NetIQ Advanced Authentication Framework - Client

User's Guide

Version 5.1.0

Table of Contents

1

Table of Contents 2

Introduction 4

About This Document 4

NetIQ Advanced Authentication Framework™ Overview 5

About NetIQ Advanced Authentication Framework™ 5

NetIQ Advanced Authentication Framework™ Technology 6

NetIQ Advanced Authentication Framework™ Supported Features 6

Terms and Abbreviations 8

Authenticator 8

Enroll Authenticator 8

Re-enroll Authenticator 8

User Authentication 8

User’s Workstation 9

Getting Started 10

The First Logon 10

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2 11

Microsoft Windows Server 2003 12

Microsoft Windows 8/Microsoft Windows Server 2012 14

Enrolling Authenticator at First Logon 15

Testing Authenticator at First Logon 18

Logon Methods 20

Logon with Authenticator 21

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2 21

Microsoft Windows Server 2003 23

Microsoft Windows 8/Microsoft Windows Server 2012 25

Logon with Password 27

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2 27

Microsoft Windows Server 2003 29

Microsoft Windows 8/Microsoft Windows Server 2012 31

Remote Logon Via Dial-Up Connection 32

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2 32

Microsoft Windows Server 2003 34

Microsoft Windows 8/Microsoft Windows Server 2012 36

Terminal Logon 38

Non-Network Logon 38

Automatic Logon 38

Managing Password 40

Changing Password 40

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2 40

Microsoft Windows Server 2003 42

Getting Password 44

NetIQ SSPR Support 44

Caching Authenticators 46
Locking/Unlocking Computer 47
Locking computer 47
Unlocking Computer 48
NetIQ Advanced Authentication Framework Run As Tool 50
Authorization By Authenticator 51
NetIQ Advanced Authentication Framework Client Tray Settings 52
General Settings 53
Language Settings 54
Password Authorization 55
Cache Management Settings 56
Troubleshooting 57
Support Information in Client Tray Menu 58
Cannot Get Authorized 61
Cannot Change Password 63
Cannot Enroll Authenticator 65
Cannot Save Authenticator 66
Index 67

Introduction

About This Document

Purpose of the Document

This User’s Guide is intended for all user categories and describes how to use the client part of NetIQ Advanced Authentication Framework solution. This document describes the work used in corporate environment.

Document 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.

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

❓ **Tips.** This sign indicates recommendations.

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

NetIQ Advanced Authentication Framework™ Overview

In this chapter:

- About NetIQ Advanced Authentication Framework TM
- NetIQ Advanced Authentication Framework TM Technology
- NetIQ Advanced Authentication Framework TM Supported Features

About NetIQ Advanced Authentication Framework™

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

Why choose NetIQ Advanced Authentication Framework™?

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

What is NetIQ Advanced Authentication Framework™?

NetIQ Advanced Authentication Framework™ is a system made up of 3 sets of components (Server components, Administrator components and Client components). Working together these components secure your access to data and allow you to forget about your account password.

What is going to happen to my password?

NetIQ Advanced Authentication Framework™ leaves NetIQ administrator a choice to determine whether to allow the use of account password or disable it. If the use of account password is enabled, you can log on with it just like you would without NetIQ Advanced Authentication Framework™.

If the use of account password is disabled, you can log on with an authenticator only. In this case your account password is changed automatically once you have enrolled an authenticator. Later on the complex random password is generated and changed at regular intervals specified by NetIQ administrator. **Passwords are unknown to everyone, including NetIQ administrator.**

NetIQ Advanced Authentication Framework™ Technology

NetIQ Advanced Authentication Framework™ technology relies on authenticator.

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

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

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

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

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

NetIQ Advanced Authentication Framework™ Supported Features

Supported Authenticator Types

- NetIQ Advanced Authentication Framework™ supports a wide range of authenticator types (biometric authenticators, smart cards, tokens, and one-time passcodes).

NetIQ Advanced Authentication Framework™ Supported Features

- You can enroll authenticator right after your first logon after NetIQ Advanced Authentication Framework has been installed;
- You can use different authenticator types (from the available ones) for logging on or unlocking your operating system instead of using weak and unsafe password;
- You can enroll several authenticators (depending on how much the administrator allows you to enroll), re-enroll or delete your authenticators (if you are permitted to);
- You can have your password changed (both, manual and on permission);
- You can execute files or run applications under another user's account using NetIQ Advanced Authentication Framework Run As tool;
- You can use authentication in the situation when you're outside of your corporate network or temporary work with network was planned (contact your NetIQ administrator in advance).

Terms and Abbreviations

In this chapter:

- Authenticator
- Enroll Authenticator
- Re-enroll Authenticator
- User Authentication
- User's Workstation

Authenticator

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

Enroll Authenticator

Enroll authenticator means to create an authenticator, “train” the system to recognize it and save the result to the database.

Re-enroll Authenticator

Re-enroll authenticator means to change the authenticator and save the changes to the database.

User Authentication

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

1. When authentication is required, the logon window is displayed and the user is prompted to submit an authenticator.
2. When the authenticators match, the user’s identity is successfully proven.

User’s Workstation

User’s workstation is a computer with installed “NetIQ Advanced Authentication Framework – Client” package and a hardware authentication device.

Getting Started

The purpose of this chapter is to provide an overview of the basic principles of the "NetIQ Advanced Authentication Framework – Client" functioning and to give the user a guidance in its initial setting for further successful operation.

ℹ The NetIQ Advanced Authentication Framework Client component is formerly known as NetIQ Advanced Authentication Framework Workstation component.

The First Logon

Once the "NetIQ Advanced Authentication Framework – Client" package has been installed on your computer, you can initially log on to Windows using your normal account password.

NetIQ Advanced Authentication Framework authentication becomes available to you once you have enrolled an authenticator.

ℹ The Logon procedure may differ depending on the operating system type you are using. Please select your operating system in the list below:

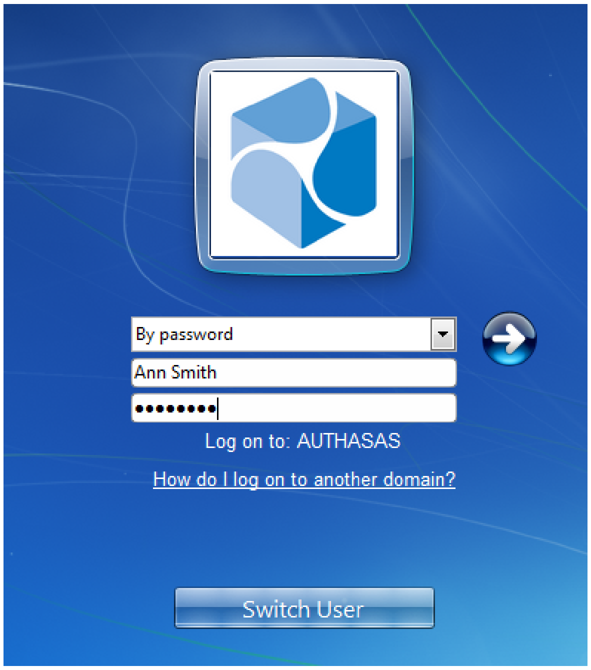
- Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows Server 2008/ Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003
- Microsoft Windows 8/Microsoft Windows Server 2012

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

1. Start your computer. From logon screen, press **[Ctrl]+[Alt]+[Del]** and select your user name if available or click **Switch User**.

2. Follow the steps below:

- Select **By Password** as a logon method and type your password.
- Click ➔ icon or press **Enter** to continue.



By password
Ann Smith
••••••••

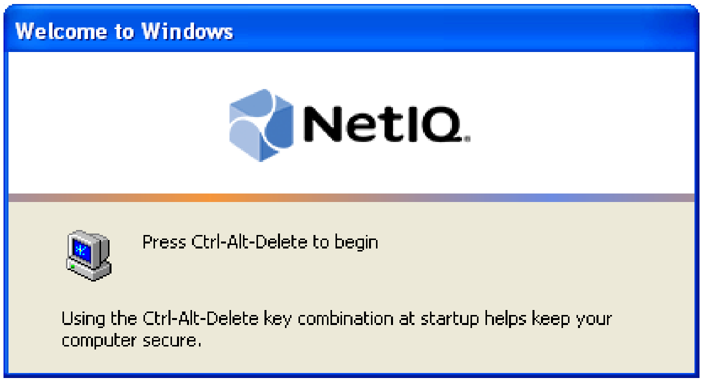
- Wait a few seconds until you are logged on to Windows. Once you are logged on, you can enroll your authenticator.

ℹ NetIQ administrator may allow you to cache authenticators. ***Caching*** means storing authentication and user data at a local storage. In such case the **Cache policy** notification is displayed after you have entered your password. See Caching Authenticators.

Microsoft Windows Server 2003

To log on with your account password:

1. Start your computer. When the **Welcome to Windows** window appears, press **[Ctrl]+[Alt]+[Del]**.

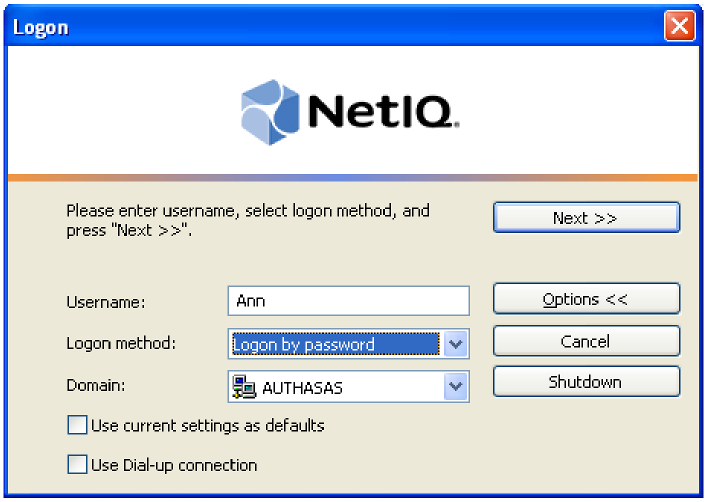


Welcome to Windows

Press Ctrl-Alt-Delete to begin

Using the Ctrl-Alt-Delete key combination at startup helps keep your computer secure.

2. The **Logon** window is displayed. From **Logon method** list, select **Logon by password**. Enter your username and password, press **Next >>**.



Logon

Please enter username, select logon method, and press "Next >>".

Username: Ann

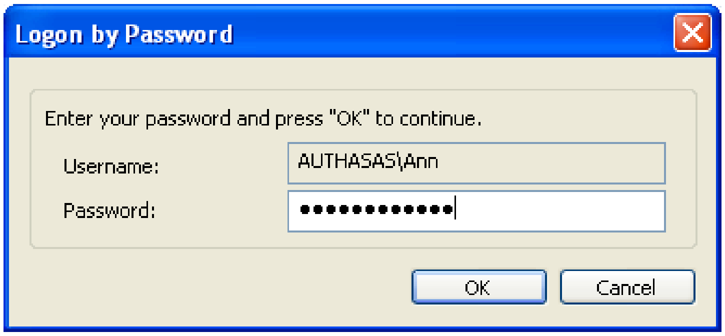
Logon method: Logon by password

Domain: AUTHASAS

□ Use current settings as defaults

□ Use Dial-up connection

3. The **Logon by Password** dialog is displayed. Type your account password in the **Password** box. Click **OK**.



Enter your password and press "OK" to continue.

Username: AUTHASAS\Ann

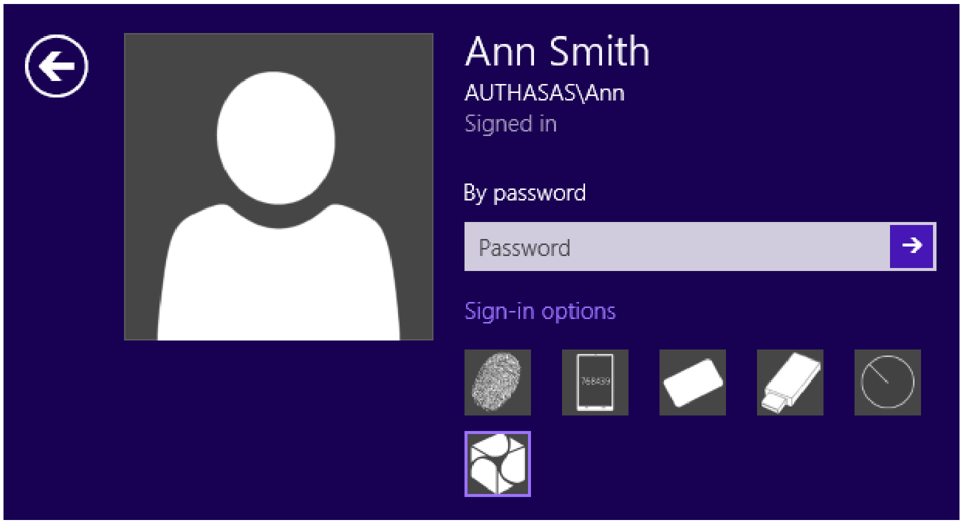
Password: ●●●●●●●●●●●●●

Microsoft Windows 8/Microsoft Windows Server 2012

1. Start your computer and select your user name.

2. Follow the steps below:

- Select **By Password** as a logon method and type your password.
- Click → icon or press **Enter** to continue.



Ann Smith

AUTHASAS\Ann

Signed in

By password

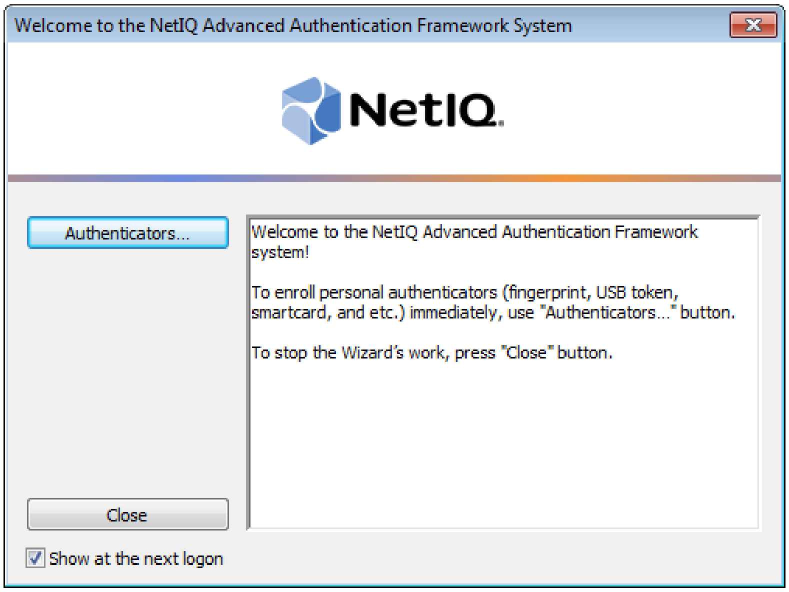
Password →

Sign-in options

- Wait a few seconds until you are logged on to Windows. Once you are logged on, you can enroll your authenticator.

Enrolling Authenticator at First Logon

1. The **Welcome to the NetIQ Advanced Authentication Framework System** window is displayed.



Welcome to the NetIQ Advanced Authentication Framework System
NetIQ
Authenticators...
Close
☑ Show at the next logon

Welcome to the NetIQ Advanced Authentication Framework system!

To enroll personal authenticators (fingerprint, USB token, smartcard, and etc.) immediately, use "Authenticators..." button.

To stop the Wizard's work, press "Close" button.

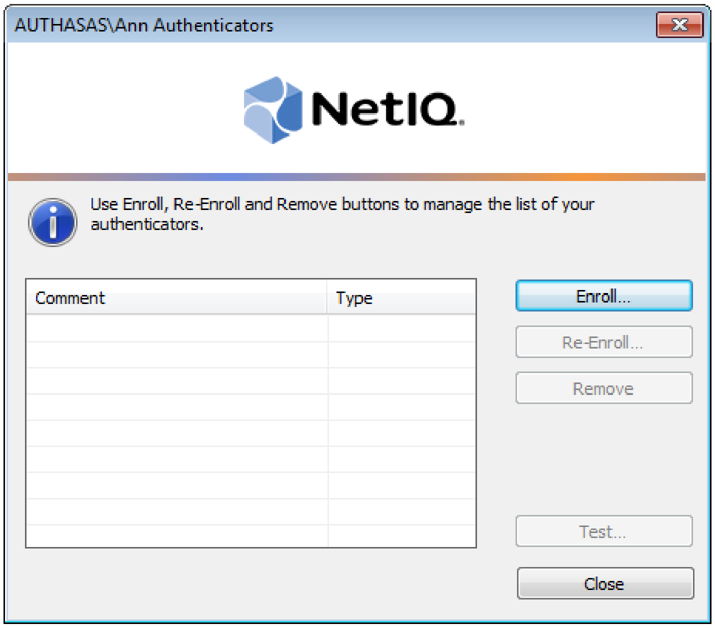
You can enroll an authenticator at once or proceed and enroll the authenticator at any time later.

a) If you choose not to enroll an authenticator at first logon, the **Welcome to the NetIQ Advanced Authentication Framework System** window will be displayed each time you log on until an authenticator is enrolled. To proceed without enrolling an authenticator, click **Close**.

If the **Show at the next logon** option is available, you can stop the welcome window being displayed repeatedly. To do this, cancel the option. As a result, the welcome window will not be shown and you will not be prompted to enroll an authenticator anymore. Later, authenticators may be enrolled and re-enrolled anytime in the **Client Tray**.

b) If you choose to enroll an authenticator at first logon, click **Authenticators**. This brings you to **Authenticators** window.

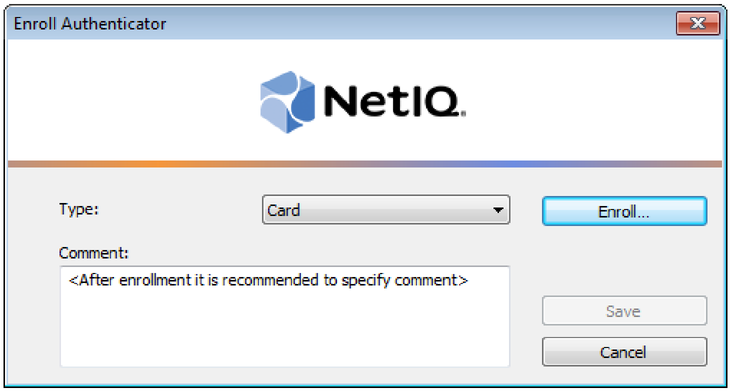
2. Click **Enroll...** button in the **Authenticators** window.


AUTHASAS\Ann Authenticators

Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

Comment	Type

3. In the opened window select the required type of authenticator to be enrolled from the **Type** drop-down menu. Click **Enroll…**

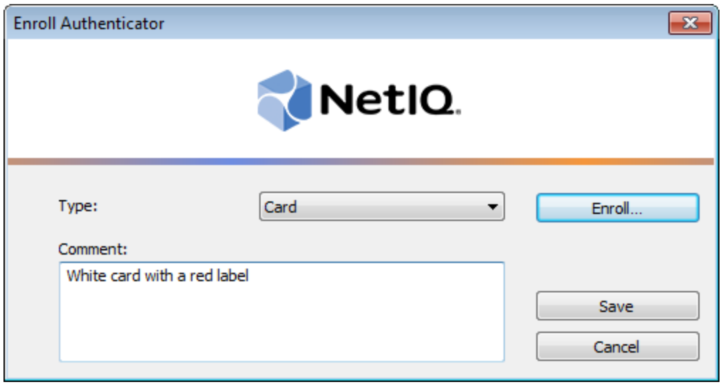

Enroll Authenticator

Type: Card

Comment:
<After enrollment it is recommended to specify comment>

4. You are shown the authentication device screen with instructions to follow, which depend on device type. Follow the instructions to enroll an authenticator.

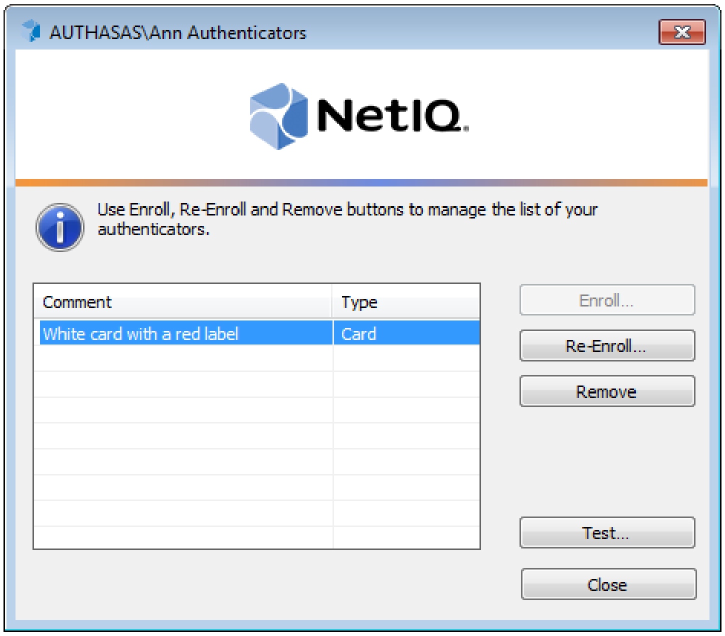
5. After successful enrollment you can add a comment to authenticator (if allowed by the NetIQ administrator).



White card with a red label

Once authenticator is successfully enrolled, you can test authenticator by clicking the **Test...** button (see Testing Authenticator at First Logon).

6. Click **Save**. <*After enrollment it is recommended to specify comment*> record appears in the Authenticators window (if comment is editable).



Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

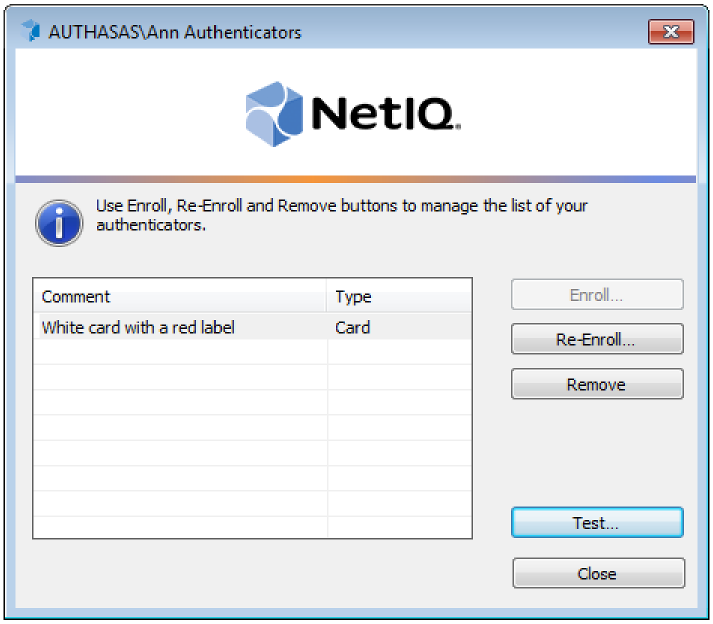
Comment	Type
White card with a red label	Card

After you have enrolled and saved an authenticator, you can:

- re-enroll or remove it;
- choose to log on either with authenticator or with your account password (if logon with password is allowed by the NetIQ administrator).

Testing Authenticator at First Logon

1. In the **Authenticators** window, click **Test**.



AUTHASAS\Ann Authenticators

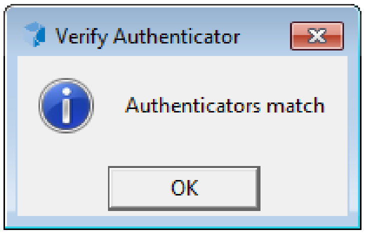
Use Enroll, Re-Enroll and Remove buttons to manage the list of your authenticators.

Comment	Type
White card with a red label	Card

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

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

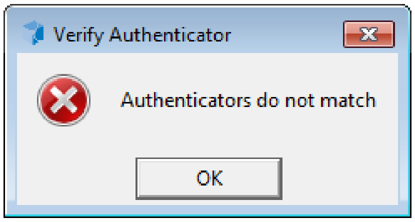
a) if test passed:



Verify Authenticator

Authenticators match

b) if test failed:



Verify Authenticator

Authenticators do not match

If test failed, you may retry testing by clicking **Retry** or click **Cancel** and re-enroll the authenticator.

Logon Methods

In this chapter:

- Logon with Authenticator
- Logon with Password
- Remote Logon Via Dial-Up Connection
- Terminal Logon
- Non-Network Logon

Logon with Authenticator

ℹ The Logon procedure may differ depending on the operating system type you are using. Please select your operating system in the list below:

- Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows Server 2008/ Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003
- Microsoft Windows 8/Microsoft Windows Server 2012

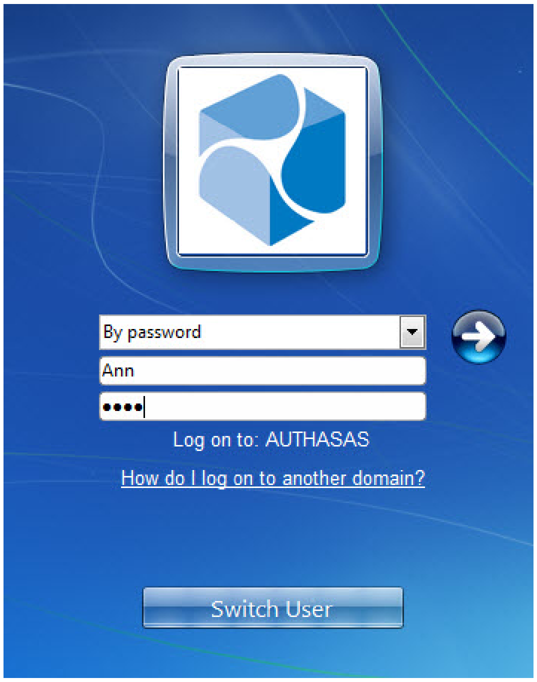
Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

To log on with authenticator:

1. Start your computer. From logon screen, press **[Ctrl]+[Alt]+[Del]** and select your user name if available or click **Switch User**.

2. Follow the steps below:

- Type your user name (not needed unless **Switch User** option has been selected).
- Select any of the available authentication methods as a logon method.
- Click ➜ icon or press **Enter** to continue.



By password

Ann

••••

Log on to: AUTHASAS

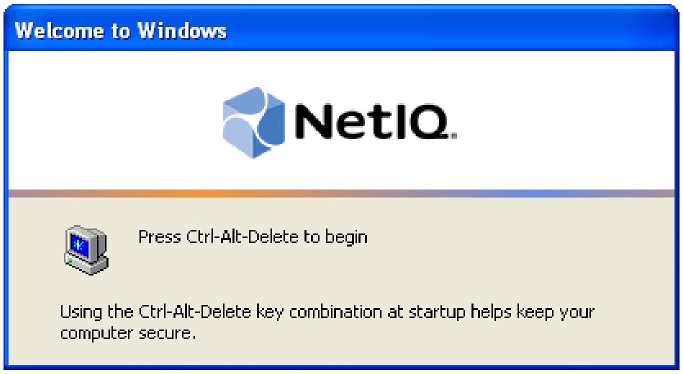
3. You are shown the authentication device screen with instructions to follow, which depend on device type. Follow the instructions to get authenticated.

Wait a few seconds until you are logged on to Windows.

Microsoft Windows Server 2003

To log on with authenticator:

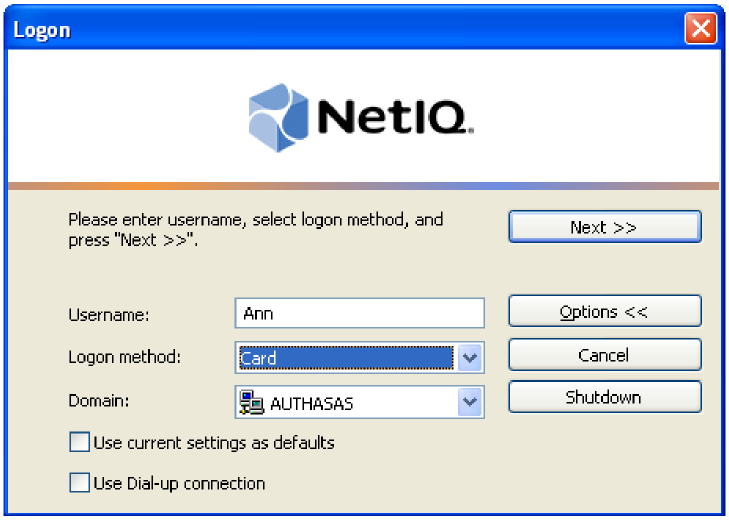
1. Start your computer. When the **Welcome to Windows** window appears, press **[Ctrl]+[Alt]+[Del]**.



Press Ctrl-Alt-Delete to begin

Using the Ctrl-Alt-Delete key combination at startup helps keep your computer secure.

2. The **Logon** window is displayed.



Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Card

Domain: AUTHASAS

☐ Use current settings as defaults

☐ Use Dial-up connection

- In the **User name** box, type your account name.
- From the **Logon method** list, select an authenticator type.
- If you need to specify the domain name, click **Options** and select the name from the **Domain list** (to refresh the list of domain names, select **Refresh**).
- Click **Next >>**.

3. You are shown the authentication device screen with instructions to follow, which depend on device type. Follow the instructions to get authenticated.

4. Wait a few seconds until you are logged on to Windows.

ℹ The **Options** button allows you to hide/show **Use current settings as defaults** and **Use Dial-up connection** options.
If you choose to use authenticator as default logon method, the authentication device screen is displayed at right after you:

- press **[Ctrl]+[Alt]+[Del]** from your desktop to log on;
- select **Manage > Authenticators** from the **Windows Security** window to open the **Authenticators** window.

ℹ The **Use current settings as defaults** option may be disabled by NetIQ administrator. The current logon settings may also be forced as defaults regardless of your wishes.

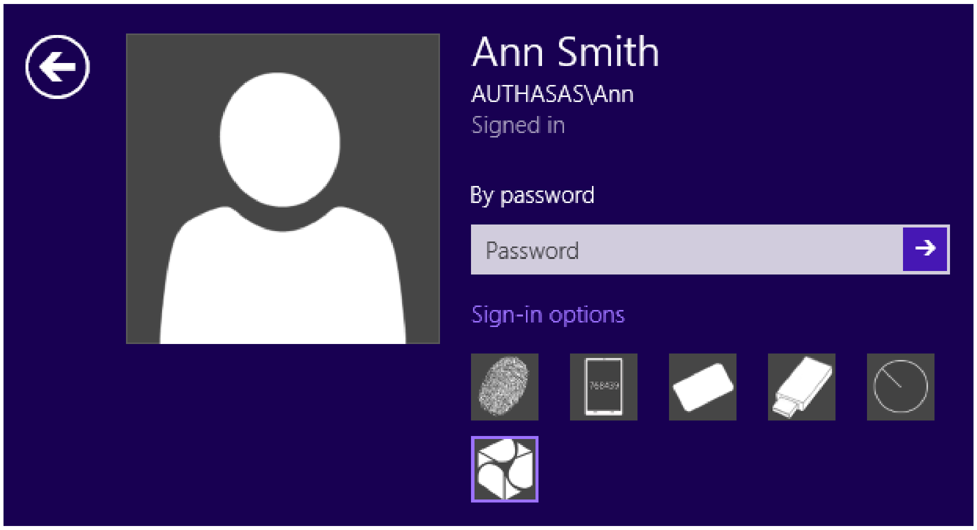
Microsoft Windows 8/Microsoft Windows Server 2012

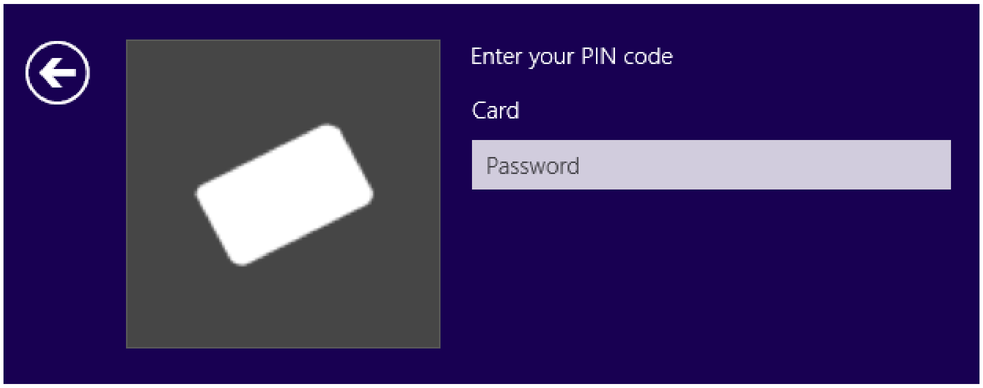
To log on with authenticator:

1. Start your computer and select your user name.

2. Follow the steps below:

- Type your user name.
- Select any of the available authentication methods as a logon method.
- Click → icon or press **Enter** to continue.





3. You are shown the authentication device screen with instructions to follow, which depend on device type. Follow the instructions to get authenticated.

Wait a few seconds until you are logged on to Windows.

Logon with Password

ℹ Please select your operating system in the list below:

- Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows Server 2008/ Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003
- Microsoft Windows 8/Microsoft Windows Server 2012

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

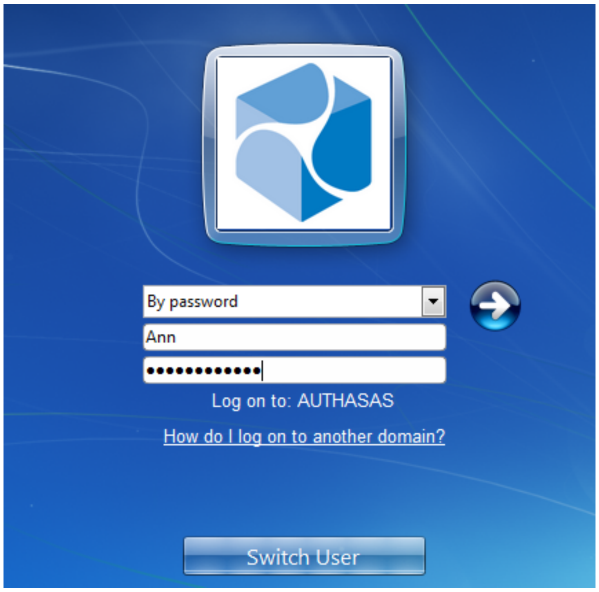
ℹ If random password was generated for your account, you can log on with an authenticator only.

To log on with your account password:

1. Start your computer. From logon screen, press **[Ctrl]+[Alt]+[Del]** and select your user name if available or click **Switch User**.

2. Follow the steps below:

- Type your user name (not needed unless **Switch User** option has been selected).
- Select **By Password** as a logon method and type your password.
- Click ➡ icon or press **Enter** to continue.



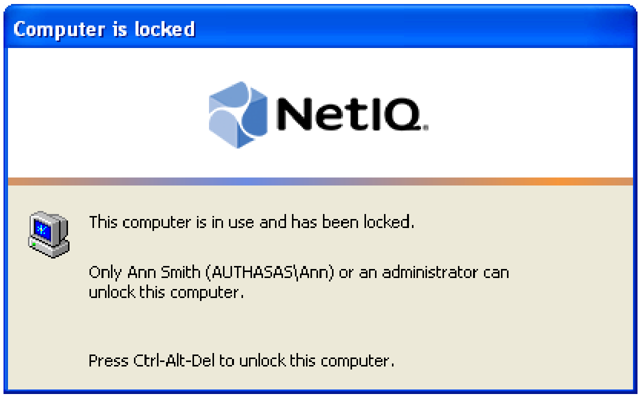
- Wait a few seconds until you are logged on to Windows.

Microsoft Windows Server 2003

ℹ If random password was generated for your account, you can log on with an authenticator only.

To log on with your account password:

1. Start your computer. When the **Welcome to Windows** window appears, press **[Ctrl]+[Alt]+[Del]**.

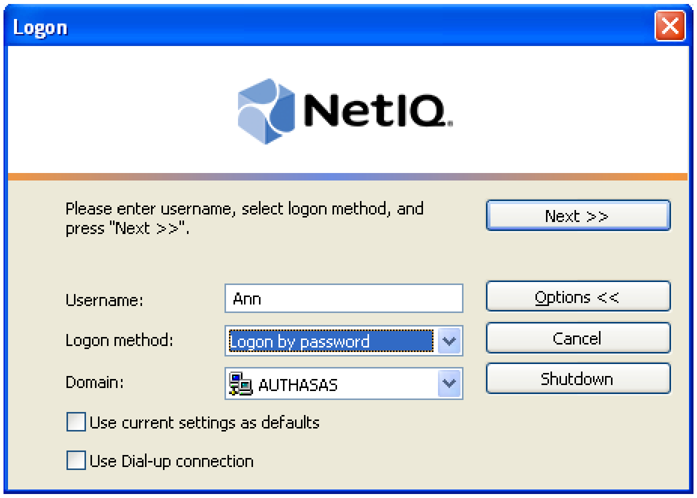


This computer is in use and has been locked.

Only Ann Smith (AUTHASAS\Ann) or an administrator can unlock this computer.

Press Ctrl-Alt-Del to unlock this computer.

2. The **Logon** window is displayed.



Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Logon by password

Domain: AUTHASAS

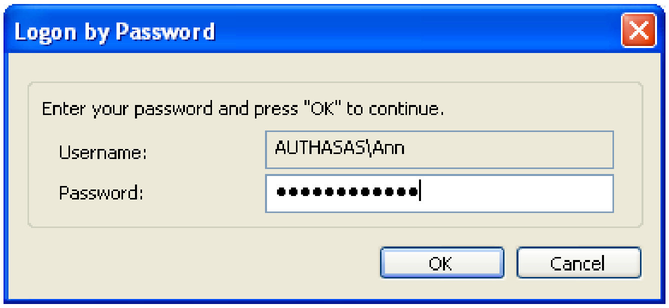
☐ Use current settings as defaults

☐ Use Dial-up connection

- In the **User name** box, type your account name.
- From the **Logon method** list, select **Logon by password**.
- If you need to specify the domain name, click **Options** and select it from the **Domain** list (to refresh the list of domain names, select **Refresh**).

- Click **Next >>**.

3. The **Logon by Password** dialog is displayed.



Logon by Password

Enter your password and press "OK" to continue.

Username: AUTHASAS\Ann

Password: ●●●●●●●●●●●●

- Type your account password in the **Password** box.
- Click **OK**.

4. Wait a few seconds until you are logged on to Windows.

ℹ The **Options** button allows you to hide/show **Use current settings as defaults** and **Use Dial-up connection** options.
If you choose to use password as default logon method, the **Logon by Password** dialog is displayed at right after you:

- press **[Ctrl]+[Alt]+[Del]** from your desktop to logon;
- select **Manage > Authenticators** from the **Windows Security** window to open the **Authenticators** window.

ℹ The **Use current settings as defaults** option may be disabled by NetIQ administrator. The current logon settings may also be forced as defaults regardless of your wishes.

Microsoft Windows 8/Microsoft Windows Server 2012

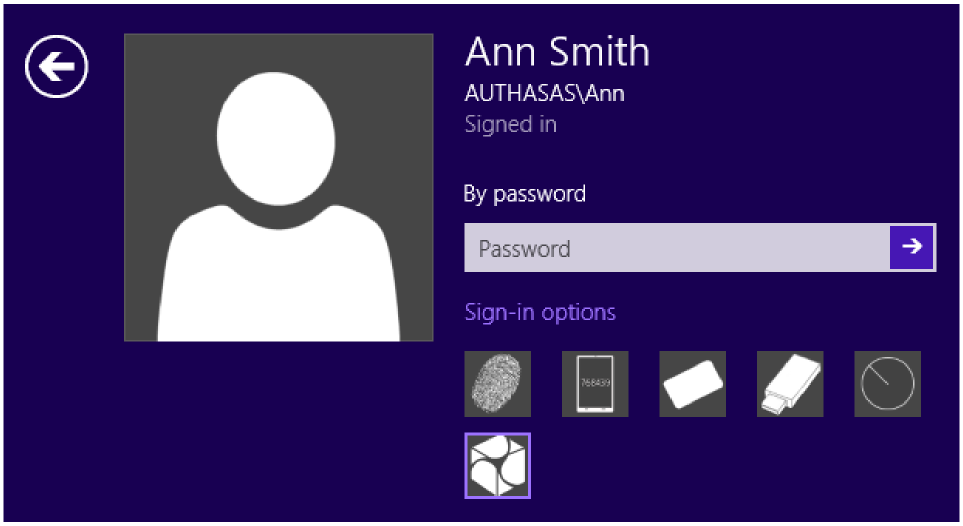
If random password was generated for your account, you can log on with an authenticator only.

To log on with your account password:

1. Start your computer. Select your user name.

2. Follow the steps below:

- Select **By Password** as a logon method and type your password.
- Click → icon or press **Enter** to continue.



- Wait a few seconds until you are logged on to Windows.

Remote Logon Via Dial-Up Connection

Please select your operating system in the list below:

- Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows Server 2008/ Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003
- Microsoft Windows 8/Microsoft Windows Server 2012

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

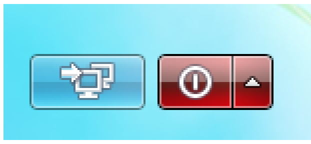
Before using this logon method you should consult NetIQ administrator and make sure the dial-up connection is configured and compatible with the network equipment you are going to use.

The **Use Dial-up connection** option may be disabled by NetIQ administrator.

To log on via dial-up connection:

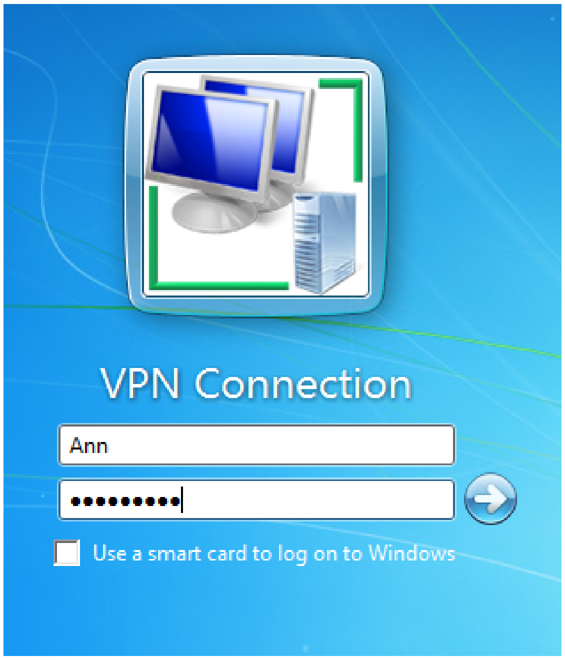
1. Start your computer. From logon screen, press **[Ctrl]+[Alt]+[Del]** and click **Switch User**.

2. Click the **Network Logon** button or select a connection (if there are several available connections, each of them appears as a separate button).



3. Follow the steps below:

- Type your user name and password.
- Click ➔ icon or press **Enter** to continue.



VPN Connection

Ann

●●●●●●●●●●

☐ Use a smart card to log on to Windows

4. Wait a few seconds until the connection is set up.

Log on with any available method (pattern/password).

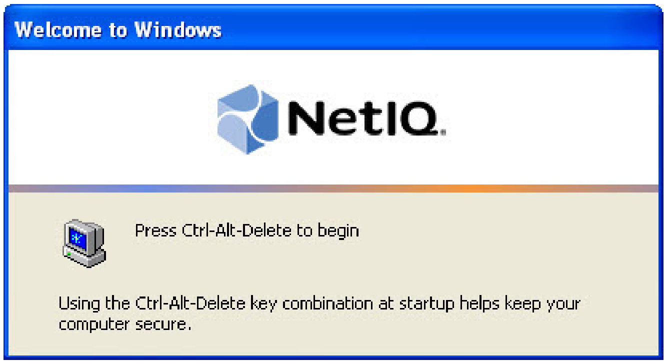
Microsoft Windows Server 2003

Before using this logon method you should consult NetIQ administrator and make sure the dial-up connection is configured and compatible with the network equipment you are going to use.

The **Use Dial-up connection** option may be disabled by NetIQ administrator.

To log on remotely via dial-up connection:

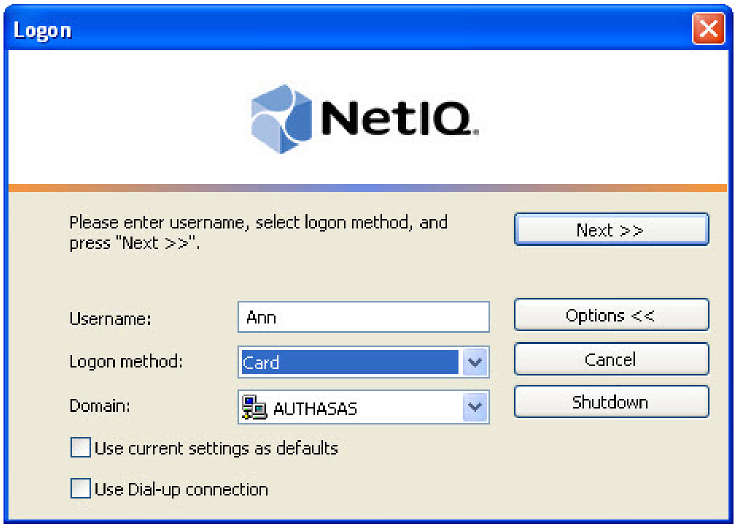
1. Start your computer. When the **Welcome to Windows** window appears, press **[Ctrl]+[Alt]+[Del]**.



Press Ctrl-Alt-Delete to begin

Using the Ctrl-Alt-Delete key combination at startup helps keep your computer secure.

2. The **Logon** window is displayed.



Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Card

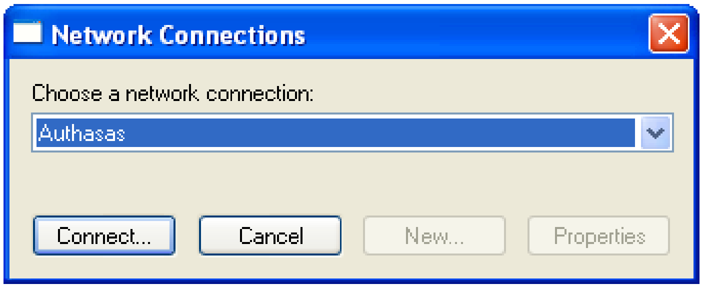
Domain: AUTHASAS

☐ Use current settings as defaults

☐ Use Dial-up connection

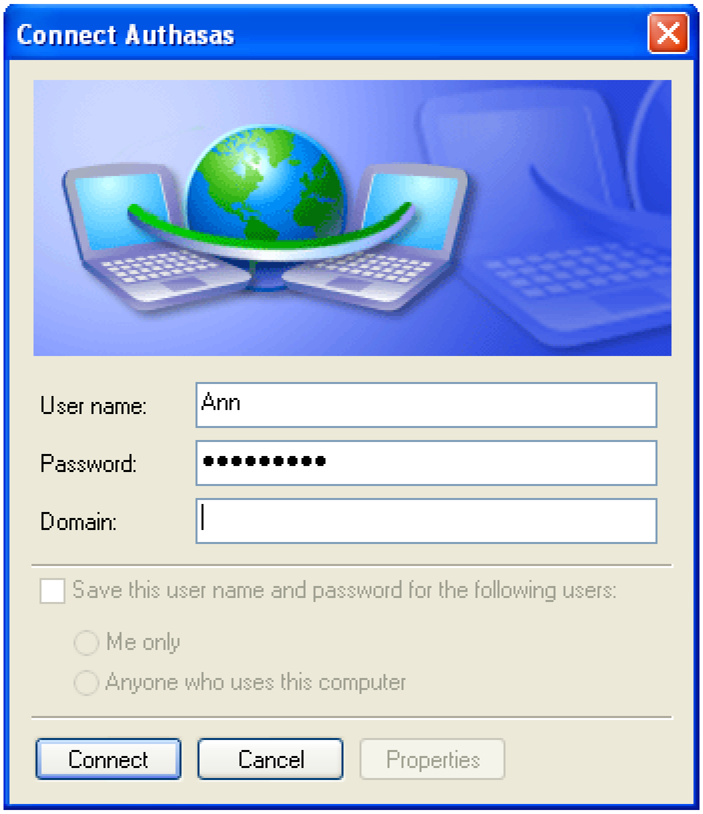
- In the **User name** box, type your account name.
- Click **Options** and check the **Use Dial-up connection** box.

3. The **Network Connections** dialog opens. Select the connection name and click **Connect...**.



Choose a network connection: Authasas

4. Enter additional credentials (if necessary) and click **Connect**.



User name: Ann

Password: ••••••••••

Domain:

□ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

5. After the dial-up connection has been set up, the **Logon** window is displayed with the **Use Dialup connection** box checked. Log on using any available method.

Microsoft Windows 8/Microsoft Windows Server 2012

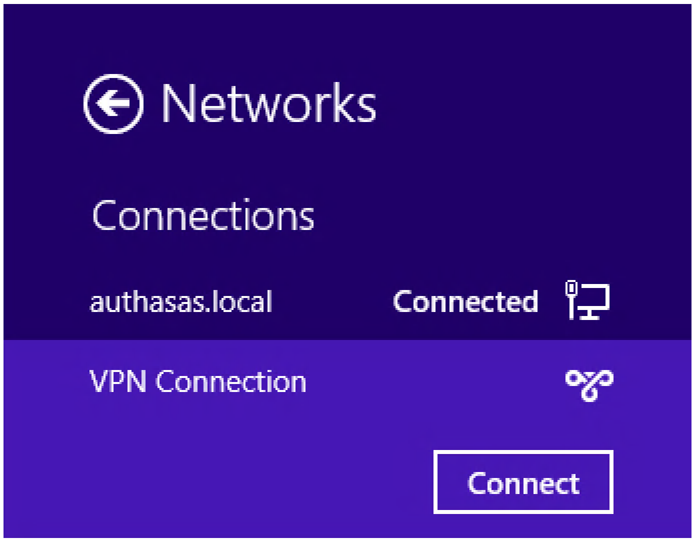
Before using this logon method you should consult NetIQ administrator and make sure the dial-up connection is configured and compatible with the network equipment you are going to use.

The **Use Dial-up connection** option may be disabled by NetIQ administrator.

To log on via dial-up connection:

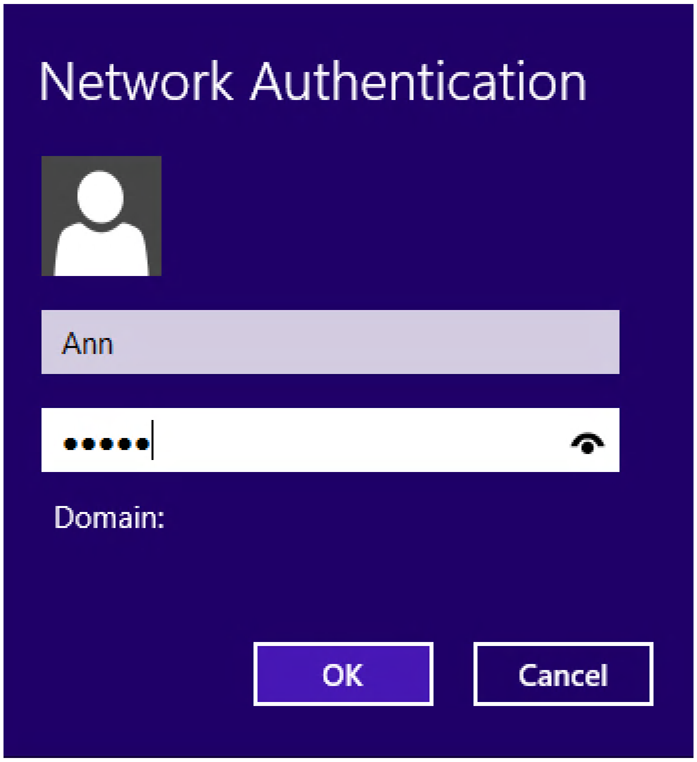
1. Start your computer.

2. Click the **Networks** button and select a connection (if there are several available connections, each of them appears as a separate button).



3. Follow the steps below:

- Type your user name and password.
- Click → icon or press **Enter** to continue.



Network Authentication

Ann

•••••

Domain:

4. Wait a few seconds until the connection is set up.

Log on with any available method (pattern/password).

Terminal Logon

NetIQ Advanced Authentication Framework™ allows you to log on to a terminal server (remote desktop) using any available logon method.

To log on to a terminal server (remote desktop) both remote desktop PC and user's PC must have terminal client and required authentication providers' modules installed.

To log on to a terminal server:

1. Start the "Remote Desktop" tool (**Start** > **Programs** > **Accessories** > **Communications** > **Remote Desktop Connection**).

2. The **Remote Desktop Connection** dialog opens. Enter the IP-address or name of the terminal server and click **Connect**.

3. After the connection has been set up, the **Logon** window is displayed. Log on using any available method.

Non-Network Logon

NetIQ Advanced Authentication Framework™ allows you to log on in offline mode, from a standalone computer/laptop that is not physically connected to the network.

Non-network logon method is available to you only if it is explicitly permitted by NetIQ administrator and if you have performed network logon at least once.

To enable non-network logon, you must have your authenticators cached (See Caching Authenticators).

Automatic Logon

ℹ The Automatic logon feature is available only on Microsoft Windows Server 2003.

In order to enable Automatic logon feature, please contact local administrator.

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

Automatic logon is a standard Microsoft feature. For more detailed information about Automatic logon and the ways of turning it on/off, see Microsoft Support page.

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

If you want to bypass the automatic logon to log on as a different user, hold down the **Shift** key after you log off, or after Windows restarts, or when you unlock PC.

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

Managing Password

In this chapter:

- Changing Password
- Getting Password
- SSPR Support

Changing Password

Please select your operating system in the list below:

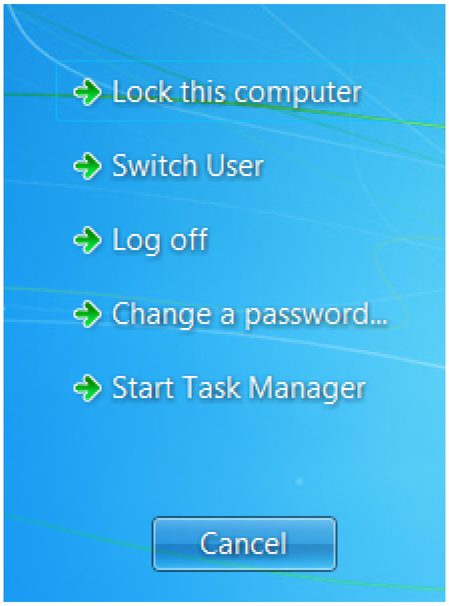
- Microsoft Windows Vista/Microsoft Windows 7/Microsoft Windows Server 2008/ Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2003

Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2

The operation may be forbidden by NetIQ administrator.

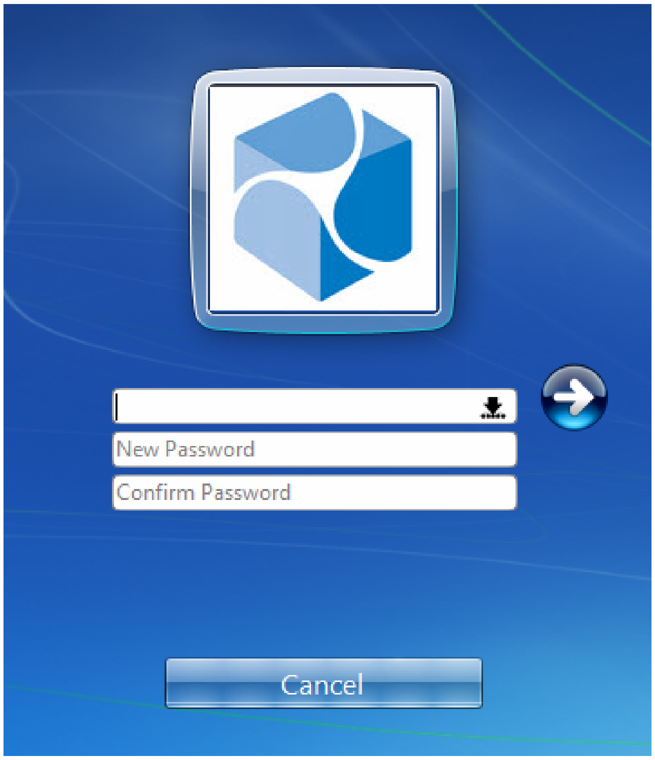
To change the password:

1. From your desktop, press **[Ctrl]+[Alt]+[Del]**. The **Windows Security** window is displayed.



2. Click **Change a Password...**.

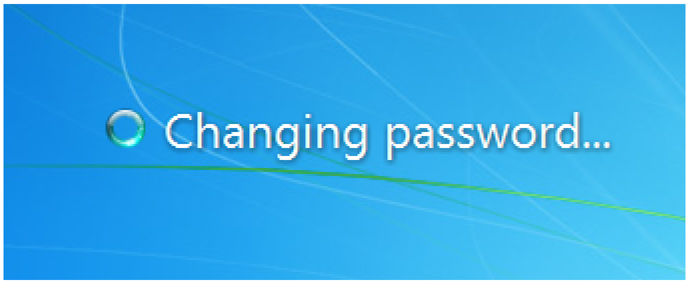
3. The **Change Password** dialog is displayed.



- Type your old password, then type a new one and confirm it.
- Click ➔ icon or press **Enter**.

ℹ If you do not know your current password, you can get it.

The password will be changed.



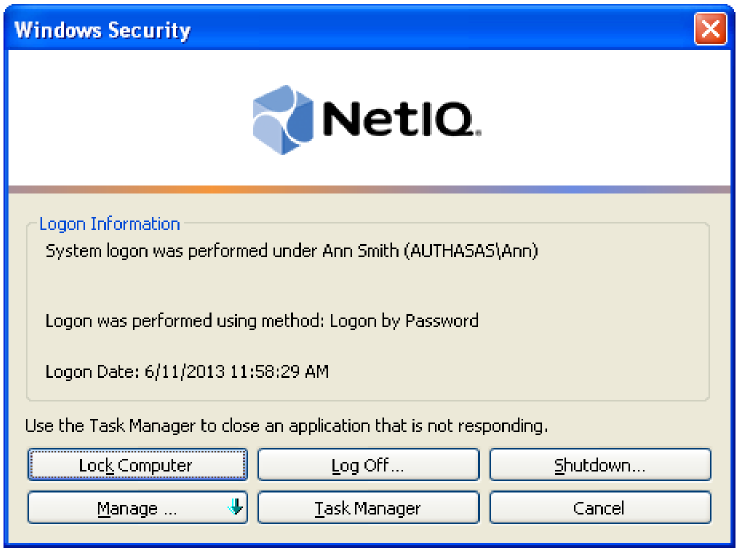
Changing password...

Microsoft Windows Server 2003

The operation may be forbidden by NetIQ administrator.

To change the password:

1. From your desktop, press **[Ctrl]+[Alt]+[Del]**. The **Windows Security** window is displayed.



Logon Information

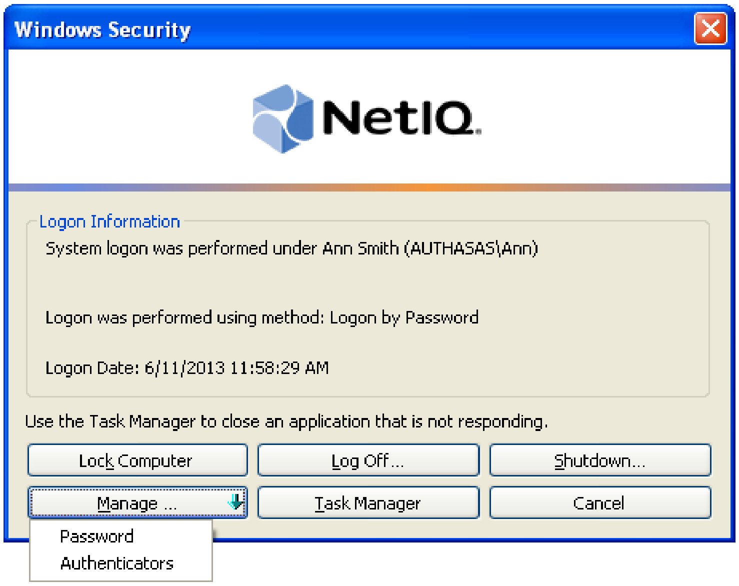
System logon was performed under Ann Smith (AUTHASAS\Ann)

Logon was performed using method: Logon by Password

Logon Date: 6/11/2013 11:58:29 AM

Use the Task Manager to close an application that is not responding.

2. Click **Manage** and select **Password**.



Logon Information

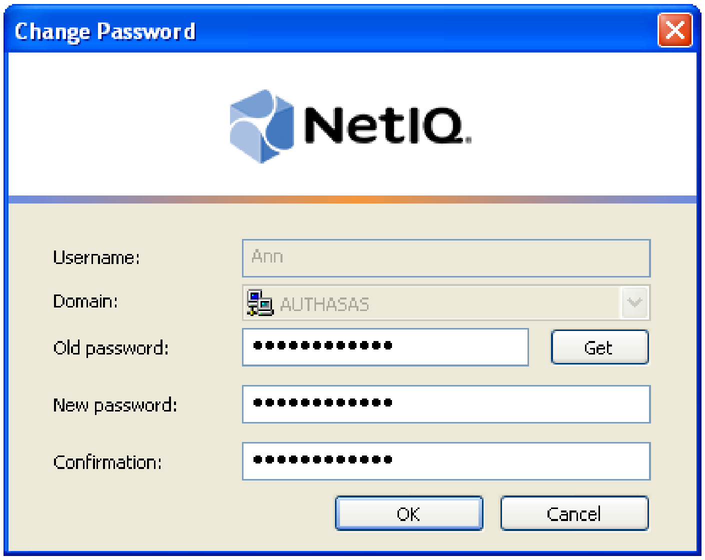
System logon was performed under Ann Smith (AUTHASAS\Ann)

Logon was performed using method: Logon by Password

Logon Date: 6/11/2013 11:58:29 AM

Use the Task Manager to close an application that is not responding.

3. The **Change Password** dialog is displayed.


Change Password

Username: Ann

Domain: AUTHASAS

Old password: ●●●●●●●●●●●●●

New password: ●●●●●●●●●●●●●

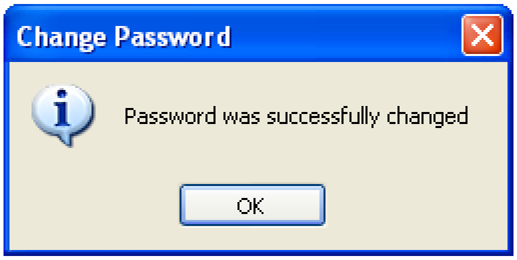
Confirmation: ●●●●●●●●●●●●●

- Type your old password, then type a new one and confirm it.

ⓘ If you do not know your current password, you can get it (see Getting Password).

- Click **OK**.

If your password is changed successfully, you receive this message:


Change Password

Password was successfully changed

Getting Password

To get your current password:

1. In the **Change Password** dialog, click **Get**.

2. You are shown the authentication device screen with instructions to follow or the **Logon by password** dialog (depending on which logon method you used last).

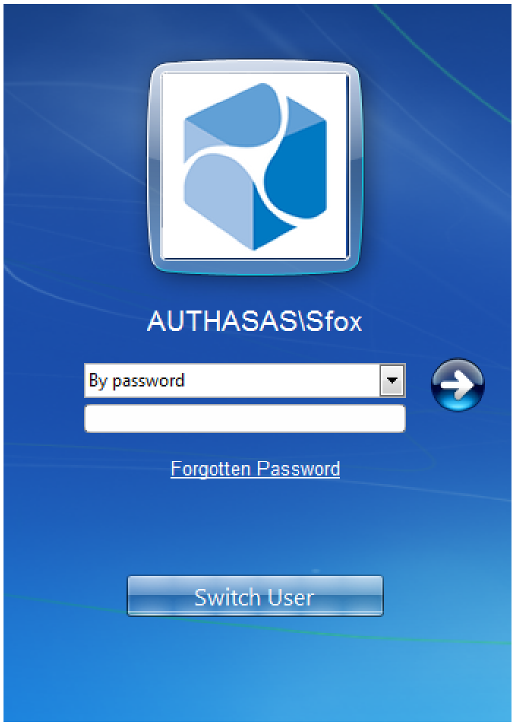
3. After successful authentication your current password appears in the **Old password** box in the **Change Password** dialog.

NetIQ SSPR Support

Self Service Password Reset (SSPR) helps to reduce help desk costs by enabling users to reset the password based on the rules specified in the password policy.

When Client Login Extension is installed on the workstation, NetIQ Client adds an item the **Forgotten password** (by default) in NetIQ Credential Provider. This allows to reduce help desk costs if passwords are still used in an environment.

✱ NetIQ SSPR is supported in Windows 7 only.


AUTHASAS\Sfox
By password
Forgotten Password
Switch User

Caching Authenticators

Caching authenticators is copying them to local memory. You need to have authenticators cached on your computer if you want to use non-network logon method.

If caching is allowed on your computer, you will see the **Cache** policy notification at your first logon. Click **OK**.

ℹ Cache management setting, which allows you to enable and disable cache at any moment, is available from NetIQ Advanced Authentication Framework Client Tray (see NetIQ Advanced Authentication Framework Client Tray Settings).

✱ Caching refreshes on authentication. If you have had your authenticator cached and then re-enrolled it, you should to re-logon using the new authenticator while connected to the network. **If connection is terminated after logoff, you will be unable to log on with the re-enrolled authenticator.**

✱ When you are logged on to the system using non-network logon, you can neither add, nor re-enroll, nor remove your authenticators.

Locking/Unlocking Computer

Locking computer

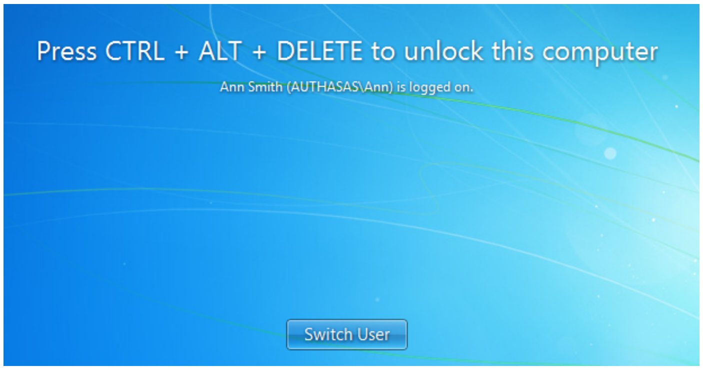
Your computer can be locked:

- automatically by screensavers when it has been idle for some time;
- automatically after returning from the hibernate mode;
- manually by pressing **[Ctrl]+[Alt]+[Del]** from your desktop and clicking **Lock Computer** in the **Windows Security** window;
- when user's authenticator (card or flash drive) has been removed, if the appropriate policy is configured by NetIQ administrator.

It is strongly recommended that you lock your computer if you are going to be away for some time.

When your computer is locked, the following window is displayed:

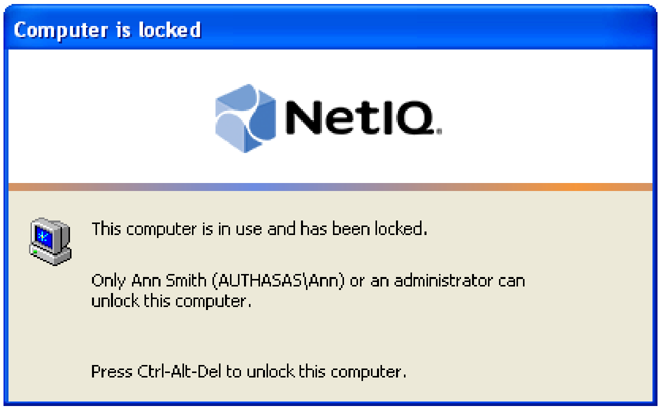
a) For Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2:



Press CTRL + ALT + DELETE to unlock this computer

Ann Smith (AUTHASAS\Ann) is logged on.

b) For Microsoft Windows Server 2003:



Computer is locked

This computer is in use and has been locked.

Only Ann Smith (AUTHASAS\Ann) or an administrator can unlock this computer.

Press Ctrl-Alt-Del to unlock this computer.

Unlocking Computer

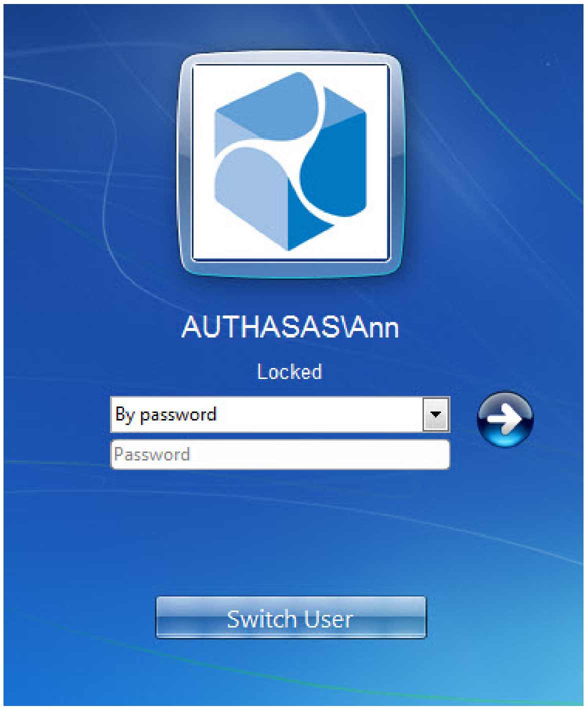
Your computer can be unlocked only by you or by NetIQ administrator (forced unlock).

To unlock your computer:

1. Press **[Ctrl]+[Alt]+[Del]**.

2. The **Unlock Computer** window is displayed. Get authorized using any available method (it does not matter which method you used initially to log on).

a) **For Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2:**

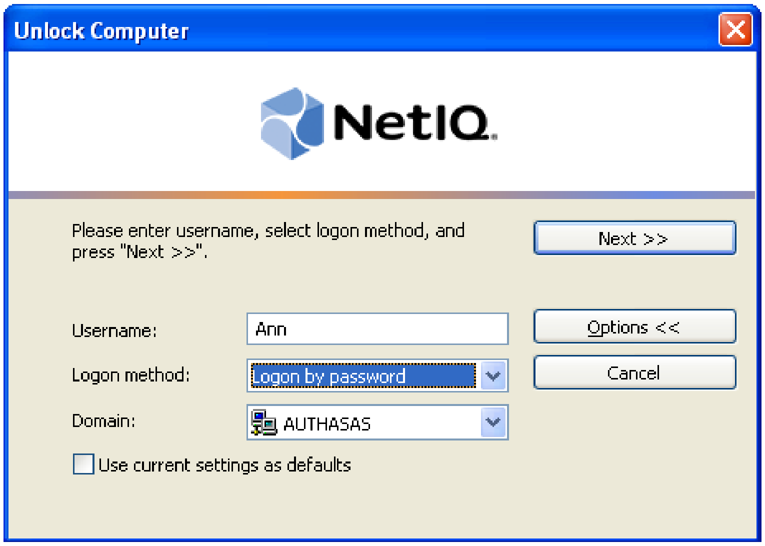


AUTHASAS\Ann

Locked

By password

b) **For Microsoft Windows Server 2003:**



Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Logon by password

Domain: AUTHASAS

□ Use current settings as defaults

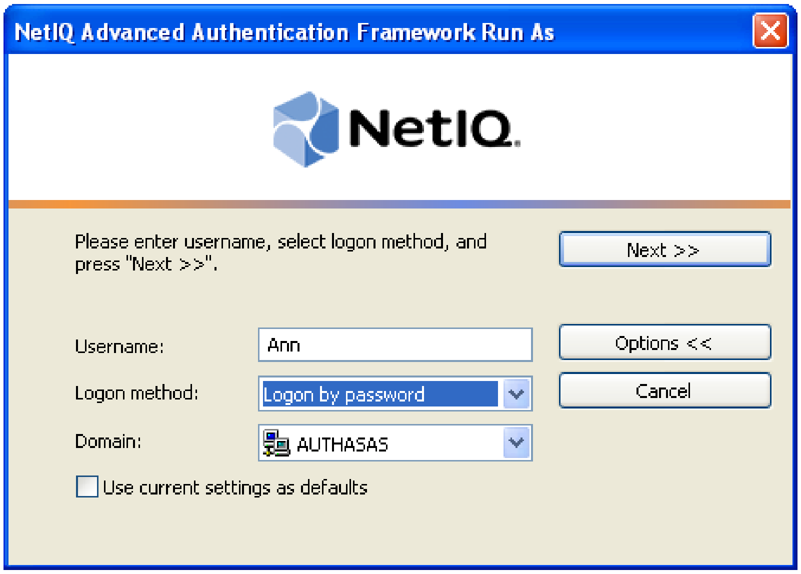
NetIQ Advanced Authentication Framework Run As Tool

NetIQ Advanced Authentication Framework Run As tool allows you to open a document/start an application under another user's account. Compared to the standard **Run As** tool, **NetIQ Advanced Authentication Framework Run As** requires you to submit an authenticator. Unless you are not authenticated successfully you cannot perform any actions under another user's account.

To use **NetIQ Advanced Authentication Framework Run As** tool:

1. Right-click the file or shortcut you would like to open and select **NetIQ Advanced Authentication Framework Run As**.

2. The **NetIQ Advanced Authentication Framework Run As** window is displayed.



NetIQ Advanced Authentication Framework Run As

Please enter username, select logon method, and press "Next >>".

Username: Ann

Logon method: Logon by password

Domain: AUTHASAS

□ Use current settings as defaults

- Type the user account name.
- Select a logon method (an authenticator type or **Logon by password**).
- Click **Next >>**.

3. Get authorized.

Authorization By Authenticator

1. In the **NetIQ Advanced Authentication Framework Run As** window, select an authenticator type. Click **Next>>**.

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

After successful authentication the **NetIQ Advanced Authentication Framework Run As** tool attempts to perform the selected action.

ℹ For the selected action to be performed successfully, in some cases (depending on the executed file or shortcut) you need to have the appropriate administrative privileges.

NetIQ Advanced Authentication Framework Client Tray Settings

In this chapter:

- General settings
- Language settings
- Password authorization
- Cache management settings

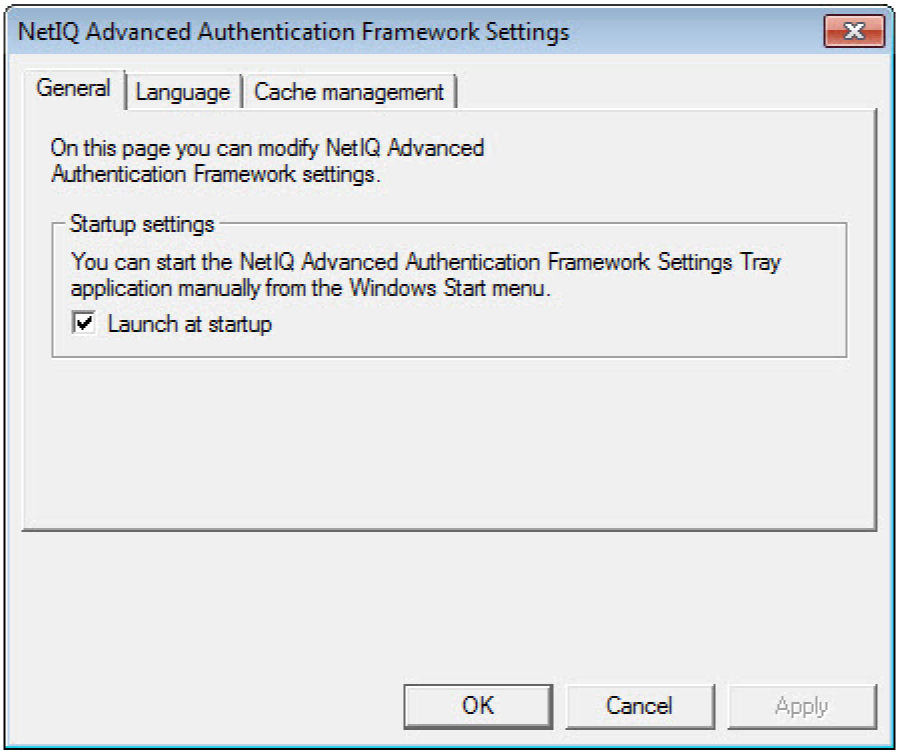
✱ Changing NetIQ Advanced Authentication Framework Logon parameters requires **Local Admins** privileges.

NetIQ Advanced Authentication Framework Client Tray allows you to change some NetIQ Advanced Authentication Framework parameters.

To access the parameters right-click the icon on the system tray and select **Settings...**.

General Settings

The **Launch at startup** box setting available on the **General** tab allows you to determine whether NetIQ Advanced Authentication Framework Client Tray is launched automatically at Windows startup or manually (**Start > Programs > NetIQ Advanced Authentication Framework > NetIQ Advanced Authentication Framework Settings Tray**). By default, the **Launch at startup** box is checked, and **NetIQ Advanced Authentication Framework Client Tray** is launched automatically.



NetIQ Advanced Authentication Framework Settings

On this page you can modify NetIQ Advanced Authentication Framework settings.

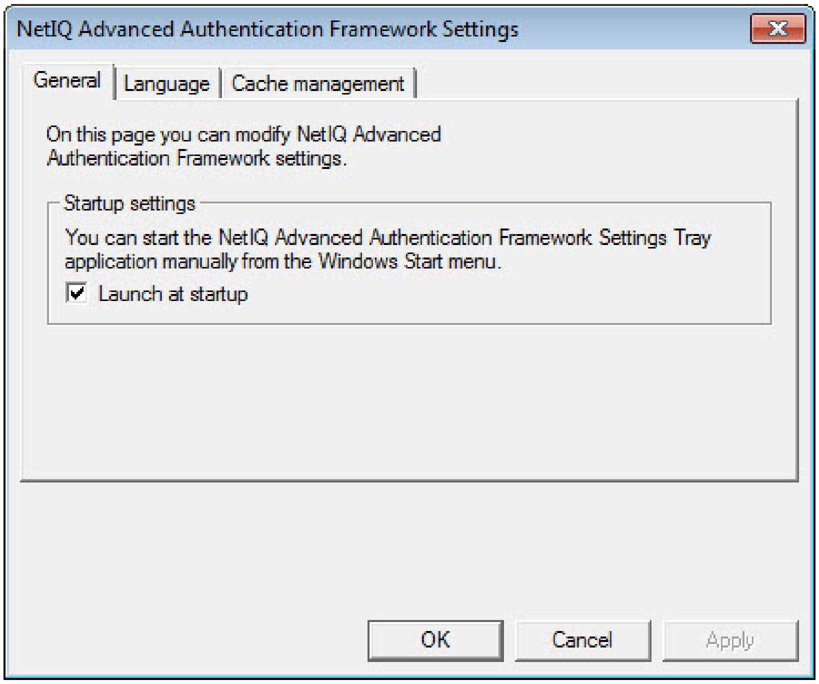
Startup settings

You can start the NetIQ Advanced Authentication Framework Settings Tray application manually from the Windows Start menu.

☑ Launch at startup

Language Settings

The **Language** list available on the **Language** tab allows you to select a language for the text displayed in NetIQ Advanced Authentication Framework Client windows. The available languages include English, Spanish and Dutch. By default, NetIQ Advanced Authentication Framework Client uses the language of the operating system.


NetIQ Advanced Authentication Framework Settings

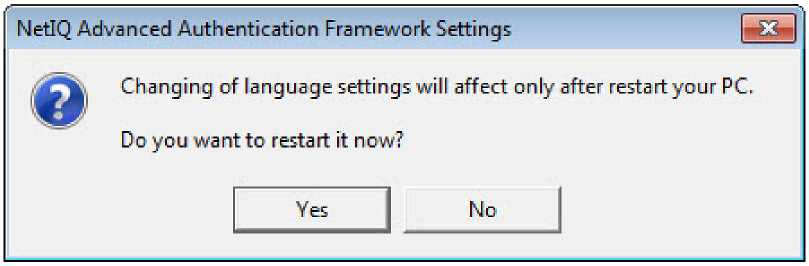
On this page you can modify NetIQ Advanced Authentication Framework settings.

Startup settings

You can start the NetIQ Advanced Authentication Framework Settings Tray application manually from the Windows Start menu.

☑ Launch at startup

You must restart your computer for the changes to take effect:


NetIQ Advanced Authentication Framework Settings

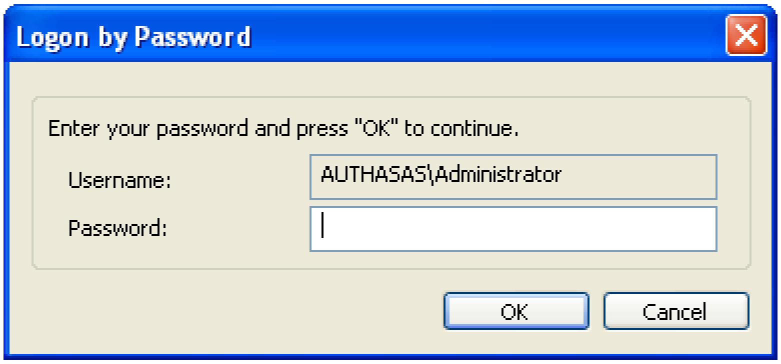
Changing of language settings will affect only after restart your PC.

Do you want to restart it now?

Password Authorization

1. In the **NetIQ Advanced Authentication Framework Run As** window, select the **Logon by password** logon method. Click **Next >>**.

2. The **Logon by password** dialog is displayed.



Logon by Password

Enter your password and press "OK" to continue.

Username: AUTHASAS\Administrator

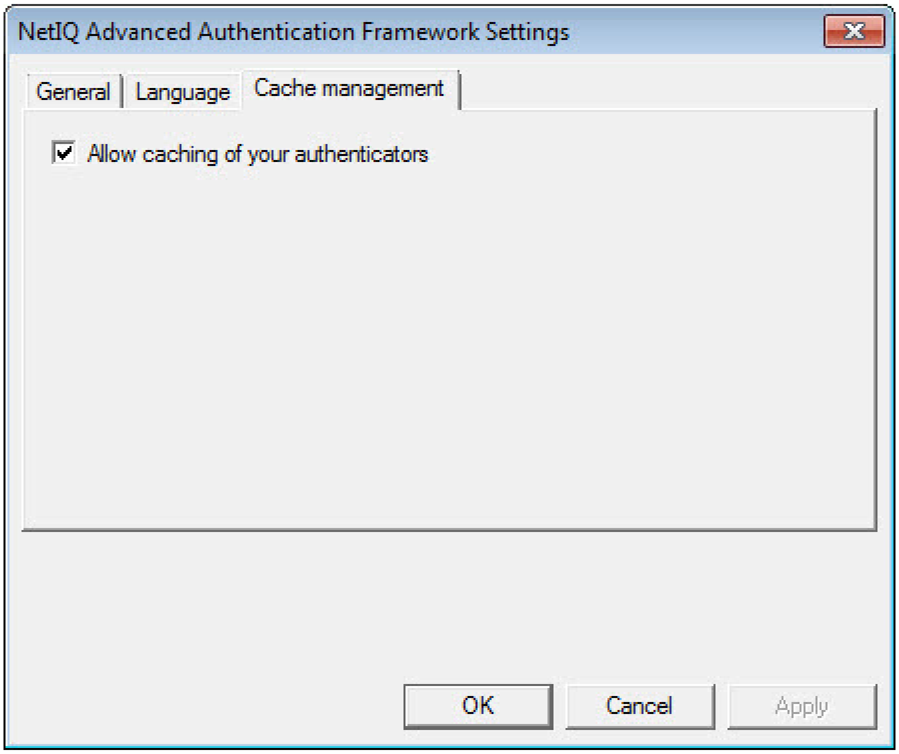
Password:

- Type the password.
- Click **OK.**

Cache Management Settings

If NetIQ administrator has disabled authenticators caching on your computer, these settings are not available.

The **Allow caching of your authenticators** option available on the **Cache management** tab allows you to enable/disable authenticators caching on your computer.


NetIQ Advanced Authentication Framework Settings

☑ Allow caching of your authenticators

Troubleshooting

In this chapter:

- Support Information in Client Tray Menu
- Cannot Get Authorized
- Cannot Change Password
- Cannot Enroll Authenticator
- Cannot Save Authenticator

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

Before contacting the support service:

We strongly request that you give a possibly detailed description of your problem to the support technicians and attach logs from the faulty computer. To obtain the logs, use the LogCollector.exe tool (\Tools\LogCollector). Follow the steps below:

1. Copy LogCollector.exe to the local C:\ disk on the faulty computer.

The tool may not work from a network drive.

2. Run LogCollector.exe.

3. In the dialog that opens, click **Enable all**. As a result, all items in the **Debugged components** section are selected. Close the dialog.

4. Reproduce the steps that caused the problem.

5. Run LogCollector.exe. again and click **Save logs**.

6. Save the logs to archive.

Support Information in Client Tray Menu

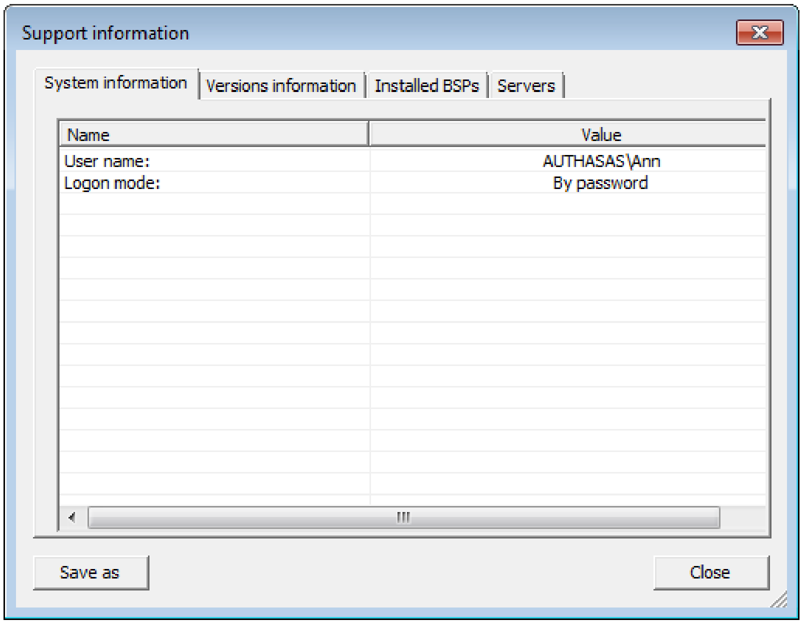
The **Client** tray menu support information might also prove useful to you when solving some of the existing problems. It contains the useful information on Authentication software and logged in user.

To see the information:

1. Right-click the icon on the system tray and select **Support...**.

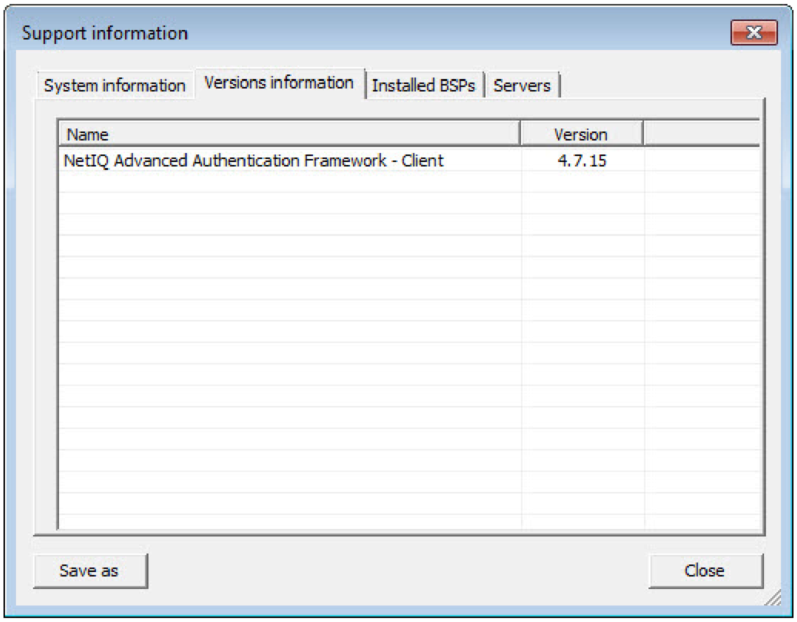
2. The **Support information** window opens, which includes the following tabs:

- **System information** tab with data on user name and logon method.



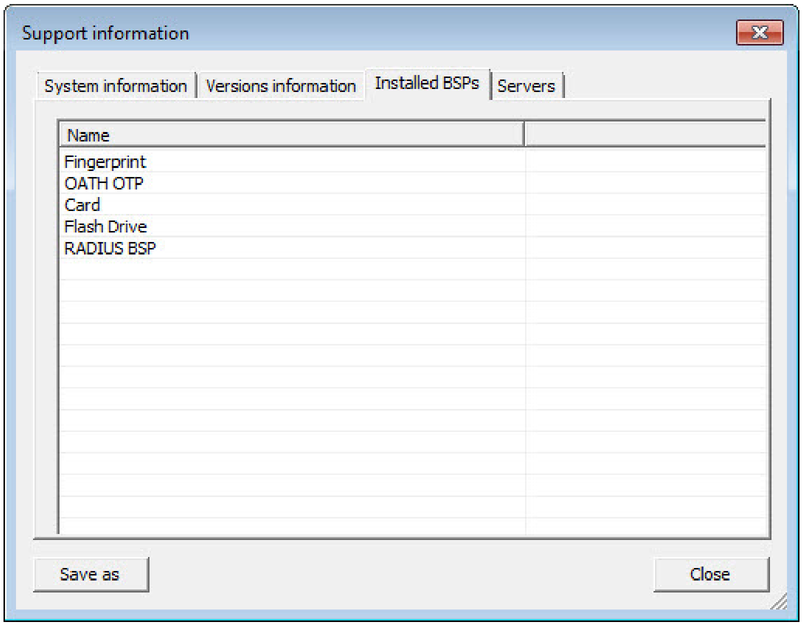
Name	Value
User name:	AUTHASAS\Ann
Logon mode:	By password

- **Versions information** tab containing NetIQ Advanced Authentication Framework software version data.



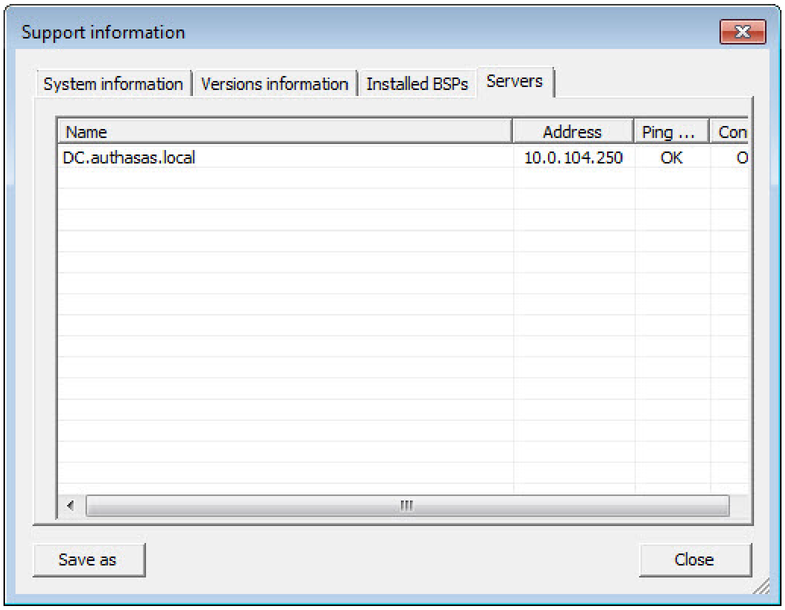
Name	Version
NetIQ Advanced Authentication Framework - Client	4.7.15

- **Installed BSPs** tab, which informs about installed authentication providers.



Name
Fingerprint
OATH OTP
Card
Flash Drive
RADIUS BSP

- **Servers** tab with basic server information.



Name	Address	Ping ...	Con
DC.authasas.local	10.0.104.250	OK	O

You also have a possibility to save all the **Support** information by clicking the **Save as** button. The data is stored in a form of a .txt file.

It would be preferable if you send this report together with the logs when contacting the technical support service.

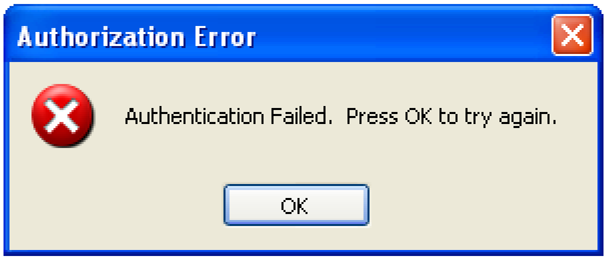
Cannot Get Authorized

Description:

Authentication is completed unsuccessfully. An error message appears.

Cause:

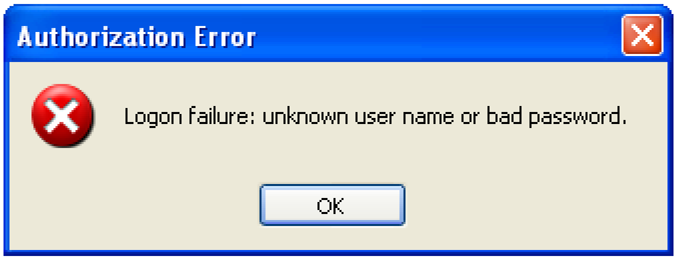
a) This message appears if you have entered the wrong account name or if authenticators do not match:



Authorization Error

Authentication Failed. Press OK to try again.

b) This message appears if you have entered the wrong account name or password when logging on with password:

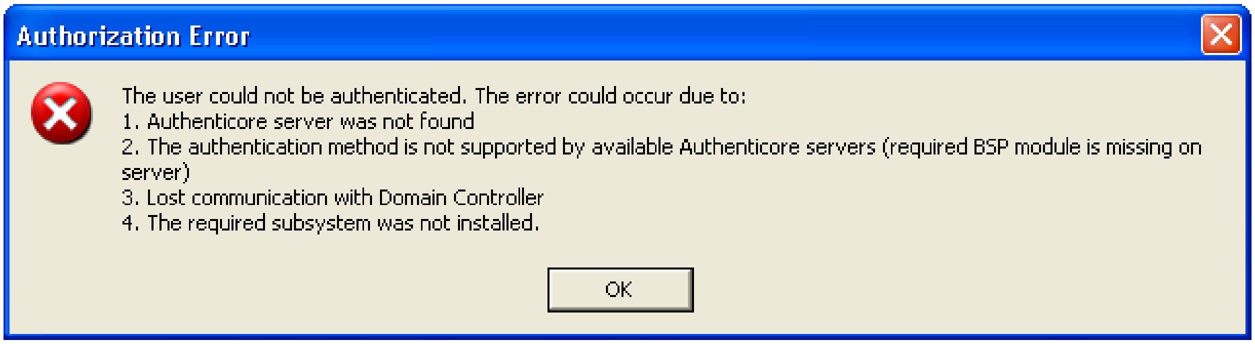


Authorization Error

Logon failure: unknown user name or bad password.

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

c) This message appears if connection to Authenticore server or Domain Controller was lost, or the logon method you selected is not supported.


Authorization Error

The user could not be authenticated. The error could occur due to:
1. Authenticore server was not found
2. The authentication method is not supported by available Authenticore servers (required BSP module is missing on server)
3. Lost communication with Domain Controller
4. The required subsystem was not installed.

Solution:

a), b) Check your credentials and try to log on again. If the error persists, contact NetIQ administrator.

c) Contact NetIQ administrator.

Cannot Change Password

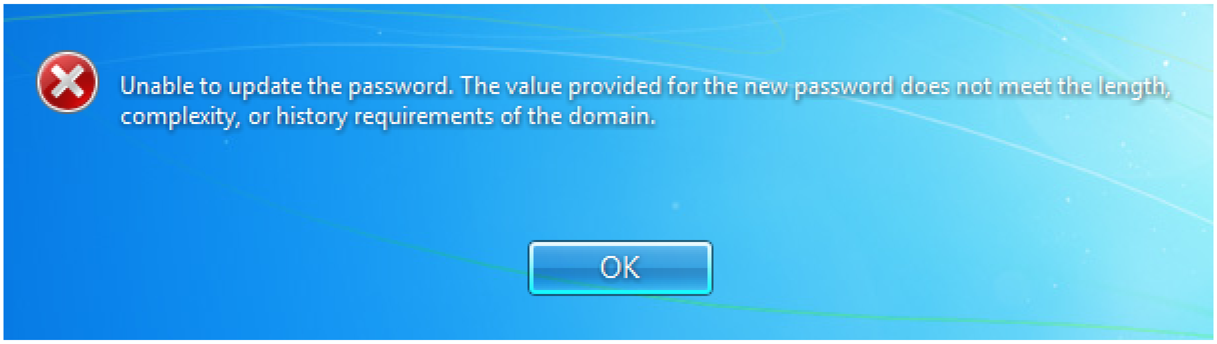
Description:

The password cannot be changed. An error message appears.

Cause:

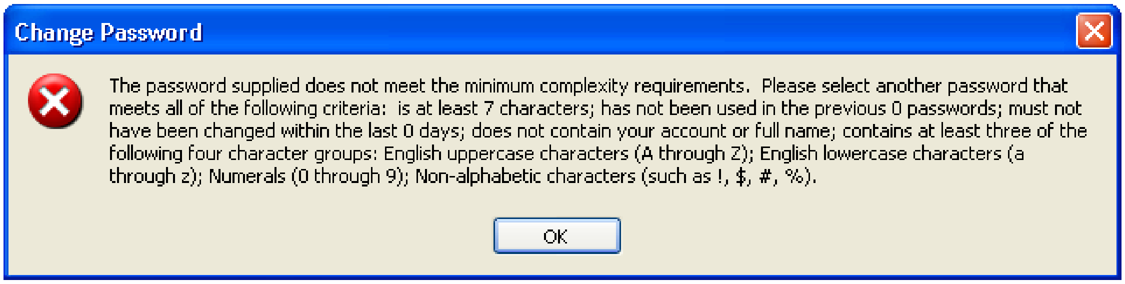
a) This message appears if your password does not meet password policy requirements or if the old password has not expired (the default life period of a password is 1 day).

- **For Microsoft Windows Vista/7/Microsoft Windows Server 2008/2008 R2:**



Unable to update the password. The value provided for the new password does not meet the length, complexity, or history requirements of the domain.

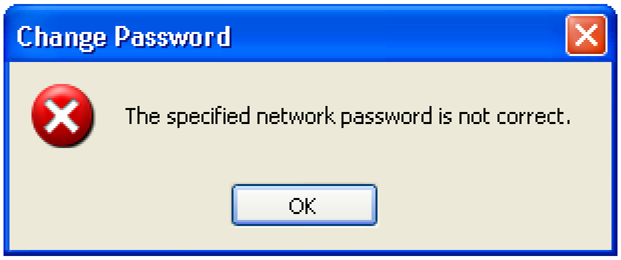
- **For Microsoft Windows Server 2003:**



Change Password

The password supplied does not meet the minimum complexity requirements. Please select another password that meets all of the following criteria: is at least 7 characters; has not been used in the previous 0 passwords; must not have been changed within the last 0 days; does not contain your account or full name; contains at least three of the following four character groups: English uppercase characters (A through Z); English lowercase characters (a through z); Numerals (0 through 9); Non-alphabetic characters (such as !, $, #, %).

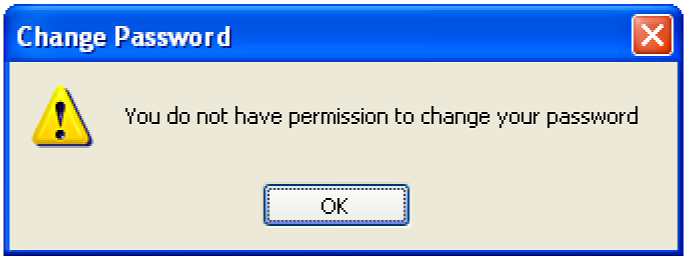
b) This message appears if you have mistyped your old password:



Change Password

The specified network password is not correct.

c) This message appears if NetIQ administrator disabled manual password change:



Change Password

You do not have permission to change your password

Solution:

a) Enter a new password, which meets the specified requirements or try again after the old password has expired. For more information, contact your NetIQ administrator.

b) Check and re-type the old password or get your password.

c) Contact NetIQ administrator.

Cannot Enroll Authenticator

Description:

Authenticator is not enrolled because:

a. The authentication device is not functioning.
b. The **Type** list in the **Enroll Authenticators** window is empty or some authenticator types are absent.
c. The **Enroll** button in the **Authenticators** window is greyed out.

Cause:

a. The device is unplugged, out of order or the proper drivers are not installed.
b. The authenticator type is not supported (no proper authentication provider is installed).
c. The operation is forbidden or you have reached the limit on the number of authenticators.

Solution:

a. Make sure the device is plugged in. Refer to device manual. If the device seems out of order, contact NetIQ administrator.
b. Contact NetIQ administrator.
c. No authenticators can be added. For more information, contact NetIQ administrator.

Cannot Save Authenticator

Description:

When you are using a flash drive or a memory card as authentication device, an error message appears upon saving an authenticator.

Cause:

The device is write-protected.

Solution:

Remove write protection.

Index

A

Authentication 1, 4-6, 8-10, 15, 38, 46, 50-55, 58, 61
Authenticator 4, 6, 8, 15, 18, 20, 51, 57, 65-66
Authenticore server 61
Automatic logon 38

C

Caching 11, 38, 46
Client 1, 9-10, 44, 54, 58
Client Tray 15, 46, 52-53
Connection 38

D

Desktop 38
Dial-up 24, 30, 32, 34, 36
Domain 23, 29

E

Enroll 8, 57, 65

L

Local 52
Locking computer 47
Logon 4, 10, 12, 17, 20-21, 23, 27, 29, 34, 38, 44, 50, 52, 55

M

Manage 24, 30, 42
Microsoft Windows Server 2003 10, 12, 21, 23, 27, 29, 32, 34, 40, 42, 47, 49, 63

N

Network 32, 35
Non-Network Logon 20, 38

P

Password 11-12, 14, 20, 27, 30-31, 40-42, 44, 52, 55, 57, 63

R

Re-enroll 8

Remote 20, 32, 38
Remove 66
Run As 7, 50-51, 55

S

Security 24, 30
Server 5
Settings 46, 52-54, 56
Support 39-40, 44, 57-58
System 15, 58

T

Terminal Logon 20, 38
Test 17

U

Unlocking Computer 47-48
User 1, 4, 8-9, 11, 21, 23, 27, 29, 32, 34
User's workstation 9

W

Windows 11-12, 14, 22-23, 25, 28-29, 31, 34, 39-40, 42, 47
Windows 7 40, 44
Windows 8 10, 14, 21, 25, 27, 31-32, 36
Windows Vista 10-11, 21, 27, 32, 40, 47-48, 63
Workstation 8, 10