

---

# Installation and Configuration Guide

## Advanced Authentication - Windows Client

Version 6.0

## 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 © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.**

---

# Contents

<b>About NetIQ Corporation</b>	<b>5</b>
<b>About this Book</b>	<b>7</b>
<b>1 System Requirements</b>	<b>9</b>
<b>2 Configuring the Preliminary Settings</b>	<b>11</b>
Setting DNS for Server Discovery . . . . .	12
Disabling 1:N . . . . .	15
Using a Specific Advanced Authentication Server . . . . .	15
Disabling Local Accounts . . . . .	15
Configuration Settings for Multitenancy . . . . .	16
Selecting an Event . . . . .	16
Configuring Timeout for Card Waiting . . . . .	16
Enabling Logon Failure after Card Timeout . . . . .	16
Configuring Automatic Logon . . . . .	17
Customizing a Logo . . . . .	17
Configuration for Verification of Server Certificates . . . . .	17
Configuring to Force Offline Login Manually . . . . .	18
Configuring Single Sign-on Support for Citrix and Remote Desktop . . . . .	18
Customizing Logon Page Background Screen . . . . .	19
Configuration to Enable the Authentication Agent Chain . . . . .	20
Configuring Integration with Sophos SafeGuard 8 . . . . .	21
Configuring the Credential Provider Chaining . . . . .	21
<b>3 Installing and Uninstalling Windows Client</b>	<b>23</b>
Installing Windows Client . . . . .	23
Uninstalling Windows Client . . . . .	23
Microsoft Windows 7 . . . . .	24
Microsoft Windows 8.1 . . . . .	24
Microsoft Windows 10 . . . . .	24
<b>4 Troubleshooting for Windows</b>	<b>25</b>
Debugging Logs for Advanced Authentication . . . . .	25
Logging for Windows Specific Advanced Authentication Events . . . . .	26
Chain Icons Cannot be Updated . . . . .	27
Long Boot . . . . .	27
Endpoint Not Found . . . . .	27
Password Synchronization Does Not Work On Standalone Workstations . . . . .	27
Cannot Restrict Users to Use Specific Workstations . . . . .	28
Unable to Login Due to JSON Parsing Error . . . . .	28



# 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.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

## 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](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto: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](http://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.

- ♦ Any of the following operating systems are installed:
  - ♦ Microsoft Windows 7 (x64 or x86) Service Pack1
  - ♦ Microsoft Windows 8.1 (x64 or x86)
  - ♦ Microsoft Windows 10 (v1703/ v1709/ v1803 x64 or x86)
  - ♦ Microsoft Windows Server 2008 R2
  - ♦ Microsoft Windows Server 2012 R2
  - ♦ Microsoft Windows Server 2016
- ♦ 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 [“Configuration 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”](#).
    - ♦ To customize the background image on logon page for Windows 7, see [“Customizing Logon Page Background Screen”](#).
    - ♦ To enable Authentication Agent chain in the Windows Client, see [“Configuration to Enable the Authentication Agent Chain”](#).
    - ♦ To integrate Advanced Authentication with the Sophos SafeGuard, see [“Configuring Integration with Sophos SafeGuard 8”](#).
    - ♦ To configure the credential provider chaining, see [“Configuring the Credential Provider Chaining”](#).

# 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**.
  - 2c 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).
  - 2d 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:

---

**NOTE:** Ensure that the LDAP SRV record exists at DNS server. If the record is not available, you must add it manually.

For best load balancing, you need to perform the following actions only for Advanced Authentication web servers. You need not create the records for Global Master, DB Master, and DB servers.

---

- 3a For Advanced Authentication servers from a primary Advanced Authentication site (a site with Global Master server):
  - 3a1 In the console tree, locate **Forward Lookup Zones** and right-click on a node with domain name and click **Other New Records**.
  - 3a2 In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.
  - 3a3 Click **Service** and then specify **\_aav6**.
  - 3a4 Click **Protocol** and then specify **\_tcp**.
  - 3a5 Click **Port Number** and then specify **443**.
  - 3a6 In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.
  - 3a7 Click **OK**.
- 3b For Advanced Authentication servers from other Advanced Authentication sites:
  - 3b1 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**.
  - 3b2 In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.
  - 3b3 Click **Service** and then specify **\_aav6**.
  - 3b4 Click **Protocol** and then specify **\_tcp**.
  - 3b5 Click **Port Number** and then specify **443**.
  - 3b6 In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.
  - 3b7 Click **OK**.

Repeat [Step 2](#) to [Step 3](#) for all the authentication servers. The Priority and Weight values for different servers may vary. For best load balancing, you need to have records only for Advanced Authentication web servers and you do not need to have the records for Global Master, DB Master, and DB servers.

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:** 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 side. You must add the parameters in the `config.properties` file.

- ♦ `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 Mac OS X 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 3 seconds.
- ♦ `discovery.connectTimeout`: Time out for the Advanced Authentication server response. The default value is 2 seconds.
- ♦ `discovery.resolveAddr`: Set the value to `False` to skip resolving the DNS. By default the value is set to `False` for Windows and Linux Clients and `True` for Mac Client.
- ♦ `discovery.wakeupTimeout`: Timeout after the system starts or resumes from sleep. The default value is 10 seconds.

## Authentication Server Discovery Flow

### Windows Client

The feature is not supported for Windows Client.

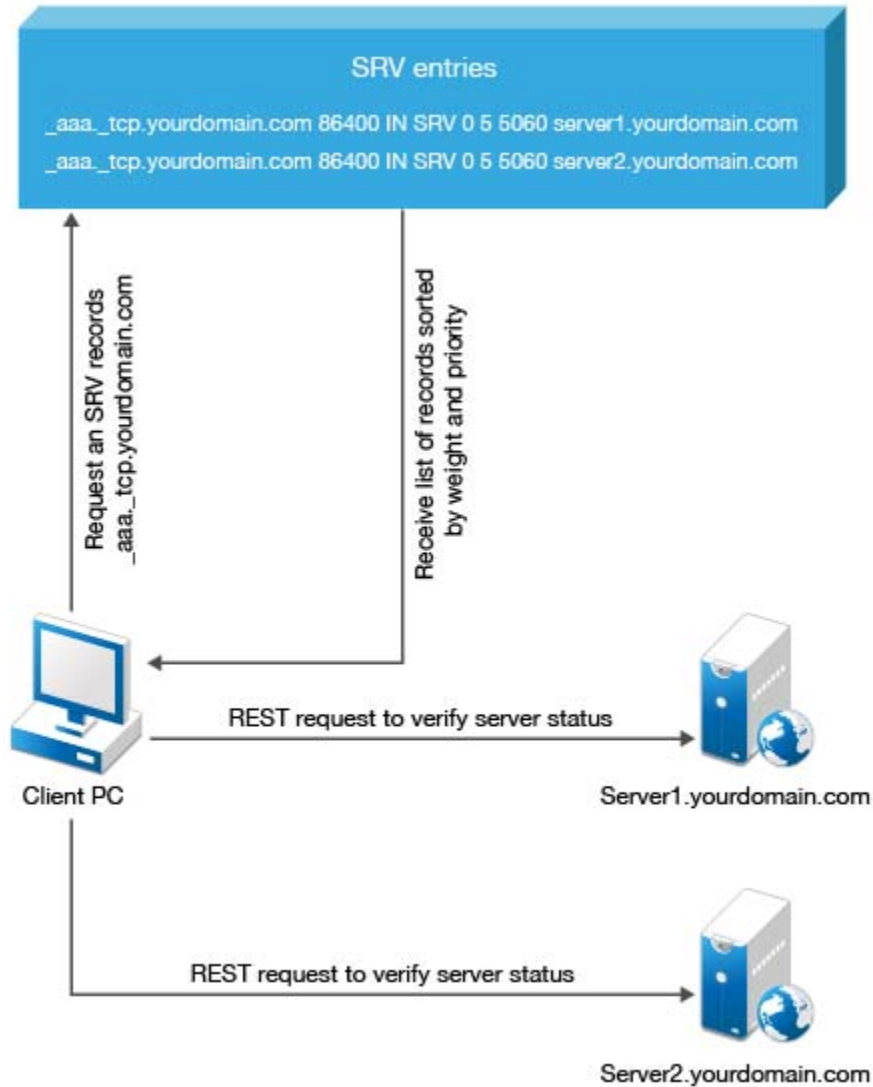
### MacOS Client/ Linux PAM module

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.



# 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.

## 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 multiple Advanced Authentication servers separated by a semicolon (;):

`discovery.hosts: aaf-1.domain.com;aaf-2.domain.com;...;aaf-n.domain.com`

You can specify a port number (optional parameter) for the client-server interaction:

`discovery.port: <portnumber>`.

The Advanced Authentication server receives the client connections through the port 443 by default. However, if the port redirection is configured on the network between the client and server then you can customize the port number manually. In the `config.properties` file of the client, you must use `discovery.port` parameter to enable the client to discover and pair with the Advanced Authentication server.

---

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

---

## 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.

# 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`.

---

## 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`

## 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.

## 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.



# 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 the registry key, it is mandatory to set the following parameters:
  - ♦ `DefaultDomainName`
  - ♦ `DefaultPassword`
  - ♦ `DefaultUserName`

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

## 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.

## Configuration 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 enable 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. Specify `verifyServerCertificate: true` (default value is `false`).
3. Restart the machine.

---

**NOTE:** You must upload the SSL certificate in the [Administration portal > Server Options](#). The SSL certificate provides high level of encryption, security, and trust. For more information about how to upload the SSL certificate, see [Uploading the SSL Certificate](#).

---

# 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 machine.

When you set the parameter to true, an **Offline login** check box appears on the user's login screen. If a user selects **Offline login**, 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 login** 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.

---

## 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.

---

**NOTE:** When the Single-sign on (SSO) for Remote Desktop is enabled, the [Interactive logon: Smart card removal behavior policy](https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-smart-card-removal-behavior) (<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-smart-card-removal-behavior>) is ignored. You need to disable SSO to make it working.

---

The single sign-on feature is enabled by default for accessing terminal servers and by default single sign-on feature works irrespective of Advanced Authentication Windows Client installation on the terminal client.

To enable single sign-on only when the Advanced Authentication Windows Client is installed on the terminal client, perform the following steps:

- 1 Open the `config.properties` at `C:\ProgramData\NetIQ\Windows Client` path.  
If the file does not exist, create a new file.
- 2 In the `config.properties` file, specify `sso_aaf_required: true` (default value is `false`).

- 3 Save the configuration file.
- 4 Restart the operating system.

To completely disable the single sign-on feature, perform the following steps:

- 1 Open the `config.properties` at `C:\ProgramData\NetIQ\Windows Client` path.  
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.

## Customizing Logon Page Background Screen

You can customize the background image of the logon page in the Windows 7 as per your requirement.

The default image is set as background on the logon page in Windows 7. To change background image, perform the following steps:

- 1 Launch **Start** and specify `regedit` in the **Run** command prompt.  
The **User Account Control** (UAC) prompt is displayed.
- 2 Click **YES** to navigate to the **Background** directory.

---

**NOTE:** The Background directory is located in `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI` directory.

---

- 3 Set `OEMBackground` entry to 1.

---

**NOTE:** If the `OEMBackground` entry does not exist then create an entry with the type **DWORD (32-bit) Value** and set value to 1.

---

- 4 Navigate to `C:\Windows\System32\Oobe` directory and create a directory as `info`.
- 5 Create a directory as `backgrounds` in the `info`.
- 6 Insert the preferred background image in `backgrounds` directory and rename the image as `backgrounddefault.jpg`.
- 7 Launch **Start** and specify `GPEDIT.MSC` in the **Run** command prompt.  
The **Local Group Policy Editor** prompt is displayed.
- 8 Navigate to `Local Computer Policy\Administrative Templates\System\Logon` directory.
- 9 Enable **Always use custom logon background** setting.

# Configuration to Enable the Authentication Agent Chain

The Authentication Agent allows you to authenticate on one computer where all the devices required for authentication are connected to get authorized access to another computer or z/OS mainframe, where one of the following condition is true:

- ♦ It is not possible to redirect the authentication devices.
- ♦ It does not support the devices used for authentication.

The Authentication Agent can be installed only on the Windows computer.

You must select **Authentication Agent** from the **Chains** list of Windows Client to initiate the authentication process on another Windows computer where the Authentication Agent is installed.

**To enable the Authentication Agent chain on the Windows Client, perform the following steps:**

- 1 Navigate to `C:\ProgramData\NetIQ\Windows Client` path and open the file `config.properties`.  
If the configuration file does not exist, you must create it.
- 2 Specify `authentication_agent_enabled = true` in the configuration file.
- 3 Click **Save**.
- 4 Restart your computer.

## An Example Scenario of Using the Authentication Agent

This scenario describes how you can perform authentication on one Windows computer and auto-sign in to another Windows computer using the Authentication Agent.

Thomas uses two Windows computers simultaneously. However, the devices required for authentication such as FIDO U2F token and card reader are connected to one Windows computer. He cannot get authenticated to the other computer because there are no authentication devices connected to this computer and cannot redirect the devices. In this case, Thomas can use Authentication Agent to perform authentication on one Windows computer and get seamless access to another Windows computer without the authentication devices.

Consider the following setup:

- ♦ Windows A is a computer with the Authentication Agent installed and is connected with the devices used for authentication such as FIDO U2F token and card reader.
- ♦ Windows B is computer without the authentication devices and the **Authentication Agent** chain is enabled using the `config.properties` file.

The following sequence describes the authentication process using the Authentication Agent:

- 1 Specify **user name** and select the **Authentication Agent** chain in Windows B computer.
- 2 The Authentication Agent on Windows A computer launches a restricted browser.
- 3 Select the chain mapped to Windows log on in the restricted browser.
- 4 Perform the authentication using the FIDO U2F token and card reader in the restricted browser.  
Thomas is logged in to Windows B computer automatically.

# Configuring Integration with Sophos SafeGuard 8

This section provides the configuration information on integrating Advanced Authentication with Sophos SafeGuard 8 easy solution. Hence, when the users are authenticated to Windows Client, they are not prompted for credentials to connect to the Sophos SafeGuard.

With this integration the Advanced Authentication is set as primary credential provider in the Windows Client. The Advanced Authentication server validates the user provided credentials and transmits the credentials to the Sophos credential provider to allow single sign-on to the Sophos SafeGuard.

To integrate Advanced Authentication with the Sophos SafeGuard 8, perform the following steps:

- 1 Navigate to the path `C:\ProgramData\NetIQ\Windows Client` and open the file `config.properties`.
- 2 Specify the following parameters with corresponding values in the configuration file:
  - ♦ `credprov_chaining_clsid: {5CDFA681-61C8-423d-999E-32EA10C5F7ED}`
  - ♦ `credprov_chaining_enabled: True`
  - ♦ `credprov_chaining_password_field: 9`
  - ♦ `credprov_chaining_username_field: 8`
- 3 Save the configuration.
- 4 Log off and log in again.

## Configuring the Credential Provider Chaining

This section describes the configuration information to integrate Advanced Authentication with any other credential provider in Windows Client. Hence, when the users are authenticated to Windows Client, they are not prompted for credentials to connect to other credential provider installed in the workstation.

To integrate Advanced Authentication with other credential provider, perform the following steps:

- 1 Enable the debug logs for Windows Client.  
For more information about debugging the logs of Windows Client, see [Debugging Logs for Advanced Authentication](#).
- 2 Navigate to the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\` and search for the CLSID of the preferred credential provider with which you want to integrate Advanced Authentication.  
Ensure to copy the CLSID for further use.
- 3 Navigate to the path `C:\ProgramData\NetIQ\Windows Client\` and open the file `config.properties`.
- 4 Specify the following parameters in the configuration file:
  - ♦ `credprov_chaining_clsid: <CLSID>`
  - ♦ `credprov_chaining_enabled: True`
  - ♦ `credprov_chaining_dump_fields: True`
  - ♦ `credprov_chaining_password_field: 0`
  - ♦ `credprov_chaining_username_field: 0`

For example: The CLSID of Sophos SafeGuard is 5CDFA681-61C8-423d-999E-32EA10C5F7ED. Therefore, set the CLSID parameter as follows:

```
credprov_chaining_clsid: {5CDFA681-61C8-423d-999E-32EA10C5F7ED}
```

5 Log off and log in again.

6 Navigate to the path C:\ProgramData\NetIQ\Windows Client\Logging\Logs then search for the parameter CpChaining::dumpFields in the logs file.

7 Search for the fields that contain label for the user name and password fields. Set the ID of these fields to the following parameters in the configuration file:

- ◆ credprov\_chaining\_password\_field:
- ◆ credprov\_chaining\_username\_field:

For example: Consider the Sophos SafeGuard 8 login form contains the user name and password fields. The ID of these fields are 8 and 9 respectively. Hence, the parameters are set as follows:

- ◆ credprov\_chaining\_password\_field: 9
- ◆ credprov\_chaining\_username\_field: 8

For more information see [Configuring Integration with Sophos SafeGuard 8](#).

8 Save the changes in the configuration file.

---

**NOTE:** There may be more than one field which contains labels such as username and password. In such case, try to use different fields and test the log in process.

---

9 Log off and log in again.

After providing the credentials, if you are able to sign in to the credential provider automatically then remove the parameter credprov\_chaining\_dump\_fields: True from the configuration file.

---

**NOTE:** While searching the labels ensure to examine the label type. You can use a label with one of the following value that indicates the label type:

- ◆ 0 - invalid
  - ◆ 1 - large text (label)
  - ◆ 2 - small text (label)
  - ◆ 3 - command link
  - ◆ 4 - edit box
  - ◆ 5 - password box
  - ◆ 6 - tile image
  - ◆ 7 - check box
  - ◆ 8 - combo box
  - ◆ 9 - submit button
-

# 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.

---

## 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.

---

## 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](#)

## 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.

## 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.

## 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 Troubleshooting for Windows

- ♦ “Debugging Logs for Advanced Authentication” on page 25
- ♦ “Logging for Windows Specific Advanced Authentication Events” on page 26
- ♦ “Chain Icons Cannot be Updated” on page 27
- ♦ “Long Boot” on page 27
- ♦ “Endpoint Not Found” on page 27
- ♦ “Password Synchronization Does Not Work On Standalone Workstations” on page 27
- ♦ “Cannot Restrict Users to Use Specific Workstations” on page 28
- ♦ “Unable to Login Due to JSON Parsing Error” on page 28

## Debugging Logs for Advanced Authentication

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 identify Advanced Authentication server, perform the following steps:

---

**NOTE:** As a prerequisite, ensure that `DiagTool.exe` file is available with the following files in the same directory:

- ♦ `DiagTool.exe.config`
  - ♦ `Ionic.Zip.dll`
  - ♦ `JHSoftware.DNSClient.dll`
- 

1. Run `DiagTool.exe` (the tool must have Microsoft .NET Framework 3.5 installed).
  2. Click **Servers**.
  3. In the **Search settings**, specify the domain name in **Domain** to find a list of Advanced Authentication servers in the specified domain.  
  
If you want to find particular server then clear **Use system DNS server** and specify the IP address of the DNS server in **DNS server**.
  4. Select **Use v6 DNS lookup** to allow the Diagnostic Tool to find the Advanced Authentication server using `_aav6` records.  
  
If you want to find the Advanced Authentication server using `_aaa` records then clear **Use v6 DNS lookup**.
  5. Click **Search**.
- 

**NOTE:** If you configure IP address of the Advanced Authentication server in the DNS service record, the Diagnostic tool cannot find and retrieve the respective record. Ensure that you configure the DNS service record with Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.

---

## Logging for Windows Specific Advanced Authentication Events

To view the logs for Windows specific Advanced Authentication events, perform the following steps:

- 1 Click **Start > Event Viewer**.
- 2 Click **Windows Logs > Application**.
- 3 Check the logs that are specific for Advanced Authentication.

The following table consists of the list of events:

MessageId	Severity	Connection to the server
1	Success	%1 was established
2	Warning	Failed to establish connection with server %1
3	Error	Server not found
4	Success	User %1 was logged on successfully on server %2. Used chain: %3
5	Success	User %1 was logged on successfully via cache. Used chain: %2

# 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.

# 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.

# 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.

# 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.

## 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.

## Unable to Login Due to JSON Parsing Error

**Issue:** It is not possible to login on a workstation. The debug log files of Windows Client contain the JSON syntax/ parsing errors.

**Reason:**

1. The third-party software (for example, Citrix XenDesktop License Manager) uses the same 8082 port.
2. An Advanced Authentication server's DNS name is specified in the `discovery.host` parameter instead of the IP address. Windows Client does not resolve the Advanced Authentication server's IP address.

**Workaround:** Perform the following to resolve the issue:

1. Change the default port by using the `offline.port` parameter, which is the cache service of Windows Client, in the `C:\ProgramData\NetIQ\Windows Client\config.properties` file to a free port.
2. Set `discovery.resolveAddr=false` to disable the resolving of the IP address, which is disabled by default on Windows.