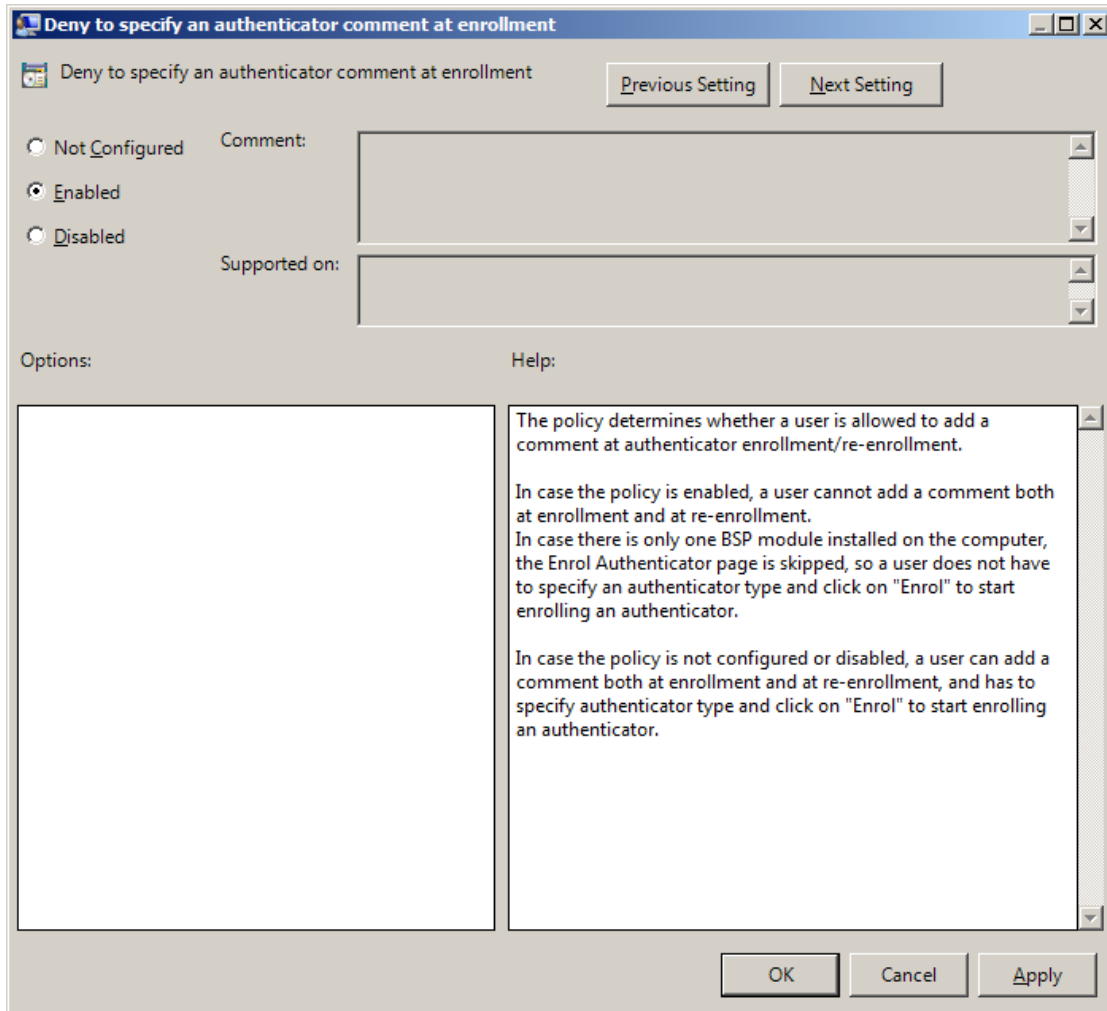
- small-size logo: 406x85 pixels;
- medium-size logo: 451x85 pixels;
- large-size logo: 495x85 pixels.

 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)

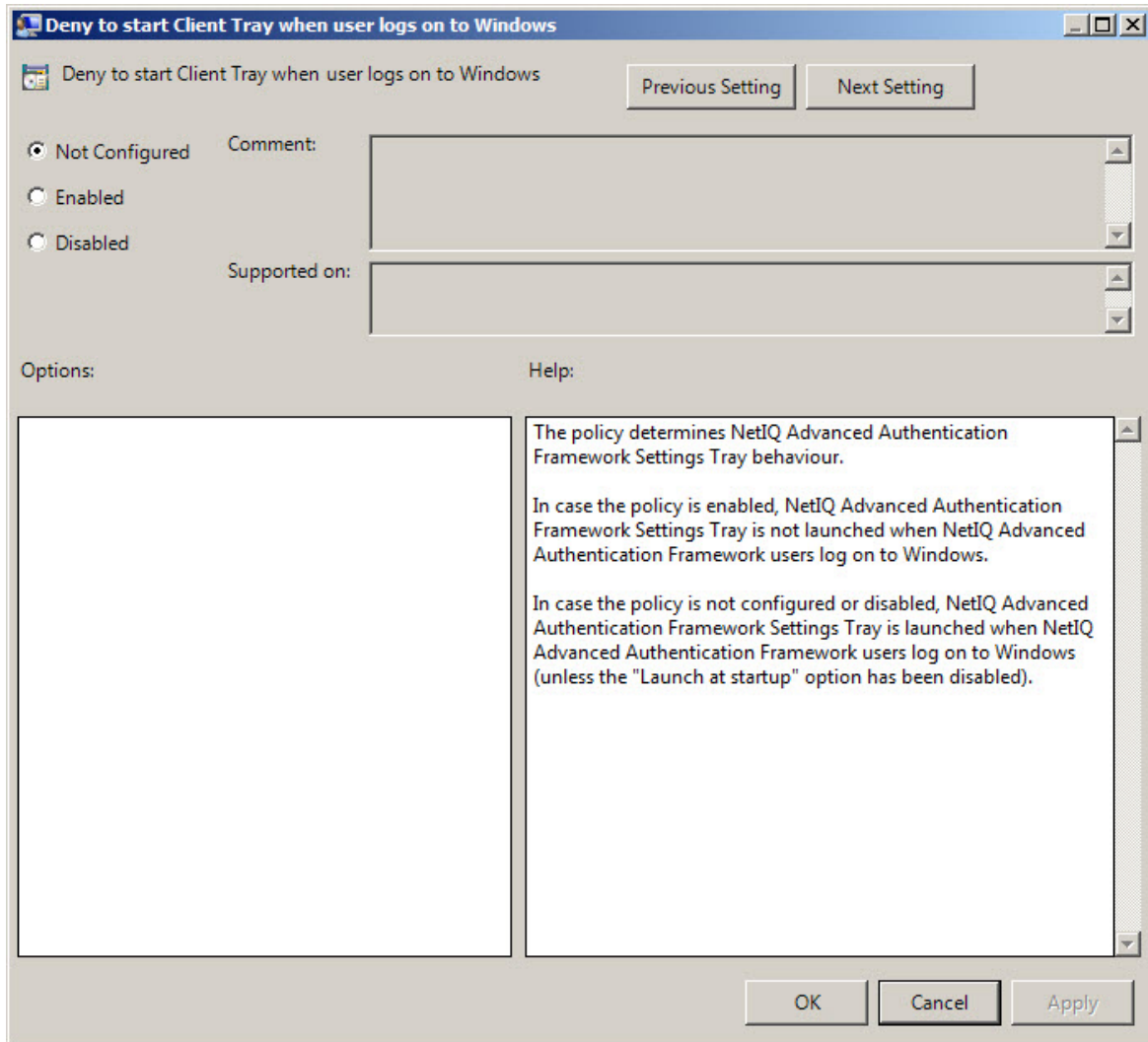
value: 0x00000001 (1)

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.



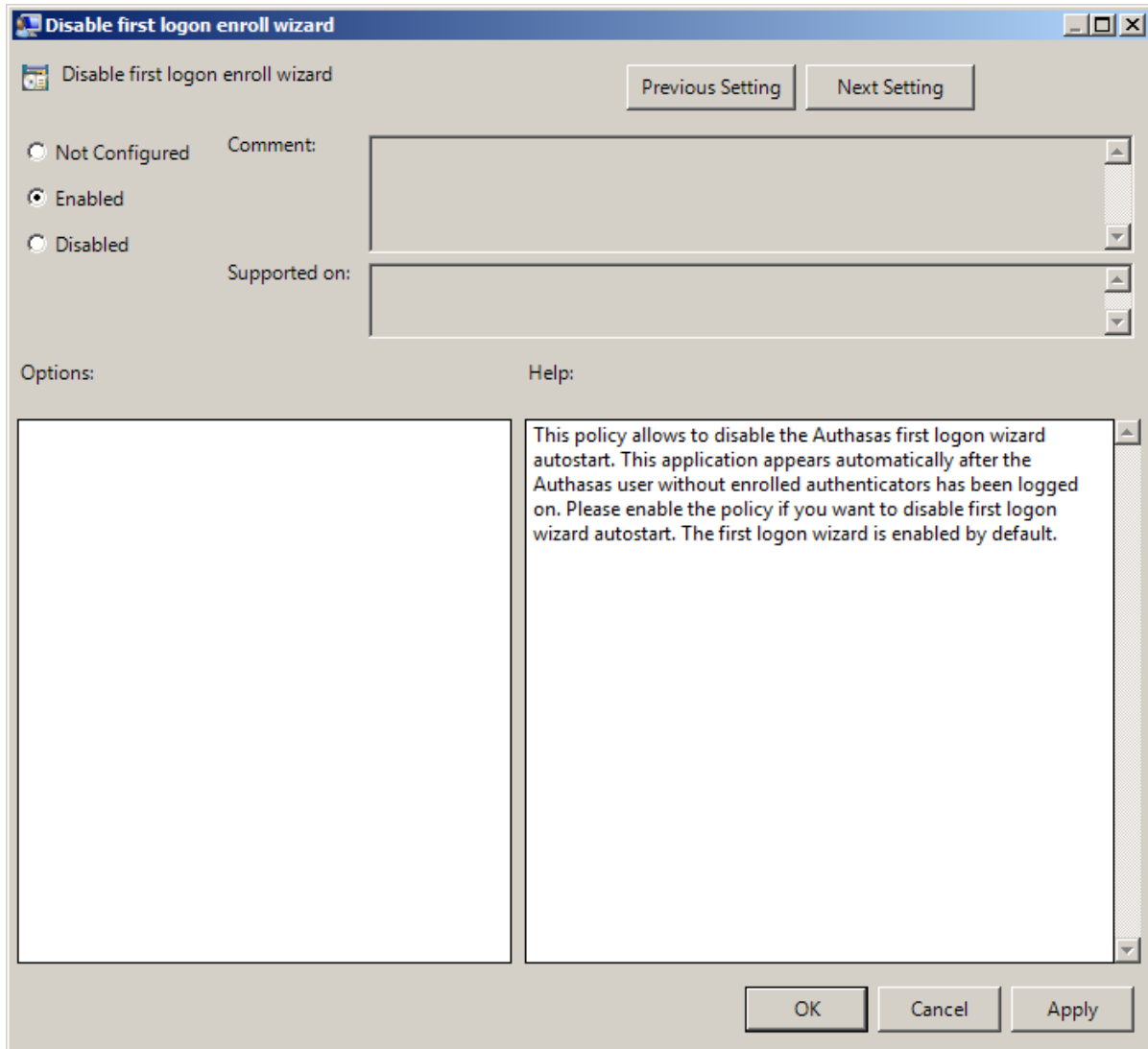
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
parameter: DenyClientTrayAutoStart (REG_DWORD)
value: 0x00000001 (1)
1 means that the policy is enabled

 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)

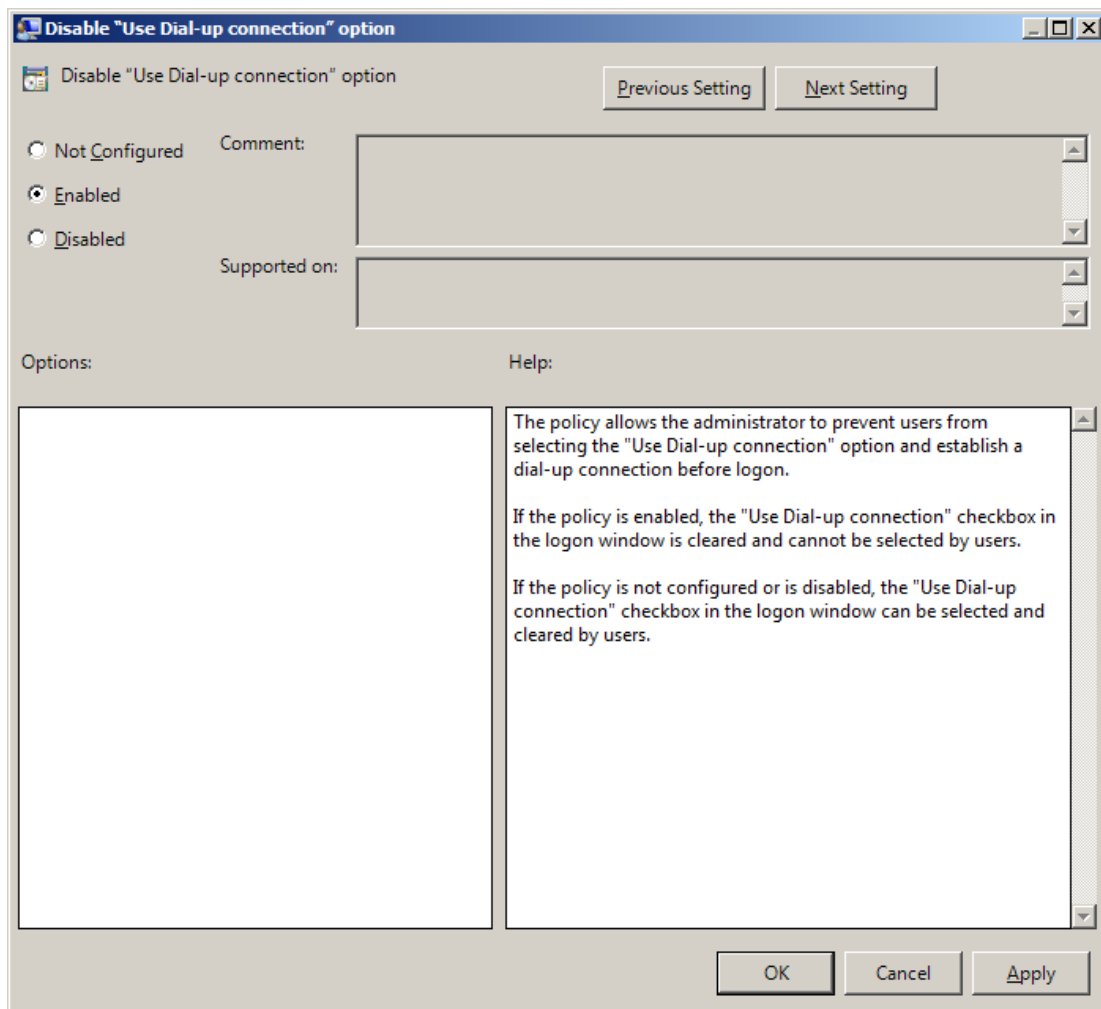
1 means that the policy is enabled

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)

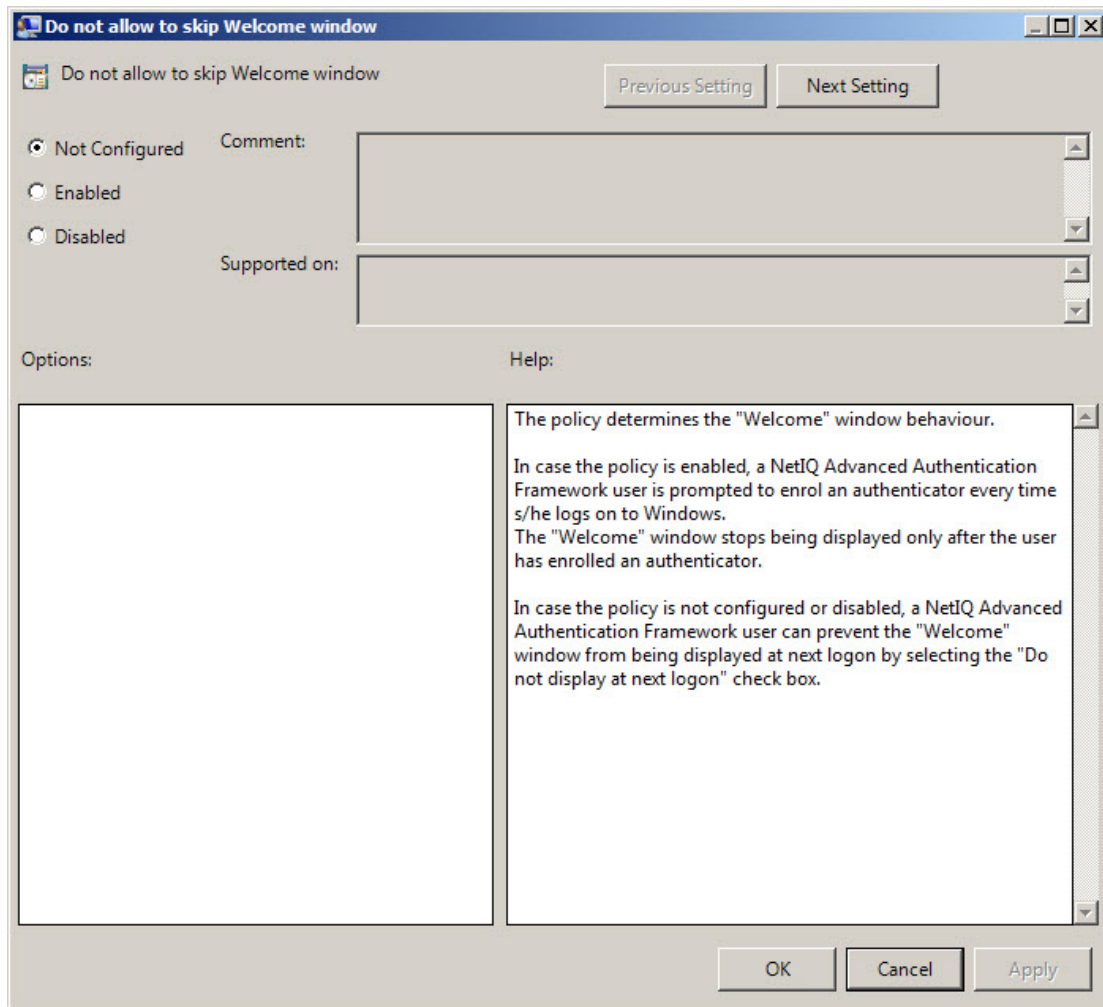
value: 0x00000001 (1)

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.

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

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.

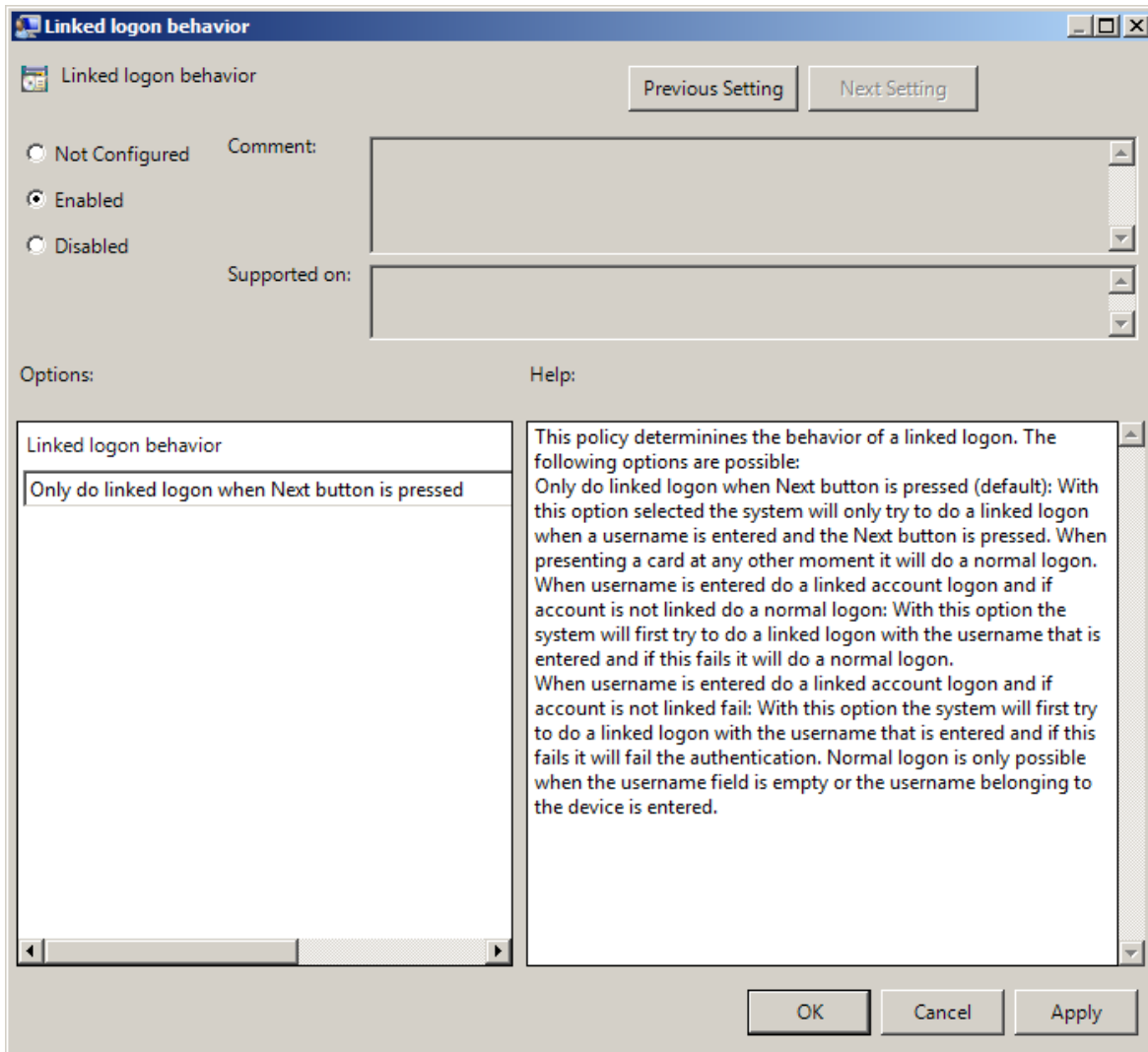
The screenshot shows a Windows-style dialog box titled "Lifetime of notification about password reset". At the top right are "Previous Setting" and "Next Setting" buttons. Below the title bar, there are three radio buttons: "Not Configured", "Enabled" (which is selected), and "Disabled". To the right of these is a "Comment:" text box. Below the radio buttons is a "Supported on:" text box. Under the "Options:" label, there is a numeric spinner box set to "14" with the label "Lifetime of notification about password reset (in days):". To the right of the spinner 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 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.

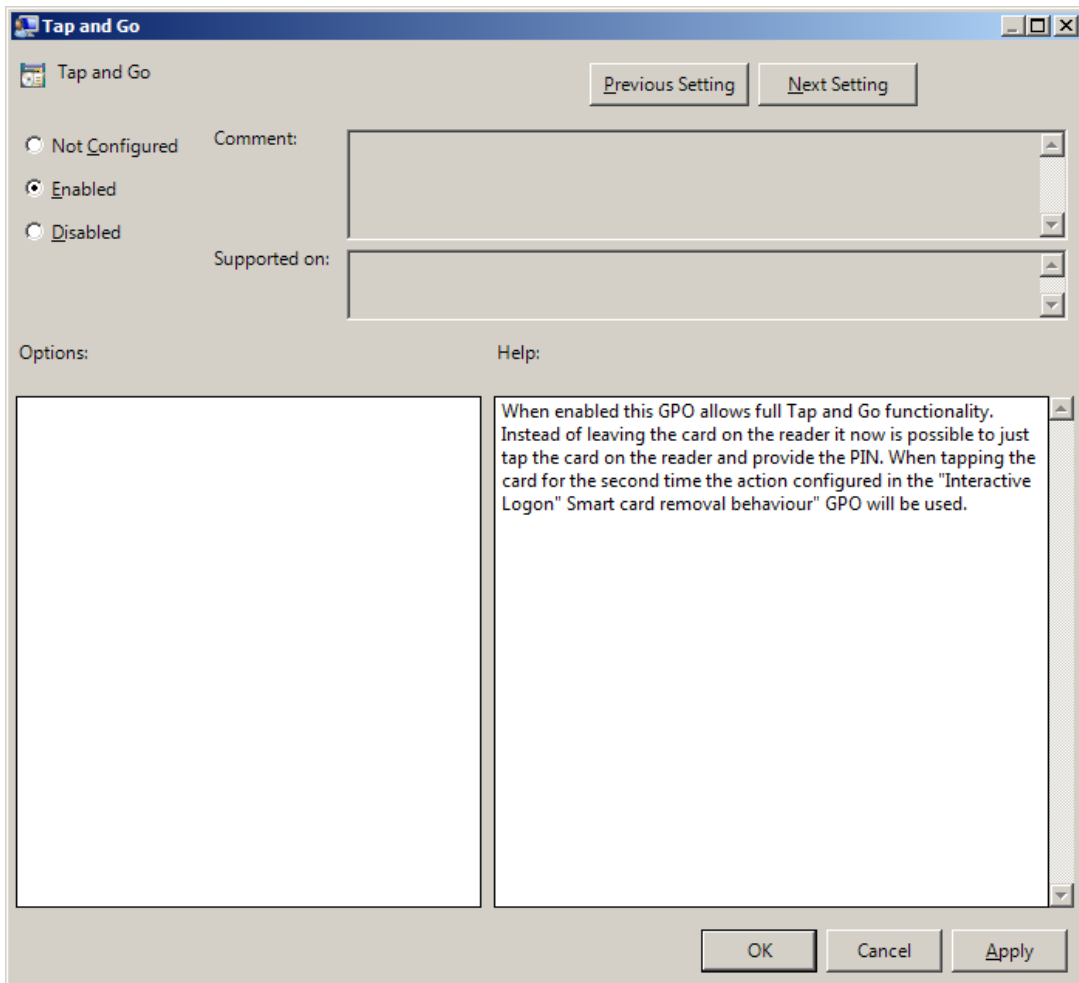


HKEY_LOCAL_MACHINE\SOFTWARE\Policies\NetIQ\NetIQ Advanced Authentication Framework
 parameter: LinkedLogonBehavior (REG_DWORD)
 value: 0x00000000 (0), 0x00000000 (0), 0x00000000 (0)
 0 means that the policy is enabled

 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



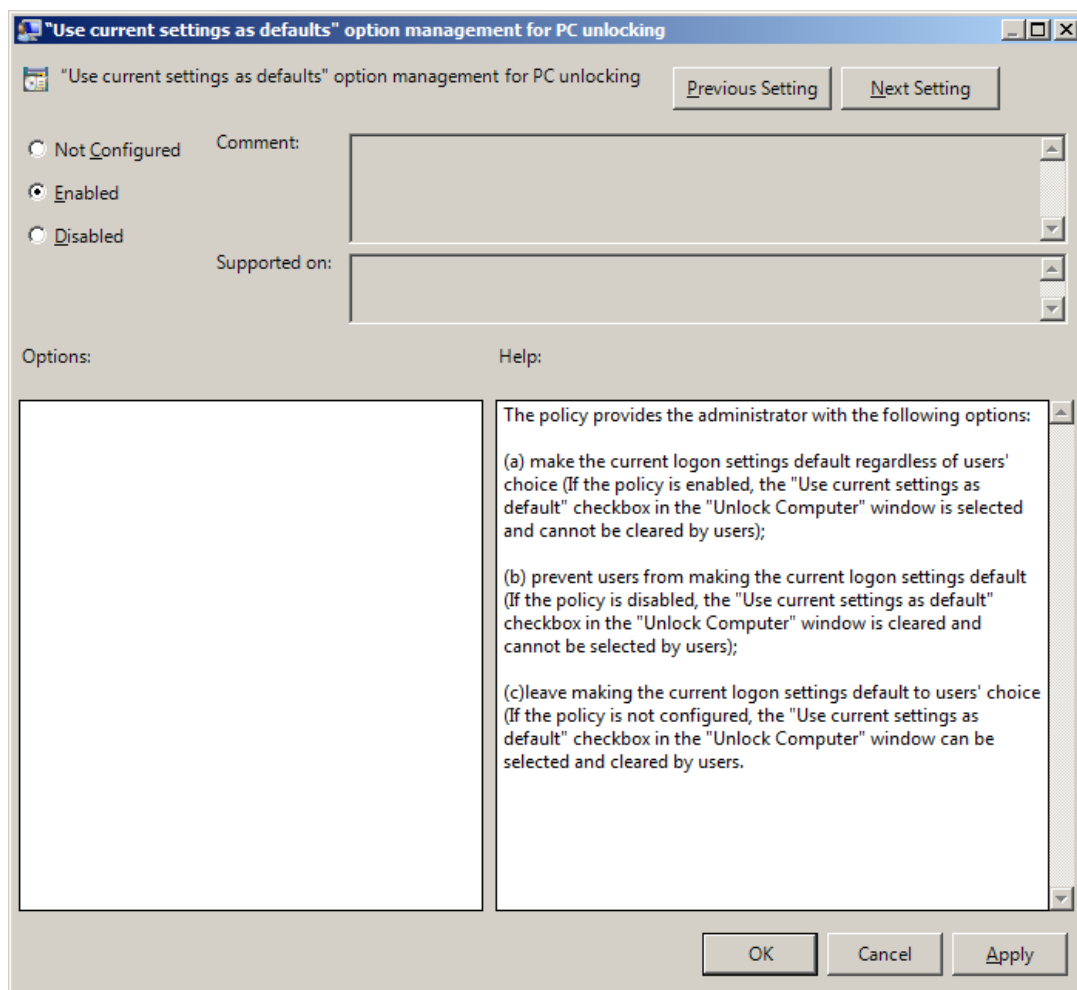
If the policy is not configured or is disabled, user cannot take the card from the reader until the Logon process is finished.

"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.

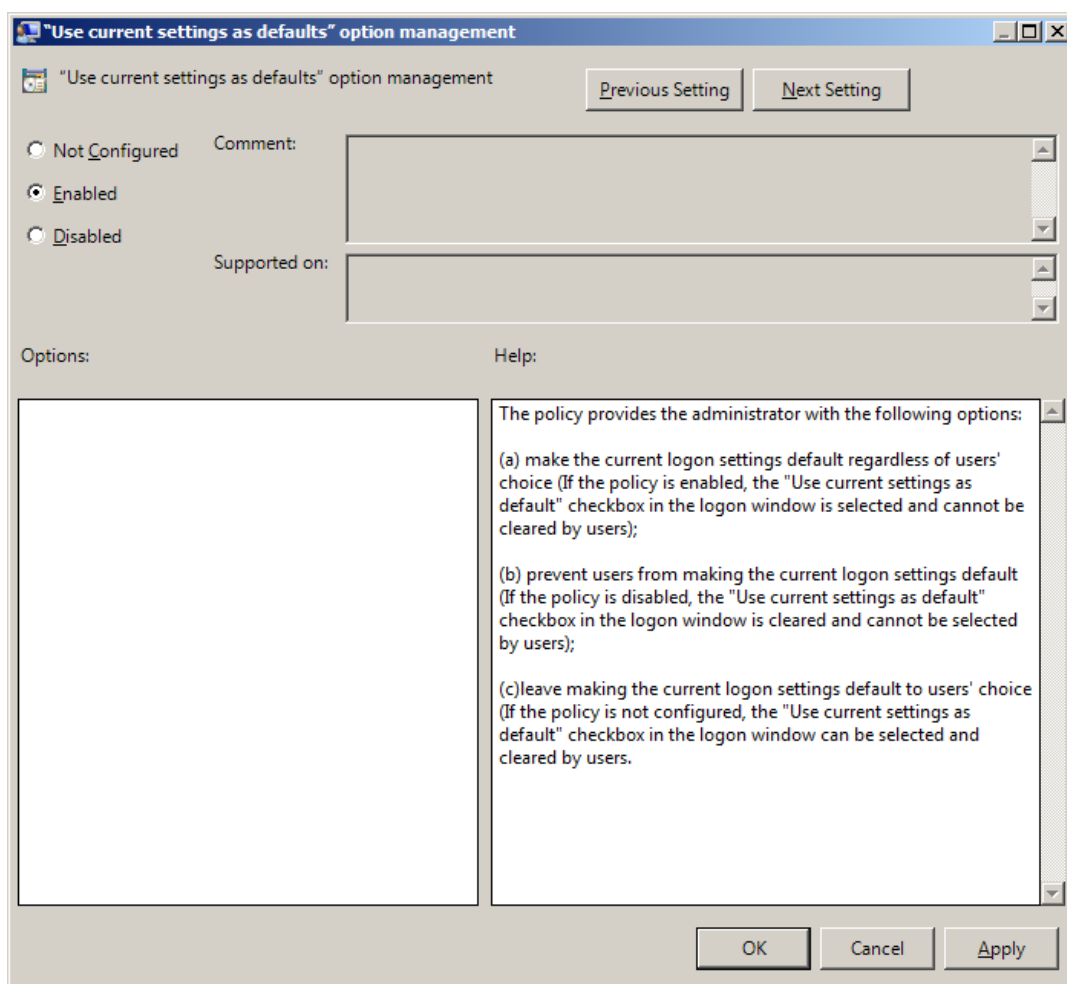
 If the policy is not configured, the **Use current settings as defaults** option is enabled and can be selected or canceled by users.

"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

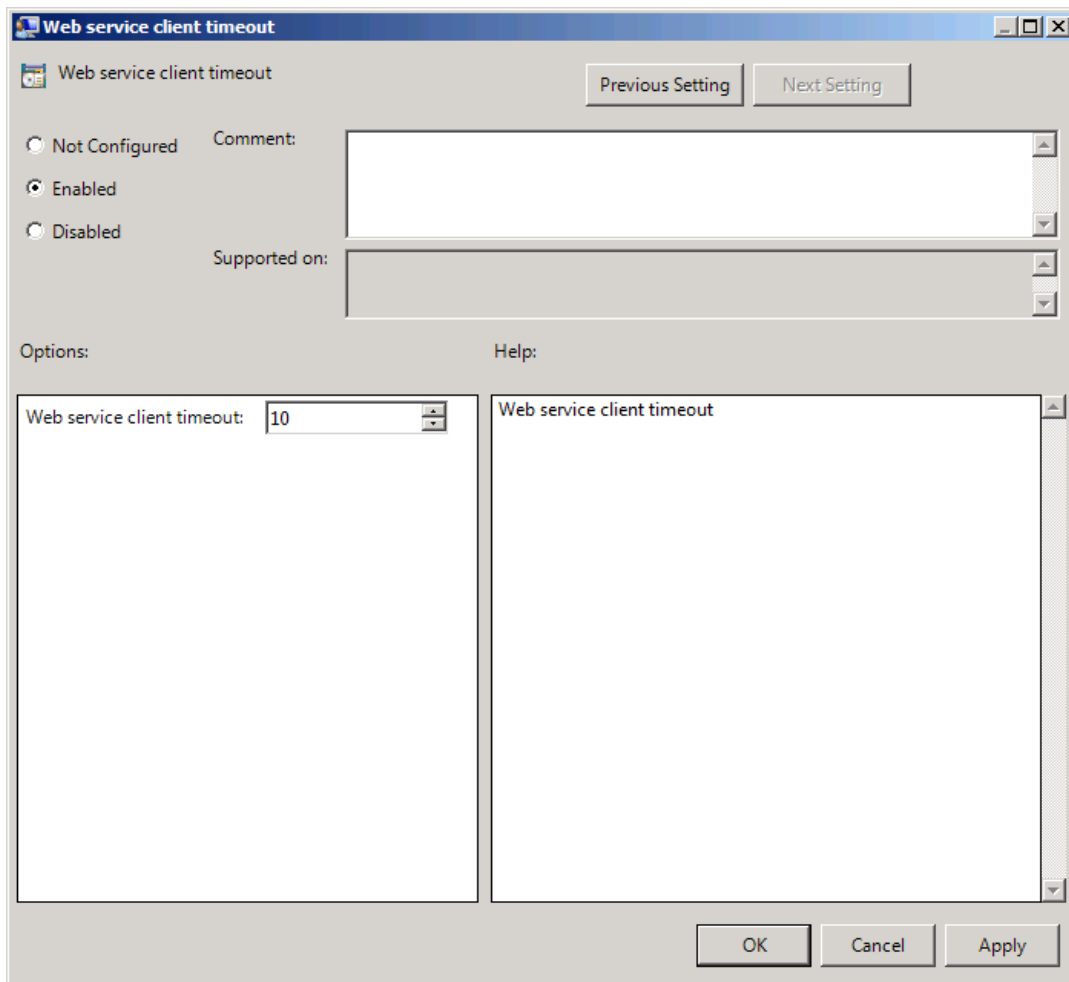
If the policy is enabled, the **Use current settings as defaults** option is always enabled and cannot be canceled by users.

 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.



The screenshot shows a Windows-style dialog box titled "Web service client timeout". At the top right, there are "Previous Setting" and "Next Setting" buttons. 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 box. Below the radio buttons is a "Supported on:" dropdown menu. Underneath, there are two sections: "Options:" and "Help:". The "Options:" section contains a label "Web service client timeout:" followed by a spinner box set to the value "10". The "Help:" section contains a label "Web service client timeout" and a large empty text area. At the bottom right, there are three buttons: "OK", "Cancel", and "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. The main area is divided into several sections:

- ADAM Settings:** Includes radio buttons for 'Not Configured', 'Enabled' (selected), and 'Disabled'. To the right is a 'Comment:' text box.
- Supported on:** A list box for selecting supported operating systems.
- Options:** A section containing two sub-sections:
 - LDAP path to root element:** A text box containing 'CN=NAAF' and a spin box for 'ADAM servers port number' set to '50000'.
 - Help:** A text box containing the text 'Configure if ADAM / AD-LDS is used as repository.'.

Navigation buttons 'Previous Setting' and 'Next Setting' are located at the top right. Action buttons 'OK', 'Cancel', and 'Apply' are located at the bottom right.

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 a Windows-style dialog box titled "Repository". At the top right, there are "Previous Setting" and "Next Setting" buttons. 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 box. Below the radio buttons is a "Supported on:" dropdown menu. In the "Options:" section, there is a "Repository Type" dropdown menu with "ADAM instance" selected. To the right of this is a "Help:" text box containing the following text: "Choose to use native Active Directory or ADAM / AD-LDS as the NetIQ repository. When Native Directory is used and the schema is not extended please configure the AD Settings GPO (AAA_REPOSITORY_AD.adm). If ADAM is chosen make sure the ADAM Settings GPO (AAA_REPOSITORY_ADAM.adm) is also configured." At the bottom right, there are "OK", "Cancel", and "Apply" buttons.

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

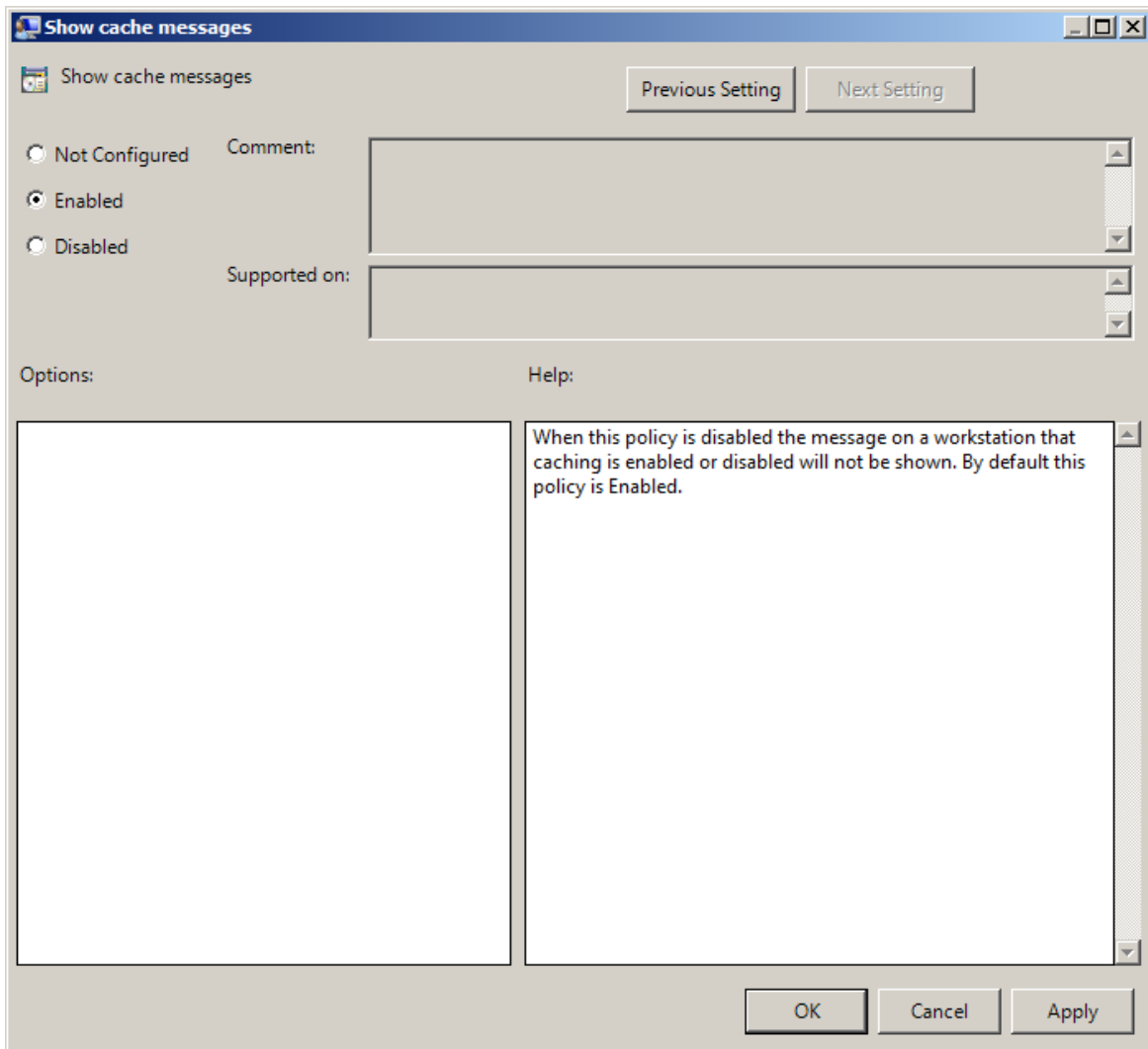
The **UI Look & Feel** section includes policies designed for terminal clients. The **UI Look & Feel** section is located in **Group Policy Management Editor** under **User Configuration -> Policies -> Administrative Templates: Policy definitions -> NetIQ Advanced Authentication Framework**.

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.

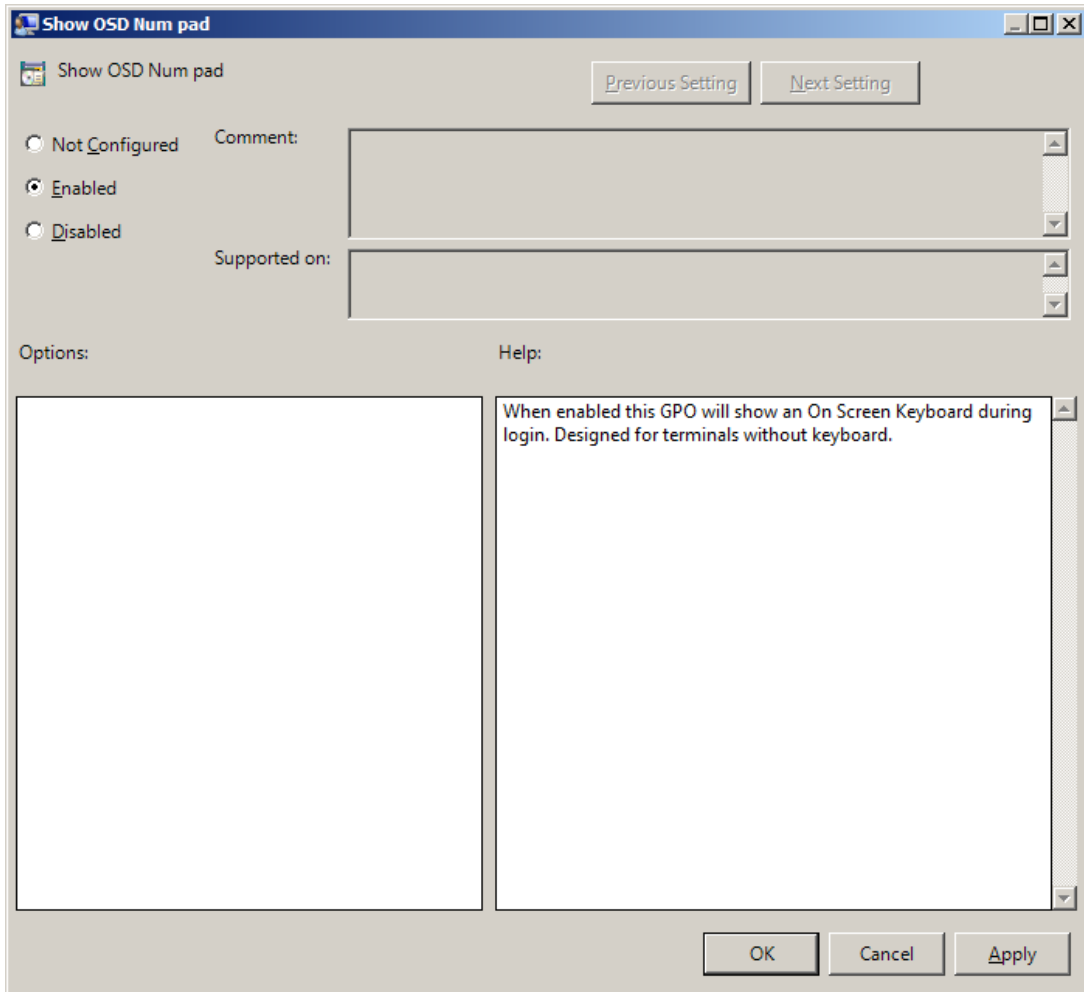


By default this policy is enabled.

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

Index

A

Account 23, 26
Active Directory 7, 73, 76
Administrator 1
Authentication 1, 4-5, 10, 12, 14-15, 17-20, 22-23, 25-26, 29, 33-34, 36-37, 39-42, 44-45, 48, 50, 52-53, 55-56, 58, 60, 62, 64, 66-68, 70, 72, 74-76, 78-80
Authenticator 4-5, 9-10, 52
Authenticore server 10

C

Caching 16, 19
Card 28, 43
Client 5, 19, 22, 41-42, 49-50, 62
Client Tray 6, 47, 53
Connection 56
Credential providers 5, 9, 12

D

Default 5, 9, 14
Device 60, 62
Dial-up 6, 47, 56
Domain 7, 51, 75

E

Error 23
Event Log 5, 31

G

Generate 5, 17
GINA 6, 47, 50

L

List 15, 21
Logo 6, 47-48, 50
Logon 4, 6, 55-56, 65, 67, 70

M

Microsoft Windows Server 2003 66

Microsoft Windows Server 2008 8

N

Network 6, 38

Notification 64

P

Password 5, 9, 17, 22, 26, 36

PIN 5, 9, 15, 20, 28-29, 38, 67, 71

Policy 1, 4, 8, 78

R

Remove 18

RTE 44, 62

S

Screen 7, 80

Security 5, 8-9, 14-15

Server 32, 38, 40, 42, 45

Settings 12, 45, 54, 68, 70, 74, 76

Software 79-80

Support 75

System 58

U

User 37, 78

W

Window 58

Windows 6, 8, 46, 50, 53, 58

Windows Vista 48

Workstation 6, 47