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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About NetIQ Corporation</td>
<td>5</td>
</tr>
<tr>
<td>About this Book</td>
<td>7</td>
</tr>
<tr>
<td>1 System Requirements</td>
<td>9</td>
</tr>
<tr>
<td>2 Preliminary Configuration</td>
<td>11</td>
</tr>
<tr>
<td>2.1 How to Set DNS for Server Discovery</td>
<td>11</td>
</tr>
<tr>
<td>2.2 Disabling 1:N</td>
<td>15</td>
</tr>
<tr>
<td>2.3 Using a Specific Advanced Authentication Server</td>
<td>15</td>
</tr>
<tr>
<td>2.4 Disabling Local Accounts</td>
<td>15</td>
</tr>
<tr>
<td>2.5 Configuring Windows Client Ports</td>
<td>15</td>
</tr>
<tr>
<td>2.6 Configuration Settings for Multitenancy</td>
<td>16</td>
</tr>
<tr>
<td>2.7 Selecting an Event</td>
<td>16</td>
</tr>
<tr>
<td>3 Installing and Removing Windows Client</td>
<td>17</td>
</tr>
<tr>
<td>3.1 Installing Windows Client</td>
<td>17</td>
</tr>
<tr>
<td>3.2 Removing Windows Client</td>
<td>17</td>
</tr>
<tr>
<td>3.2.1 Microsoft Windows 7</td>
<td>18</td>
</tr>
<tr>
<td>3.2.2 Microsoft Windows 8.1</td>
<td>18</td>
</tr>
<tr>
<td>3.2.3 Microsoft Windows 10</td>
<td>18</td>
</tr>
<tr>
<td>4 Troubleshooting for Windows</td>
<td>19</td>
</tr>
<tr>
<td>4.1 Chain Icons Cannot be Updated</td>
<td>19</td>
</tr>
<tr>
<td>4.2 Long Boot</td>
<td>20</td>
</tr>
<tr>
<td>4.3 Endpoint Not Found</td>
<td>20</td>
</tr>
</tbody>
</table>
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 User Guide has been designed for all users and describes the system requirements and the 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 replaces standard way of log on to Microsoft Windows by a more secure using the authentication chains configured in Advanced Authentication.

**IMPORTANT:** 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 log on with Microsoft account enter `<WorkstationName>\<MicrosoftAccount>` in the username field, e.g. `win81x64\pjones@live.com`.

**NOTE:** Use of Run as administrator with a domain account on a non-domain workstation is not supported.
1 System Requirements

**IMPORTANT:** Installing and removing Windows Client requires Local Admins privileges.

The following system requirements should be fulfilled:

- 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.
- DNS is properly configured for Advanced Authentication Server discovery (see How to Set DNS for Server Discovery) or a specific Advanced Authentication server must be specified in the configuration file.
The chapter contains articles about required pre-configuration.

- Section 2.1, “How to Set DNS for Server Discovery,” on page 11
- Section 2.2, “Disabling 1:N,” on page 15
- Section 2.3, “Using a Specific Advanced Authentication Server,” on page 15
- Section 2.4, “Disabling Local Accounts,” on page 15
- Section 2.5, “Configuring Windows Client Ports,” on page 15
- Section 2.6, “Configuration Settings for Multitenancy,” on page 16
- Section 2.7, “Selecting an Event,” on page 16

## 2.1 How to Set DNS for Server Discovery

**Question:**

I would like to set DNS for server discovery. How can I do it and what is its workflow?

**Answer:**

To set a DNS for the Server Discovery, perform the following steps:

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:
   a. In the console tree, right-click the forward lookup zone that includes your domain name and click New Host (A or AAAA).
   b. Specify a DNS name for the Advanced Authentication Server in Name.
   c. Specify the IP address for the Advanced Authentication Server in IP address. You can specify the address in IP version 4 (IPv4) format (to add a host (A) resource record) or IP version 6 (IPv6) format (to add a host (AAAA) resource record).
   d. Select Create associated pointer (PTR) record to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you provided in Name and IP address.
3. Add an SRV record:
   a. For Advanced Authentication servers from a primary Advanced Authentication site (a site with Global Master server):
      i. In the console tree, locate Forward Lookup Zones and right-click on a node with domain name and click Other New Records.
      ii. In the Select a resource record type list, click Service Location (SRV) and then click Create Record.
      iii. Click Service and then specify _aaa.
      iv. Click Protocol and then specify _tcp.
v. Click **Port Number** and then specify **443**.

vi. In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.

vii. Click **OK**.

b. For Advanced Authentication servers from the other Advanced Authentication sites:

i. In the console tree, locate **Forward Lookup Zones**, switch to a node with domain name then to `_sites` node, right-click on an appropriate site name and click **Other New Records**.

ii. In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.

iii. Click **Service** and then specify `_aaa`.

iv. Click **Protocol** and then specify `_tcp`.

v. Click **Port Number** and then specify **443**.

vi. In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.

vii. Click **OK**.

Repeat steps 2 to 3 for all the authentication servers. The Priority and Weight values for different servers may vary.

**DNS server contains** SRV entries `_service._proto.name TTL class SRV priority weight port target`. The following descriptions define the elements present in the DNS server:

- **Service**: symbolic name of an applicable service
- **Proto**: transport protocol of an applicable service. Mostly, TCP or UDP.
- **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**: canonical host name of the machine providing the service. It ends with a dot.

**Configuring Authentication Server Discovery on client side**

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

- **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 AD sites.
- **discovery.useOwnSite**: Set the value to **True** to use the local site (Windows Client only).
- **discovery.dnsTimeout**: Time out for the DNS queries. The default value is 15 seconds.

**Authentication Server Discovery Flow**

Windows Client

The feature is not supported in 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 is as follows:

- **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 graphically.
SRV entries

aaa._tcp.yourdomain.com 86400 IN SRV 0 5 5060 server1.yourdomain.com
aaa._tcp.yourdomain.com 86400 IN SRV 0 5 5060 server2.yourdomain.com

Client PC

Request an SRV records _aaa._tcp.yourdomain.com

Receive list of records sorted by weight and priority

REST request to verify server status

Server1.yourdomain.com

REST request to verify server status
2.2 Disabling 1:N

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

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 a certain Advanced Authentication server on a workstation that can be used when a workstation is joined to a domain, but user wants to force connection to a specific Advanced Authentication server and when a workstation with Windows Client is not 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:

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 Configuring Windows Client Ports

You can configure the ports in the file C:\ProgramData\NetIQ\Windows Client\config.properties.

port: 8082, which is the default port, is used to interact with the Advanced Authentication server.

offline.port: 8082, which is the default port, is used to interact with the local cache server if local caching is enabled.
2.6 Configuration Settings for Multitenancy

If Multi-tenancy is enabled, you must add the parameter `tenant_name` with a used tenant name as 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`.

2.7 Selecting an Event

By default Windows logon event is used. However, in some cases it is required to 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`

**NOTE:** Caching is not supported for the custom events.
3 Installing and Removing Windows Client

In this chapter:

- Installing Windows Client
- Removing Windows Client

**NOTE:** To upgrade the Windows Client from 5.2 to 5.4, you must not uninstall 5.2 because it does not support the removal of endpoints during uninstallation. In this case, the administrator will have to remove the endpoint manually. See Installing Windows Client to perform the upgrade.

### 3.1 Installing Windows Client

To install Windows Client via Setup Wizard:

1. Check System properties (Control Panel\All Control Panel Items\System) to detect your System type.
3. Click Next to continue.
4. Read the License Agreement. Select the I accept the terms in the license agreement checkbox and click Next.
5. Click Next to install to the default folder or click Browse to choose another.
   - To change the destination folder, click the Change button and select an applicable destination.
   - To continue, click Next.
6. Click Install and wait until the component is installed.
7. Click Finish to close the Wizard.

**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 and follow the procedure in the section "Using a Specific Advanced Authentication Server" to specify an Advanced Authentication server.

**IMPORTANT:** It is required to set Require admin password to register endpoint/workstation to OFF in Endpoint management options on Advanced Authentication Administrative Portal. Otherwise the required endpoint won't be created.

8. Click Yes to restart the operating system.

### 3.2 Removing Windows Client

Windows Client can be removed via Setup Wizard or Control Panel.
NOTE: It is recommended to remove the component only in the online mode, when Advanced Authentication Server is available. Otherwise the endpoint will not be removed and administrator will need to remove it manually.

To remove Windows Client via Setup Wizard, follow the steps:

2. Click Next to continue.
3. Select Remove as an applicable operation and click Next to remove Windows Client from your computer.
4. Click Remove to confirm removal.

To remove Windows Client via Control Panel, select one of the links that corresponds to your 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.
4. Wait a few seconds until the removal is completed.

### 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.
4. Wait a few seconds until the removal is completed.

### 3.2.3 Microsoft Windows 10

1. Right-click the Start button and select Control Panel > Programs > Programs and Features.
2. Select NetIQ Windows Client and click Uninstall.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.
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.
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.

### 4.1 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.

**4.2 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.

**4.3 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.