
Installation Guide

Advanced Authentication - Windows Client

Version 5.6

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 System Requirements	9
2 Configuring the Preliminary Settings	11
2.1 Setting DNS for Server Discovery	11
2.2 Disabling 1:N	14
2.3 Using a Specific Advanced Authentication Server	15
2.4 Disabling Local Accounts	15
2.5 Configuration Settings for Multitenancy	15
2.6 Selecting an Event	15
2.7 Configuring Timeout for Card Waiting	16
2.8 Enabling Logon Failure after Card Timeout	16
2.9 Configuring Automatic Logon	16
2.10 Customizing a Logo	16
2.11 Configuring for Verification of Server Certificates	17
2.12 Configuring to Force Offline Login Manually	17
2.13 Configuring Single Sign-on Support for Citrix and Remote Desktop	18
3 Installing and Uninstalling Windows Client	19
3.1 Installing Windows Client	19
3.2 Uninstalling Windows Client	19
3.2.1 Microsoft Windows 7	20
3.2.2 Microsoft Windows 8.1	20
3.2.3 Microsoft Windows 10	20
4 Client Login Extension Support for Windows Client	21
5 Troubleshooting for Windows	23
5.1 Chain Icons Cannot be Updated	23
5.2 Long Boot	24
5.3 Endpoint Not Found	24
5.4 Password Synchronization Does Not Work On Standalone Workstations	24
5.5 Cannot Restrict Users to Use Specific Workstations	25

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About this Book

The Windows Client Installation guide has been designed for users and describes the system requirements and installation procedure for Windows Client.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

About Windows Client

Windows Client enables you to log in to Microsoft Windows in a more secure way by using the authentication chains configured in Advanced Authentication.

Advanced Authentication Windows Client supports offline logon (when the Advanced Authentication server is not available) for non-local accounts of the authentication chains that contain the methods: LDAP Password, Password, PKI, HOTP, TOTP, Smartphone (offline mode), Card, FIDO U2F, and Fingerprint.

TIP: To login with Microsoft account, specify <WorkstationName>\<MicrosoftAccount> in **user name**. For example, win81x64\pjones@live.com.

NOTE: You cannot use the command **Run as administrator** with a domain account on a non-domain workstation.

1 System Requirements

You must have the local administrator privileges to install and uninstall Windows Client.

Ensure that the following requirements are met:

- ♦ Microsoft Windows 7 (x64/x86) SP1 / Microsoft Windows 8.1 (x64/x86) / Microsoft Windows 10 (x64/x86) / Microsoft Windows Server 2008 R2 / Microsoft Windows Server 2012 R2 / Microsoft Windows Server 2016 is installed.
- ♦ DNS is configured appropriately for Advanced Authentication server discovery (see [Setting DNS for Server Discovery](#)) or a specific Advanced Authentication server must be specified in the [configuration file](#).

2 Configuring the Preliminary Settings

This chapter contains sections about the pre-configuration settings on Windows Client.

- ◆ You need to setup an interaction between Windows Client and Advanced Authentication server.
 - ◆ To make Windows Client interact with Advanced Authentication servers through DNS, see [“Setting DNS for Server Discovery”](#).
- Or
- ◆ To manually specify a custom Advanced Authentication server, see [“Using a Specific Advanced Authentication Server”](#).
- ◆ If you want to use both domain-joined and non-domain machines, you can use a custom event for the specific machines. For more information, see [“Selecting an Event”](#).

In a non-domain mode, it is recommended to disable the local accounts. For more information, see [“Disabling Local Accounts”](#).
- ◆ If you use Multitenancy, you must point Windows Client to a specific tenant. For more information, see [“Configuration Settings for Multitenancy”](#).
- ◆ **Optional Settings:**
 - ◆ To disable automatic detection of username for Card and PKI methods, see [“Disabling 1:N”](#).
 - ◆ To change a default Card waiting timeout, see [“Configuring Timeout for Card Waiting”](#).
 - ◆ To emulate the logon failure after the Card waiting timeout, see [“Enabling Logon Failure after Card Timeout”](#).
 - ◆ To configure an automatic logon, see [“Configuring Automatic Logon”](#).
 - ◆ To customize a logo for Windows Client, see [“Customizing a Logo”](#).
 - ◆ To configure the verification of server certificates for LDAP connection, see [“Configuring for Verification of Server Certificates”](#).
 - ◆ To force offline login manually for users, see [“Configuring to Force Offline Login Manually”](#).
 - ◆ To configure single sign-on for Citrix and Remote Desktop, see [“Configuring Single Sign-on Support for Citrix and Remote Desktop”](#).

2.1 Setting DNS for Server Discovery

- 1 Open a DNS Manager. To open the DNS Manager, click **Start**, point to **Administrative Tools**, and click **DNS**.
- 2 Add Host A or AAAA record and PTR record:
 - 2a In the console tree, right-click the forward lookup zone that includes your domain name and click **New Host (A or AAAA)**.
 - 2b Specify a DNS name for the Advanced Authentication Server in **Name**.

- ♦ **Name:** domain name for which this record is valid. It ends with a dot.
- ♦ **TTL:** standard DNS time to live field.
- ♦ **Class:** standard DNS class field (this is always IN).
- ♦ **Priority:** priority of the target host. Lower value indicates that it is more preferable.
- ♦ **Weight:** a relative weight for records with the same priority. Higher value indicates that it is more preferable.
- ♦ **Port:** TCP or UDP port on which the service is located.
- ♦ **Target:** host name of the machine providing the service. It ends with a dot.

Configuring Authentication Server Discovery on Client

You can use the following options for server discovery on the client:

- ♦ `discovery.Domain`: DNS name of the domain. For Windows Client, this value is used if workstation is not connected to the domain.
- ♦ `discovery.subDomains`: list of additional sub domains separated by a semicolon. You can use them on MacOS Client or Linux Client to list Active Directory sites.
- ♦ `discovery.useOwnSite`: Set the value to `True` to use the local site (Windows Client only).
- ♦ `Authentication Server Discovery Flowdiscovery.dnsTimeout`: Time out for the DNS queries. The default value is 15 seconds.

Authentication Server Discovery Flow

Windows Client

The feature is not supported for Windows Client.

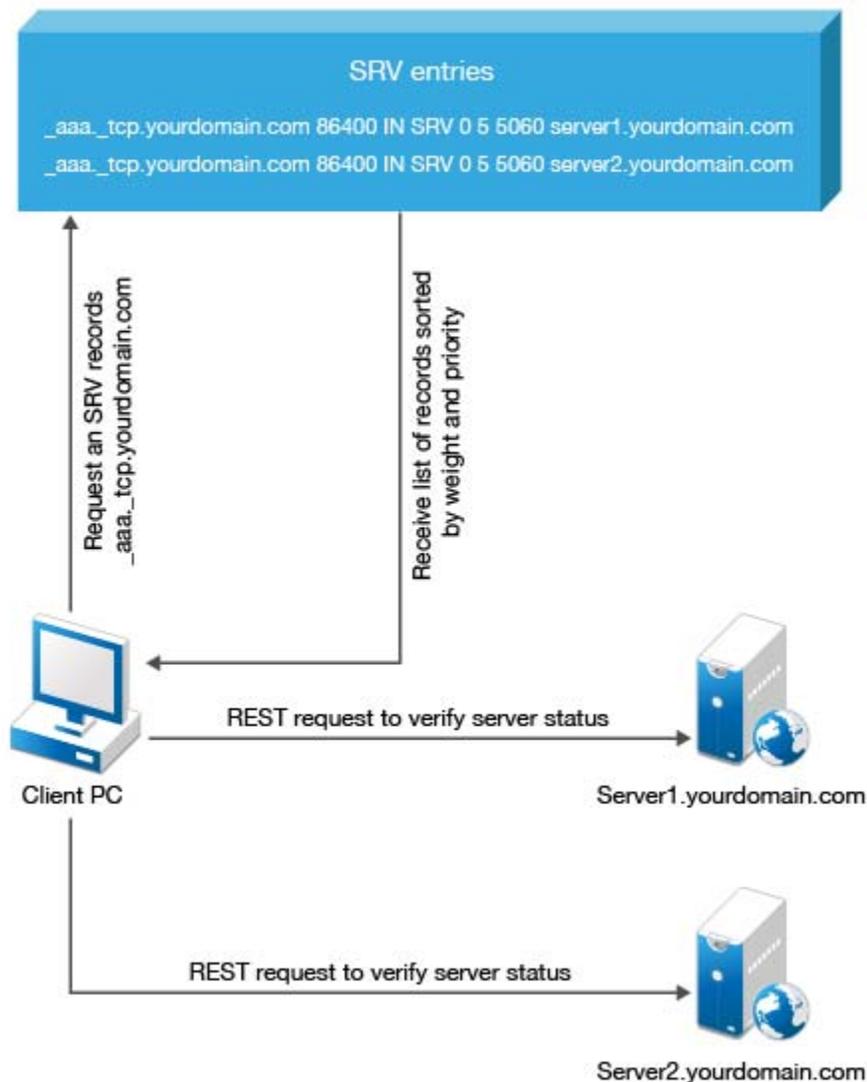
MacOS Client/ Linux PAM module

1. Get servers from the sub domains listed in `discovery.subDomain`.
2. Get servers from the domain specified in `discovery.Domain` (global list).

Path for the configuration file for MacOS Client and Linux PAM module is:

- ♦ **MacOS Client:** `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.
- ♦ **Linux PAM module:** `/opt/pam_aucore/etc/pam_aucore.conf`.

The following diagram illustrates the server discovery workflow.



2.2 Disabling 1:N

You can disable the 1:N feature that allows you to detect the user name automatically while authenticating with the Card and PKI methods.

To disable the 1:N feature, perform the following steps:

- 1 Open the file `C:\Program Data\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
- 2 Add the line `disable_1N: true` to the file.
- 3 Save the file and restart the operating system.

2.3 Using a Specific Advanced Authentication Server

You can specify an Advanced Authentication server on a workstation that can be used when a workstation is not joined to a domain. You can also use this option when the user wants to force a connection to a specific Advanced Authentication server when a workstation with Windows Client is joined to a domain.

In the `C:\ProgramData\NetIQ\Windows Client\config.properties` file, configure `discovery.host = <IP_address|domain_name>`.

For example, `discovery.host = 192.168.20.40` or `discovery.host = auth2.mycompany.local`.

You can specify a port number (optional parameter) for the client-server interaction: `discovery.port = <portnumber>`.

NOTE: For **Windows logon** event, select the **OS Logon (local)** Event type if you want to use Windows Client on non-domain joined workstations.

2.4 Disabling Local Accounts

It is recommended to disable local accounts for the non-domain mode to ensure security.

To disable local accounts, perform the following steps:

- 1 Open the file `C:\Program Data\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
- 2 Add a line `disable_local_accounts: true` to the file.

If you do not disable the local accounts for a non-domain mode, it is possible to unlock the operating system and change the password using a local account with password authentication (one factor). This can lead to security issues.

2.5 Configuration Settings for Multitenancy

If Multi-tenancy is enabled, you must add the parameter `tenant_name` with a used tenant name as the value in the configuration file: `C:\ProgramData\NetIQ\Windows Client\config.properties`. For example, specify `tenant_name=TOP` for the top tenant in the file. If the configuration file does not exist, you must create it.

NOTE: If you do not add the parameter `tenant_name`, you might get an error `Tenant not found`.

2.6 Selecting an Event

By default, Windows Client uses the Windows logon event. However, in some scenarios you must create a separate event. For example, when the predefined event is used for domain joined workstations, you can create a custom event with type `Generic` for the non-domain joined workstations. In this case you will need to point these non-domain workstations to the custom event using the following parameter in the `event_name: <CustomEventName>` configuration file:

`C:\ProgramData\NetIQ\Windows Client\config.properties`

2.7 Configuring Timeout for Card Waiting

You can configure the time for which the card waiting dialog is displayed, when the user authenticates using the card method. If the user does not present the card for the timeout period, the `Hardware timeout` message is shown and then the card waiting dialog is closed and user login selection screen is displayed.

By default the card timeout is 60 seconds.

To configure the timeout for card waiting, perform the following steps:

1. Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
2. Enter `card.timeout: X` in the `config.properties` file. X is the timeout value in seconds.
3. Save the configuration file.
4. Restart the operating system.

2.8 Enabling Logon Failure after Card Timeout

By default card timeout is not considered as a logon failure. However, if required you can configure the card timeout as a logon failure. To enable logon failure during card timeout, perform the following steps:

1. Open the file `C:\ProgramData\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
2. Enter `card.fail_on_timeout: true` in the `config.properties` file.
3. Save the configuration file.
4. Restart the operating system.

2.9 Configuring Automatic Logon

To enable the system to perform an automatic logon, perform the following steps:

- 1 Go to `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon`
- 2 In registry key, set the following parameters:
 - ◆ `DefaultDomainName`
 - ◆ `DefaultPassword`
 - ◆ `DefaultUserName`

For more information about how to enable automatic logon on Windows, see the [link](#).

2.10 Customizing a Logo

You can customize the logo of Windows Client according to your requirement. The format of the logo must meet the following requirements:

- ◆ **Image format:** `png, jpg, gif`
- ◆ **Resolution:** `400x400px`
- ◆ **Maximum file size:** `100Kb`

To customize the logo, perform the following steps:

1. Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
2. Enter `logo_path: C:\\dir\\filename.png`.
You cannot use the logo from shared folders.
3. Save the configuration file.
4. Restart the machine.

2.11 Configuring for Verification of Server Certificates

This option allows you to ensure a secure connection between a workstation and Advanced Authentication Servers with a valid self-signed SSL certificate, thus preventing any attacks on the connection and ensuring safe authentication.

The option for verification of server certificates is disabled by default. You must start by importing the trusted certificates to the `Local Computer\Trusted Root Certification Authorities` folder.

To disable verification of the server certificates, perform the following steps:

1. Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
2. Enter `verifyServerCertificate: true` (default value is `false`).
3. Restart the machine.

2.12 Configuring to Force Offline Login Manually

When the network connection is slow or unstable, the login process might take several minutes. A solution to this is to allow users to force offline login manually. This saves the user's time for the login process.

To allow users to force offline login manually, perform the following steps:

1. Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`. If the file does not exist, create a new file.
2. Specify `force_offline_enabled: true` (default value is `false`) in the `config.properties` file.
3. Save the configuration file.
4. Restart the operating system.

When you set the parameter to `true`, an **Offline logon** check box appears on the user's login screen. If a user selects **Offline logon**, Windows Client does not try to reach an Advanced Authentication server but goes directly to cache.

You can also set the offline login as a default value by specifying `force_offline_default: true` in the `config.properties` file. This enables the **Offline logon** check box to be selected by default on the user's login screen.

NOTE: Before you force offline login, a user must have logged into the workstation once (with online login) to cache the authenticators.

2.13 Configuring Single Sign-on Support for Citrix and Remote Desktop

You can configure the Windows Client to use the single sign-on feature for establishing a connection to a Citrix and a Remote Desktop server. Hence, when the users are authenticated to the Windows domain, they are not prompted for credentials to connect to the terminal servers such as, Citrix StoreFront and Remote Desktop Connection. This facilitates users not to specify the credentials again when they login to terminal server such as Remote Desktop or Citrix StoreFront, after they have performed the authentication to Microsoft Windows. To achieve this, you must install the Advanced Authentication Windows Client on the terminal server.

The single sign-on feature is enabled by default for accessing terminal servers. To disable this feature, perform the following steps:

- 1 Open the `config.properties` at `C:\ProgramData\NetIQ\Windows Client\config.properties`.
If the file does not exist, create a new file.
- 2 In the `config.properties` file, specify `sso_logon_enabled: false`.
- 3 Save the configuration file.
- 4 Restart the operating system.

3 Installing and Uninstalling Windows Client

This chapter contains the following sections:

- ♦ [Installing Windows Client](#)
- ♦ [Uninstalling Windows Client](#)

NOTE: When you upgrade from Windows Client 5.2, the endpoints are not removed automatically. The administrator must remove the endpoints manually. For installation instructions, see [“Installing Windows Client”](#).

You can find the Windows Client in the Advanced Authentication Enterprise Edition distributive package.

3.1 Installing Windows Client

To install Windows Client with the setup wizard, perform the following steps:

- 1 See the **System properties** (Control Panel > All Control Panel Items > System) to detect your **System type**.
- 2 Run `naaf-winclient-x86-release-<version>.msi` for 32-bit operating system or `naaf-winclient-x64-release-<version>.msi` for 64-bit operating system.
- 3 Click **Next**.
- 4 Accept the **License Agreement** and click **Next**.
- 5 Click **Next** to install on the default folder or click **Browse** to select a different folder.
- 6 Click **Install**.
- 7 Click **Finish**.

NOTE: If you are installing Windows Client on a non-domain workstation, create a configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties` before you restart the system and follow the procedure in the section [“Using a Specific Advanced Authentication Server”](#) to specify an Advanced Authentication server.

3.2 Uninstalling Windows Client

You can uninstall Windows Client through the setup wizard or Control Panel.

NOTE: You must uninstall Windows Client only when the Advanced Authentication server is available. Otherwise the endpoint is not removed automatically and administrator will need to remove it manually.

To uninstall Windows Client through the setup wizard, perform the following steps:

- 1 Run `naaf-winclient-x86-release-<version>.msi` for 32-bit operating system or `naaf-winclient-x64-release-<version>.msi` for 64-bit operating system.
- 2 Click **Next**.
- 3 Select **Remove** and click **Next**.
- 4 Click **Remove** to confirm removal.

You can remove Windows Client through the Control Panel based on your corresponding operating system:

- ♦ [Microsoft Windows 7](#)
- ♦ [Microsoft Windows 8.1](#)
- ♦ [Microsoft Windows 10](#)

3.2.1 Microsoft Windows 7

- 1 In the **Start** menu, select **Control panel** and then double-click **Programs and Features**.
- 2 Select NetIQ **Windows Client** and click **Uninstall**.
- 3 Confirm the removal.

3.2.2 Microsoft Windows 8.1

- 1 In the **Search** menu, select **Apps > Control Panel > Programs > Programs and Features**.
- 2 Select NetIQ **Windows Client** and click **Uninstall**.
- 3 Confirm the removal.

3.2.3 Microsoft Windows 10

- 1 Right-click **Start** and select **Control Panel > Programs > Programs and Features**.
- 2 Select NetIQ **Windows Client** and click **Uninstall**.
- 3 Confirm the removal.

4 Client Login Extension Support for Windows Client

You can now reset your password through Client Login Extension that facilitates password self-service by adding a link to the Windows login screen. When you click the **Forgot Password** link on the **LDAP Password** method page, the login client launches the Client Login Extension restricted browser to access the Self Service Password Reset password reset page. You can use Client Login Extension to configure the label for the URL that should be displayed for the **LDAP password** method page in Windows Client.

Prerequisites

Ensure that the following prerequisites are met before you use Client Login Extension for the password reset on Windows Client:

- ◆ Client Login Extension is installed on your Windows Client. The recommended version is CLE 3.10 and later. For information on Client Login Extension, see the [NetIQ Client Login Extension 3.10 Administration Guide](#).
- ◆ Self Service Password Reset is installed in the environment.

5 Troubleshooting for Windows

To investigate the possible issues you may be asked to collect the debug logs.

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Click **Clear All** (if applicable) in the **Debug logs** tab.
3. Click **Enable**.
4. Restart the system.
5. Reproduce your problem.
6. Run `DiagTool.exe`.
7. Click **Save logs** in the **Debug logs** tab.
8. Specify a file name and path. Click **Save** to save the logs.
9. Click **Disable** to disable the logging.
10. Click **Clear All**.

If you don't have the Diagnostic Tool you can perform the actions manually:

1. Create a text file `C:\ProgramData\NetIQ\Logging\config.properties`.
2. Add a string to the file: `logEnabled=True` that ends by a line break.
3. Create a directory: `C:\ProgramData\NetIQ\Logging\Logs\`.
4. Restart the machine.
5. Reproduce your problem.
6. Pack the logs located in `C:\ProgramData\NetIQ\Logging\Logs\` into a zip file.
7. Change `logEnabled=True` to `logEnabled=False` in the folder, `C:\ProgramData\NetIQ\Logging\config.properties`

With the Diagnostic Tool, you can check the network problems on a workstation, issues in connection between a workstation and DNS Server, and to get a list of the Advanced Authentication Servers that can be discovered. To this, perform the following steps:

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
2. Switch to the **Servers** tab.
3. In the **Search settings** you must enter FQDN in **Domain** and click **Search**. A list of Advanced Authentication Servers is displayed.
4. If the list is not displayed, clear **Use system DNS server** and enter the IP address of your DNS server in **DNS server** and click **Search** again.

5.1 Chain Icons Cannot be Updated

Issue

System administrator applied the new icons for the used authentication chains, but they were not updated on the Windows Client.

Solution

Windows Client does not update the icons to reduce the traffic. Please remove the folder `C:\ProgramData\NetIQ\Windows Client\logocache` to clear the icons cache.

5.2 Long Boot

Question:

With the Windows Client installed I experience longer Please wait screen during OS boot?

Answer:

It happens because Advanced Authentication has to wait for network to get and show a list of available authentication chains.

5.3 Endpoint Not Found

Issue

After installing the client component and rebooting, the client reports Endpoint not found error and it is not possible to login.

Reason

An endpoint for the client already exists on server or in configuration file on the client.

Solution

1. Remove the endpoint for the client on the server in Administrative Portal - Endpoints section (if it exists).
2. Boot in Safe mode and remove `endpoint_id`, `endpoint_name` and `endpoint_secret` parameters from `C:\ProgramData\NetIQ\Windows Client\config.properties`.
3. Reboot.

5.4 Password Synchronization Does Not Work On Standalone Workstations

Issue

Password synchronization is requested during the logon to standalone workstation. The synchronization is not done as the Wrong password. Try again error appears.

Solution

1. Ensure you specify a valid password.
2. Contact your system administrator to check if your workstation is pointed to an event with **OS logon (domain)** type. If the workstation is not joined to a domain, select the **OS logon (local)** or **Generic** event type.
3. Ask your system administrator to reset the password for your account.

5.5 Cannot Restrict Users to Use Specific Workstations

Issue: When you restrict the kiosk user accounts to use specific computers in Active Directory, and users try to login to Windows with those accounts, an `Invalid Credentials` error message is displayed from the Advanced Authentication Windows Client. If the option is changed to **This user can log on to All computers** in Active Directory, the account is able to login successfully. This happens because when using the LDAP Password method, Advanced Authentication tries to bind to Domain Controller to validate the password and it fails.

Workaround: Perform the following:

- 1 Open the user properties from the Domain Controller and goto the **Account** tab and click **Log on To**.
- 2 Add Domain Controllers to the list of allowed workstations for that particular user.
- 3 Now to prevent that user from accessing the Domain Controllers, go to **Group Policy Management > Domain Controllers > Default Domain Controller policy > Edit**.
- 4 Then from the **Group Policy Editor** go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
- 5 Add that particular user or a group to **Deny Log On Locally** and **Deny Log On Through Remote Desktop Services** in the Policy setting.
- 6 Run `gpupdate /force` to push these group policy changes.

