Contents

Advanced Authentication 6.3

Windows Client Installation Guide

February 2019

Legal Notices

About This Book

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

Intended Audience

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

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.

1 System Requirements

For system requirements of Advanced Authentication Windows Client, see Client Components Requirements.

If you are using Client Login Extension Support for Windows Client, see System Requirements (https://www.netiq.com/documentation/client-login-extension-3-10/idm_cle/data/bg4suo5.html) for system requirements of CLE.

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

---

2 Offline Support for Windows Client

You can log in to the Advanced Authentication Windows Client in the offline mode (when the Advanced Authentication server is not available) with non-local accounts using the authentication chains. These chains can contain any combination of the following methods:

- **Bluetooth**
- **Emergency Password**
- **LDAP Password**
- **Password**
- **PKI**
- **HOTP** and **TOTP**
- **Smartphone** (offline mode)
- **Card**
- **FIDO U2F**
- **Fingerprint**
- **Windows Hello**

As a prerequisite for using the offline mode, you must log in to the Advanced Authentication Windows Client in the online mode, using all the chains available to cache each method.

TIP: To log in with a Microsoft account, you must specify the `<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.

---

3 Configuring the Preliminary Settings

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

Configuring the Mandatory Settings

Perform one of the following to set up an interaction between the Windows Client and the Advanced Authentication server:

- To configure Advanced Authentication server lookup in a non-domain mode, manually specify a custom Advanced Authentication server. For more information see, "Using a Specific Advanced Authentication Server in a Non-Domain Mode".

  Or

- To configure the DNS for Advanced Authentication server lookup, you must make Windows Client interact with the Advanced Authentication servers through the DNS. For more information see, "Setting a DNS for Advanced Authentication Server Discovery".

Prerequisite for Advanced Authentication Server discovery

Ensure that the DNS is configured appropriately for Advanced Authentication server discovery (see Setting a DNS for Advanced Authentication Server Discovery) or a specific Advanced Authentication server must be specified in the configuration file.

Using a Specific Advanced Authentication Server in a Non-Domain Mode

You can achieve the following requirements with this setting:

- To enforce a connection to a specific workstation where the DNS is not available.
- To override a DNS based entry for a specific workstation and use the settings specified in the `config.properties` file.

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`.

For fault tolerance support, you can add an additional entry of `\"discovery.hosts:\` to 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>`.

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

Setting a DNS for Advanced Authentication Server Discovery

You can configure a DNS to allow the Windows Client to connect with the Advanced Authentication server through the DNS.

To configure the DNS for server discovery, perform the following tasks:

- “Adding a Host to DNS” on page 14
- “Adding an SRV Record” on page 14
- “Configuring Authentication Server Discovery in Client” on page 17

Adding a Host to DNS

NOTE: When the Advanced Authentication servers are located in cloud, you do not need to add a host to DNS.

---

1. Open the DNS Manager. To open the DNS Manager, click **Start** > **Administrative Tools** > **DNS**.
2. Add the A or AAAA host record and a PTR record:
   - **2a** Right-click your domain name, then click **New Host (A or AAAA)** under **Forward Lookup Zone** in the console tree.
   - **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 have provided in **Name** and **IP address**.

Adding an SRV Record

For best load balancing, it is recommended 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.

- Adding an SRV Record from a Primary Advanced Authentication Site
- Adding an SRV Record from Other Advanced Authentication Sites

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

Adding an SRV Record from a Primary Advanced Authentication Site

To add an SRV record for the Advanced Authentication servers from a primary Advanced Authentication site (a site with the Global Master server), perform the following steps:

1. Right-click on a node with the domain name and click **Other New Records** in the **Forward Lookup Zones** of the console tree.
2. Select **Service Location (SRV)** from **Select a resource record type**.
3. Click **Create Record.**
4. Specify **_aav6** in **Service** of the **New Resource Record** window.
5. Specify **_tcp** in **Protocol**.
6. Specify **443** in **Port Number**.
7. Specify the Fully Qualified Domain Name (FQDN) of the server that is added in **Host offering this service**. For example, `authsrv.mycompany.com`.
8. Click **OK**.

Adding an SRV Record from Other Advanced Authentication Sites

1. Expand the preferred domain name node and select **_sites** in the **Forward Lookup Zones** of the console tree.
2. Right-click on the preferred site name and click **Other New Records**.
3. Select **Service Location (SRV)** from **Select a resource record type**.
4. Click **Create Record**.
5. Specify **_aav6** in **Service** of **New Resource Record** window.
6. Specify **_tcp** in **Protocol**.
7. Specify **443** in **Port Number**.
8. Specify the FQDN of the server that is added in **Host offering this service.** For example, `authsrv.mycompany.com`.
9. Click **OK**.

You must add a host and SRV records in DNS for all the authentication servers. The Priority and Weight values for different servers may vary. For best load balancing, you must have records only for the Advanced Authentication web servers instead of records for Global Master, DB Master, and DB servers.

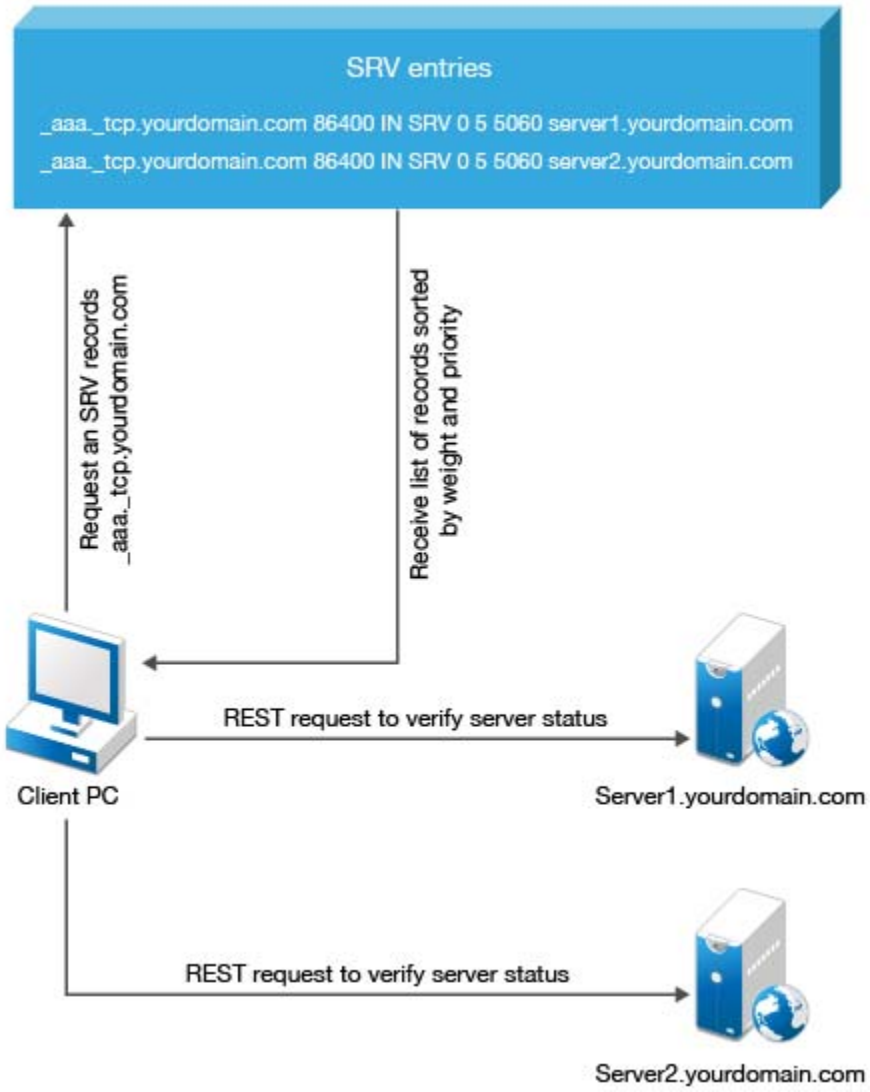
DNS Server Entries

The DNS server contains the following elements in an SRV record: SRV `entries _service._proto.name TTL class SRV priority weight port target`. The following table defines these elements present in an SRV record:

Element	Description
Domain	Domain name for which this record is valid. It ends with a dot.
Service	Symbolic name of an applicable service.
Protocol	Transport protocol of an applicable service. Typically, TCP or UDP.
Priority	Priority of the target host. Lower the value, higher the priority.
Weight	A relative weight for records with the same priority. Higher the value, higher the priority.
Port number	TCP or UDP port on which the service is located.
Target (Host offering this service)	Canonical hostname of the machine providing the service. It ends with a dot.

Authentication Server Discovery Flow

The following diagram illustrates the server discovery workflow.



Configuring Authentication Server Discovery in Client

You can configure server discovery in the Windows Client by using the following parameters in the `config.properties` file:

Parameter	Description
`discovery.Domain`	DNS name of the domain. For Windows Client, this value is used if the workstation is not connected to the domain.
`discovery.port`	Option to specify the port number for the client-server interaction.
`discovery.host`	Option to specify the DNS name or the IP address of an Advanced Authentication server.

Parameter	Description
`discovery.subDomains`	Lists additional sub domains separated by a semicolon.
`discovery.useOwnSite`	Set the value to `True` to use the local site (Windows Client only).
`discovery.dnsTimeout`	Set 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 Client.
`discovery.wakeupTimeout`	Timeout after the operating system starts or resumes from sleep. The default value is 10 seconds.
`discovery.hosts`	Option to specify the DNS server(s) name or the IP address of a multiple Advanced Authentication server(s).
`discovery.skipAlreadyTriedPeriod`	A delay for which the Windows Client stops searching the server after an unsuccessful search attempt. The default value is 5 minutes after which the Client switches to the online mode. During background operations (for example, policy updates) if the cache determines that the server is available, then the set period can be reduced.

Configuring Optional Settings

The following table describes the optional settings that you can do for Windows Client.

Setting	Description
disable_1N: true	To disable the automatic detection of username for Card and PKI methods. For more information, see "Disabling 1:N"
disable_local_accounts: true	In a non-domain mode, it is recommended to disable the local accounts. For more information, see "Disabling the Local Accounts".
tenant_name	If you use Multitenancy, you must point Windows Client to a specific tenant. For more information, see "Configuration Settings for Multitenancy".
event_name: <CustomEventName>	If you want to use DNS and non-domain based machines, you can use a custom event for the specific machines. For more information, see "Selecting an Event".
card.timeout: X	To change a default Card waiting timeout. For more information, see "Configuring Timeout for Card Waiting".
card.fail_on_timeout: true	To configure the login failure after the Card waiting timeout. For more information, see "Enabling Login Failure After Card Timeout".

Setting	Description
u2f.timeout: X	To configure the timeout for authentication with the U2F token. For more information, see "Configuring Timeout for the U2F Authentication".
logo_path: C:\\dir\\filename.png	To customize a logo for Windows Client. For more information, see "Customizing a Logo".
verifyServerCertificate: true	To configure the verification of server certificates for LDAP connection. For more information, see "Configuring to Verify Server Certificates".
forceCachedLogon: true	To configure the cached login for client unlock. For more information, see "Configuring the Enforced Cached Login".
sso_aaf_required: true	To configure single sign-on for Citrix and Remote Desktop. For more information, see "Configuring Single Sign-on Support for Citrix and Remote Desktop".
select_terminal_client_user: true	To configure settings for a saved Remote Desktop session (.rdp file). For more information, see "Configuring Settings for a Saved Remote Desktop Connection".
endpoint_name	To edit the name of an endpoint. For more information, see "Changing an Endpoint Name".
authentication_agent_enabled = true	To enable Authentication Agent chain in the Windows Client. For more information, see "Configuring to Enable the Authentication Agent Chain".
• **credprov_chaining_clsid** • **credprov_chaining_enabled** • **credprov_chaining_password_field** • **credprov_chaining_username_field**	To integrate Advanced Authentication with the Sophos SafeGuard. For more information, see "Configuring Integration with Sophos SafeGuard 8".
• **credprov_chaining_clsid** • **credprov_chaining_enabled** • **credprov_chaining_dump_fields** • **credprov_chaining_password_field** • **credprov_chaining_username_field**	To configure the credential provider chaining. For more information, see "Configuring the Credential Provider Chaining".
tlsVersion: value	To configure the TLS Version for HTTPS connection. For more information, see "Configuring the TLS Version".
allowUnknownUserOfflineCredUI: true	To allow local users to log in to the remote desktop through offline mode. For more information, see "Enabling Non-Enrolled Users to Log In to Remote Desktop and User Account Control through Offline Mode".
enableLinkedChainsOffline: false	To disable linked chains for offline login. For more information, see "Disabling Linked Chains for Offline Login".
enable_last_chain_selection: false	To auto-select the last authenticated chain for login. For more information, see "Enabling Last Logged In Authentication Chain for Login".

Setting	Description
sso_flex_enabled: true	To enable flexible sign-on to skip LDAP password in authentication chain during Citrix or RDP login. For more information, see Enabling Flexible Sign-on for Citrix VDI or Remote Desktop Login
offline.port:<port number>	To configure the port that manages the Windows Client Cache Service. For more information, see "Configuring the Port for Windows Client Cache Service".
provider.AuthenticationProtocol: value	To configure the authentication protocol that the Local Security Authority applies during Windows OS logon. For more information, see "Configuring the Authentication Protocol".
show_copyright: false	To disable the copyright information on the login screen. For more information, see "Hiding the Copyright Information".
rest_profiling: true	To enable the profiling tool that helps in analyzing the performance and CPU utilization of different programs. For more information, see "Enabling the Profiling Tool".
allowedProviders: {classID of provider}	To configure the primary or third-party credential providers in Windows workstation that verify users' identity during the logon process and grant access. For more information, see "Enabling the Third-Party Credential Provider".

You can configure the following settings in the registry:

- To configure an automatic login, see "Configuring Automatic Login".

You can change the system locale for Windows Client with the setting, "Changing the Locale for Windows Client".

You can localize the Advanced Authentication resources for your language with the instructions, Localizing the Messages for Clients

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 `config.properties` file.
3. Save the `config.properties` file and restart the Windows operating system.

Disabling the Local Accounts

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

To disable the 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 parameter **disable_local_accounts: true** to the `config.properties` 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 the Multi-tenancy option is enabled, you must add the parameter `tenant_name` with a 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 for authentication. However, in some scenarios you must create a separate custom event. For example, when the predefined event is used for DNS based workstations, you can create a custom event with the type as **Generic** for the non-domain based workstations. You must point these non-domain based workstations to the custom event using the `event_name: <CustomEventName>` parameter in the 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 specified timeout period, the `Hardware timeout` message is displayed and the card waiting dialog is closed. The 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. Specify `card.timeout: X` in the `config.properties` file. X is the timeout value in seconds.

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

Configuring Timeout for the U2F Authentication

You can configure the timeout for which the authentication fails when the U2F token is not touched for authentication. The default value for the timeout is 60 seconds after which the authentication fails.

To configure the timeout for U2F authentication, 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 `u2f.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 Login Failure After Card Timeout

By default, the card timeout is not considered as a login failure. However, you can configure the card timeout as a login failure.

To enable login 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. Specify `card.fail_on_timeout: true` in the `config.properties` file.
3. Save the configuration file.
4. Restart the Windows operating system.

Configuring Automatic Login

To enable the Windows operating system to perform an automatic login, 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:
   - `DefaultDomain`
   - `DefaultPassword`
   - `DefaultUserName`

For more information about how to enable automatic login on Windows, see the Microsoft Support 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. Specify `logo_path: C:\\dir\\filename.png` in the `config.properties` file.

   You cannot use the logo from shared folders.
3. Save the configuration file.
4. Restart the Windows operating system.

Configuring to Verify 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. This helps to prevent attacks on the connection and ensure safe authentication.

The option for verification of server certificates is disabled by default. You must import 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`) in the `config.properties` file.
3. Restart the Windows operating system.

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 the Enforced Cached Login

When the network connection is slow or unstable, the client login or unlock process can take several minutes. A solution to this is to enforce the cached login. The Client connects to Advanced Authentication server to validate the credentials in the background after the cached login. By default, the enforced cached login is not used and the Client will always try to connect to Advanced Authentication server to validate the credentials.

Perform the following steps to allow users to use the enforced cached login:

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

Following are different behavior of the Cache Service:

- If a user account is marked as disabled, expired, or locked in the local cache, the Cache Service tries to switch online and based on the server status one of the following occurs:
  - When the Advanced Authentication server is available, the user is allowed to log in once. During the subsequent login, after selecting a chain and before providing credentials, an error message that states the account being disabled is displayed.
  - When the Advanced Authentication server is unavailable, the user can log in once. During the subsequent login, an error message is displayed after submitting the credentials.
- If a user account is not marked as disabled, expired, or locked in the local cache, the Cache Service processes the login request and updates the user data in background.

Configuring Single Sign-on Support for Citrix and Remote Desktop

You can configure the Windows Client to use the Single Sign-on (SSO) feature for establishing a connection to a Citrix and a Remote Desktop server. Therefore, 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 prevents users from specifying the credentials again when they login to terminal servers (remote machine to which the user is connecting from the Terminal Client) 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 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) is ignored. You need to disable SSO to make this policy to work.

Default value of SSO parameters is specific to the version of Advanced Authentication Windows Client, therefore refer one of the following sections as per your requirement:

- For Advanced Authentication 6.3 to 6.3 Service Pack 4
- For Advanced Authentication 6.3 Service Pack 4 Patch 1 and Later Versions

For Advanced Authentication 6.3 to 6.3 Service Pack 4

The SSO feature is enabled by default for accessing the terminal servers. By default, SSO feature works irrespective of the Advanced Authentication Windows Client installation on the terminal client (user workstation on which the terminal connection is initiated).

To enable SSO only when the Advanced Authentication Windows Client is installed on the terminal client, perform the following steps on the terminal server:

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 Windows operating system.

To disable the SSO feature, perform the following steps on the terminal server:

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

   If the file does not exist, create a new file.
2. Specify `sso_logon_enabled: false` (default value is `true`).
3. Save the configuration file.
4. Restart the Windows operating system.

For Advanced Authentication 6.3 Service Pack 4 Patch 1 and Later Versions

The SSO feature is disabled by default for accessing the terminal servers. To enable the SSO feature, perform the following steps on the terminal server:

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

   If the file does not exist, create a new file.
2. Specify `sso_logon_enabled: true` (default value is `false`).
3. Save the changes.
4. Restart the Windows operating system.

If you have enabled the SSO, by default it will work only when you have the Advanced Authentication Windows Client installed on the terminal client. To disable SSO irrespective of the Advanced Authentication Windows Client installation of the terminal client, perform the following steps on the terminal server:

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: false` (default value is `true`).
3. Save the changes.
4. Restart the Windows operating system.

Configuring Settings for a Saved Remote Desktop Connection

This setting allows you to accomplish the following for a saved Remote Desktop Connection for a remote login.

- If `select_terminal_client_user: true`, users cannot change their credentials while logging in.
- If `select_terminal_client_user: false`, users can change their credentials while logging in.

NOTE: Advanced Authentication must be installed both on the terminal client and the terminal server.

To configure this setting, 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 `select_terminal_client_user: true` in the `config.properties` file. The default value is `true`.

   Users will be not be able to edit the login credentials of the saved Remote Desktop connection on the Advanced Authentication Credential Provider.
3. Save the configuration file.
4. Restart the Windows operating system.

If you set `select_terminal_client_user: false`, users will be able to edit the login credentials of the saved Remote Desktop connection on the Advanced Authentication Credential Provider.

Changing an Endpoint Name

You can edit the name of an endpoint based on your requirement.

To change an endpoint name, 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 `endpoint_name: <endpoint name>` in the `config.properties` file. For example, endpoint name can be computer 1.
3. Save the configuration file.
4. Restart the Windows operating system.

Configuring to Enable the Authentication Agent Chain

NOTE: The `authentication_agent_enabled` parameter is valid for Advanced Authentication 6.3 SP4 and prior versions. This parameter is not required from Advanced Authentication 6.3 SP5.

The Authentication Agent allows you to authenticate on one computer where all the devices required for authentication are connected. This helps 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 devices that are used for authentication.

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

You must select **Authentication Agent** in 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 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 preferred chain to log in to Windows B 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.

Changing the Locale for Windows Client

This option allows you to change the locale of Windows Client. By default, Windows Client uses the locale of the Windows operating system.

To change the locale of Windows Client on Windows 10, perform the following steps:

1 Specify **Settings** in the Search space.

2 Open the **Settings** window.

3 Click the **Language** tab.

4 Click **Administrative language settings** in **Related settings**.

5 Click **Change system locale** in the **Administrative** tab.

6 Select the language from the **Current system locale** list.

7 Click **OK**.

8 A restart is recommended to apply the changes. Click **Restart now**.

Configuring the Credential Provider Chaining

This option allows you to integrate Advanced Authentication with any other credential provider in Windows Client. Therefore, when 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 out 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 the 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. Therefore, 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 that contain labels such as username and password. Here, you must use different fields and test the log in process.

---

9 Log out and log in again.

After providing the credentials, if you are able to sign in to the credential provider automatically, 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

Examples of Integration for the Credential Provider Chaining

This section contains the following examples for the CP chaining:

Configuring Integration with Sophos SafeGuard 8

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

With this integration, 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 out and log in again.

Configuring Integration with TrendMicro FileEncryption

This section provides the configuration information on integrating Advanced Authentication with TrendMicro FileEncryption.

To integrate Advanced Authentication with the TrendMicro FileEncryption, 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: {5077AF65-B1B6-417b-A1E0-A05B2837A752}`
   - `credprov_chaining_dump_fields: True`
   - `credprov_chaining_enabled: True`
   - `credprov_chaining_password_field: 2`
   - `credprov_chaining_username_field: 1`
3. Save the configuration.
4. Log out and log in again.

Configuring the TLS Version

You can configure the TLS version that the network library of the Windows Client uses for establishing HTTPS connection with the Advanced Authentication server. The default version is TLSv1.2.

To configure the TLS version, 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 `tlsVersion: value`. The values are defined as follows:
   - TLSv1.2 (default)
   - TLSv1.1
   - TLSv1
   - all: Network library will choose the TLS version automatically.

   NOTE: If you set invalid or unknown value for the `tlsVersion` parameter, then the default value TLSv1.2 is set automatically.
3. Save the changes.
4. Restart the Windows operating system.

Enabling Non-Enrolled Users to Log In to Remote Desktop and User Account Control through Offline Mode

You can enable the non-enrolled repository users to perform offline login to the remote desktop and User Account Control (UAC) with the `allowUnknownUserOfflineCredUI` parameter.

By default, the Windows Client does not allow non-enrolled users to do offline login to remote desktop and UAC.

Before you enable this parameter, ensure that the **Username disclosure** option is set to **ON** in the **Login Options** policy of the Administration portal.

To allow non-enrolled users to do offline login to the remote desktop and UAC, 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 `allowUnknownUserOfflineCredUI:true` (default value is false) in the `config.properties` file.
3. Save the configuration file.

Disabling Linked Chains for Offline Login

With a linked chain, users can authenticate to the Windows client within the grace period after successful authentication with the required chain.

For example, LDAP Password+Card is a required chain, and Card is a linked chain. The users must use the LDAP Password+Card chain once in every 8 hours and within this period, they can only provide card without the LDAP Password to authenticate.

By default the linked chains are available in both online and offline mode.

NOTE: An administrator must ensure that the **Enable linked chains** option is set to **ON** in the **Linked chains** policy of the Administration portal to allow users to log in with the linked chain.

To disable linked chains for offline login, 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 `enableLinkedChainsOffline:false` (default value is true) in the `config.properties` file.
3. Save the configuration file.

Enabling Last Logged In Authentication Chain for Login

You can allow users to authenticate with the previous logged in authentication chain to the Windows Client without prompting the chain selection dropdown. However, user can still click back arrow to view the list of authentication chains.

To enable selection of last logged in authentication chain for login, 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 `enable_last_chain_selection:true` (default value is false) in the `config.properties file`.
3. Save the configuration file.

Enabling Flexible Sign-on for Citrix VDI or Remote Desktop Login

You can configure the Windows Client to enable the Flexible sign-on feature for remote login. Therefore, when a user needs to connect to a remote machine launched via Citrix StoreFront, the user needs to perform the following actions:

1. Specify the URL of Citrix StoreFront in a browser.
2. Enter the Username and LDAP Password to login to Citrix StoreFront.
3. Select the published Windows desktop.

4 Enter the username.

5 Authenticate with the preferred authentication method(s) of the chain.

If Flexible SSO is enabled and the user selects the chain that has LDAP password method in it, then the user can skip the LDAP password prompt in **Step 5** while accessing the published Windows desktop.

Ensure the following prerequisites are met before enabling flexible sign-on for remote login:

- Create a chain with LDAP password in it and assign the chain to **Windows Logon** event.
- Install Advanced Authentication Windows Client on remote machine.

Default value of Flexible sign-on parameter varies based on the version of Advanced Authentication Windows Client, therefore refer one of the following sections as per your requirement:

- For Advanced Authentication Windows Client 6.3 Service Pack 4 and Prior Versions
- For Advanced Authentication Windows Client 6.3 Service Pack 4 Patch 1 and Later Versions

For Advanced Authentication Windows Client 6.3 Service Pack 4 and Prior Versions

Perform the following steps on the remote machine to enable flexible sign-on for LDAP password in the authentication chain:

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

If the file does not exist, create a new file.

2 Specify `sso_flex_enabled: true` (default value is `false`).

3 Save the configuration file.

4 Restart the Windows operating system.

For Advanced Authentication Windows Client 6.3 Service Pack 4 Patch 1 and Later Versions

By default, the flexible sign-on is enabled for LDAP password on the remote machine. To disable the flexible sign-on for LDAP password, perform the following steps:

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

If the file does not exist, create a new file.

2 Specify `sso_flex_enabled: false` (default value is `true`).

3 Save the changes.

4 Restart the Windows operating system.

Localizing the Messages for Clients

You can localize error messages, method message, and prompt message displayed on endpoints to an unsupported language.

To localize the client messages to an unsupported language, perform the following steps:

1. Navigate to `C:\Program Files\NetIQ\Windows Client\locale\`.
2. Create a new folder for preferred language and name the folder as per ISO nomenclature standards.

   To know more about ISO nomenclature standard, see `http://www.loc.gov/standards/iso639-2/php/langcodes-search.php`.

   For example, if you need to create a new folder for Latin, name the folder `la`.

   NOTE: While naming the folder, keep the following points in mind:

   - The name of the language folder should be in lower case.
   - If the ISO standard name of a language contains any special character such as hyphen or period, replace the special character with an underscore.

     For example, if the ISO code of a language is `fr.ca`, name the language folder `fr_ca.`

   ---
3. Inside the preferred language folder, create a new folder and name it `LC_MESSAGES`
4. Copy `aaacachesrv.pot, aucore.pot,` and `CredentialProvider.pot` files, and paste it in `C:\Program Files\NetIQ\Windows Client\locale\<language>\LC_MESSAGES`.
5. Open the `aaacachesrv.pot, aucore.pot,` and `CredentialProvider.pot` files in a text editor. For example, PoEditor.
6. Specify the preferred language message in the `msgstr ""`.

   For example, if you need to localize `password will expire in $(days) days` message to Latin, specify `in password erit exspirare $ (dies) dierum` in `msgstr ""` as in the following image.

```
1  msgctxt "errors.user_not_found"
2  msgid "User not found"
3  msgstr ""
4
5  msgctxt "method.swisscom.user_should_accept_request"
6  msgid "The user should accept your request with his/her mobile phone"
7  msgstr ""
8
9  msgctxt "method.messaging.cannot_determine_recipient_address"
10 msgid "Cannot determine OTP recipient address"
11 msgstr ""
12
13 msgctxt "method.virtual_password.password_will_expire"
14 msgid "Password will expire after ${days} days"
15 msgstr "Password will expire in ${days} days"
16
17 msgctxt "method.emergency_password.password_is_not_effective"
18 msgid "Emergency password is not effective yet. Wait ${wait_days} day(s)"
19 msgstr ""
20
```

7. Save the changes.

8 Convert the `aaacachesrv.pot, aucore.pot,` and `CredentialProvider.pot` files to `.mo` format using Po editing tools. For example, PoEditor.

9 Change the Administrative language of the operating system to the preferred language. For more information, see Changing the Locale for Windows Client

10 Restart the operating system.

Configuring the Port for Windows Client Cache Service

The Windows Client Cache Service listens on the port 8082 by default. If port 8082 is in use with another application, then the Cache Service listens on the port 8083 or 8084. When all the three ports are in use, the installation fails.

Before installing the Windows Client, you can configure a specific port that manages the Windows Client Cache Service and prevent installation failure.

You can define the offline port in one of the following ways:

- Modifying the Configuration File
- Using MSI Command

Modifying the Configuration File

1 Navigate to the `C:\ProgramData\NetIQ\` path and create a folder `Windows client`.

2 Create a file `config.properties` within `Windows client`.

3 Specify `offline.port:<port number>` in the configuration file.

For example, `offline.port:8083`

4 Save the changes.

Using MSI Command

The MSI command to initiate the installation of Windows Client and define the offline port is as follows:

```
msiexec /i netiq_naaf-winclient-x64-release-<version>.msi
OFFLINE_PORT=<port number>
```

For example, `msiexec /i netiq_naaf-winclient-x64-release-6.3.3.msi OFFLINE_PORT=8092`

To define multiple offline ports, use comma as a separator. You can configure maximum of three ports.

```
msiexec /i netiq_naaf-winclient-x64-release-<version>.msi
OFFLINE_PORT=<port number1>, <port number2>,..
```

```
msiexec /i netiq_naaf-winclient-x64-release-6.3.3.msi
OFFLINE_PORT=8090,8091,8092
```

Configuring the Authentication Protocol

Sometimes, the Logon Filter functionalities might not work as expected. In such case, you can enforce an alternate authentication protocol that the Local Security Authority applies during Windows OS logon process. The default authentication package is Negotiate.

To enforce the preferred authentication protocol in Windows operating system, 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 `provider.AuthenticationProtocol: value`. The values are defined as follows:
   - `0` (default value): Represents Negotiate. Windows operating system selects Kerberos or NTLM, depending on the capability.
   - `1`: Represents Kerberos authentication protocol.
   - `2`: Represents NTLM authentication protocol.

   NOTE: When the `provider.AutheticationProtocol` parameter is set to 0 (Negotiate) or 2 (NTLM) and the Windows workstation is disconnected from network, users can still log in. However, when the parameter is set to 1 (Kerberos), user cannot log in if the workstation is disconnected from network.
3. Save the configuration file.

Hiding the Copyright Information

This parameter allows you to hide the copyright information from the login screen of Windows Client. Perform the following steps to conceal the copyright information:

1. Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`.

   If the file does not exist, create a new file.
2. Specify `show_copyright: false`.

   The default value of `show_copyright` parameter is `True`.
3. Save the configuration file.

Enabling the Third-Party Credential Provider

With Advanced Authentication Windows Client installed on the Windows workstation, during login, the Client acts as the Credential Provider to confirm the identity of a user and authenticate. By default, Windows Client blocks other Credential Providers to enhance the security. You can enable primary or custom Credential Providers in Windows workstations and allow users to select the

preferred providers that verify users' identity during the logon process and grant access. This feature can also be used when the Credential Provider chaining does not help to integrate with a third-party Credential Provider (like baramundi).

To allow other credential providers in Windows workstation, 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 `allowedProviders: {classID of provider}`

   You can configure more than one credential providers use comma or semicolon as a separator.

   For example, `allowedProviders: {25CBB996-92ED-457e-B28C-4774084BD562}, {48B4E58D-2791-456C-9091-D524C6C706F2}`

3. Save the configuration.

Configuring in Case of Advanced Authentication as a Service

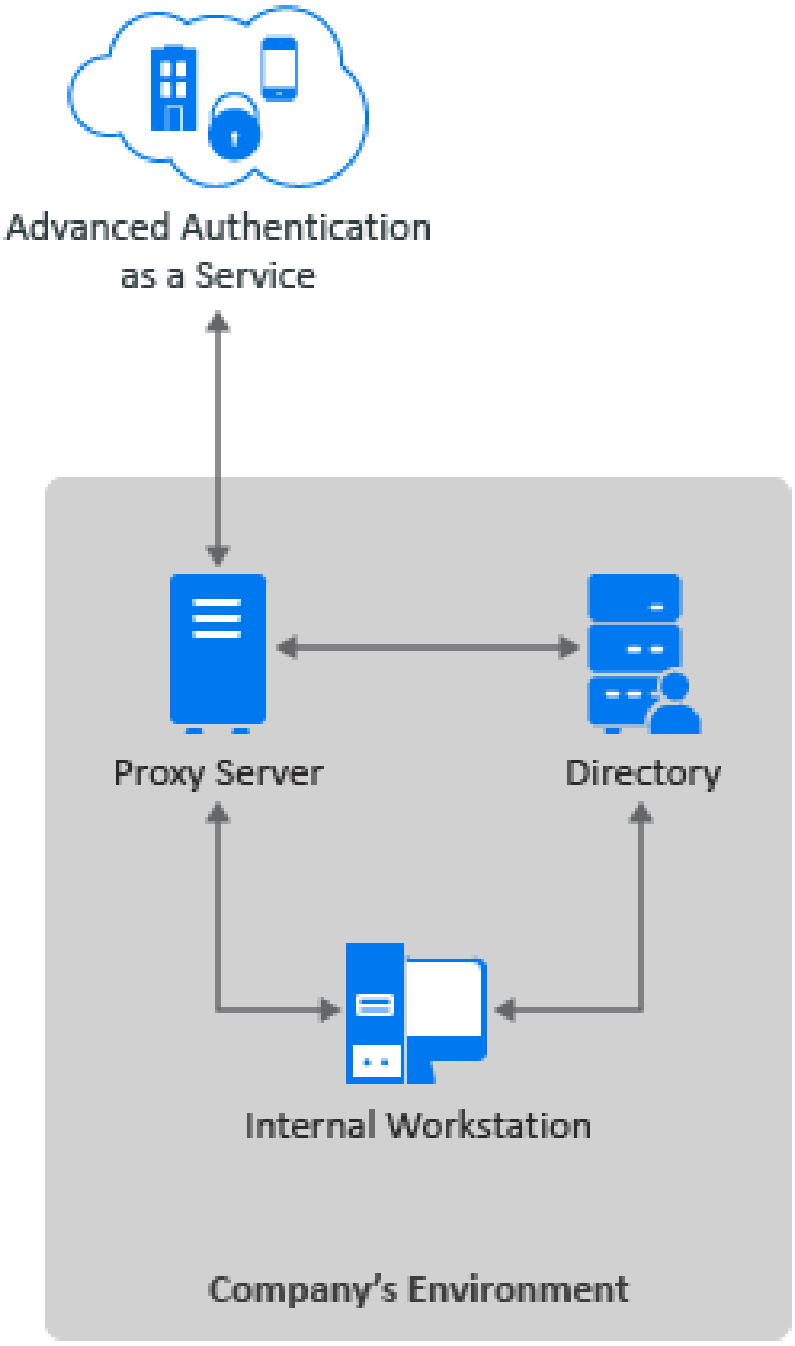
The following table describes the parameters to configure Windows Client in case of Advanced Authentication as a Service.

Parameter	Description
`discovery.host`	DNS name of the Advanced Authentication as a Service server.
`discovery.connectTimeout`	Parameter to specify the Advanced Authentication servers discovery timeout in seconds. The default value is 2 seconds. Recommended value is 10 seconds.
`discovery.dnsTimeout`	Parameter to specify the time out for the DNS queries in seconds. The default value is 3 seconds. Recommended value is 10 seconds.
`tenant_name`	parameter to specify your tenant name. For example, tenant_name: YOURTENANTNAME

To enable Windows client to work with Advanced Authentication via HTTP Proxy, see Configuring to Connect Via HTTP Proxy

Configuring to Connect Via HTTP Proxy

You can configure the Windows Client to work with Advanced Authentication Servers via HTTP Proxy. Perform the following steps to configure the Windows Client.



1 Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`.

2 Specify the following parameters:

- Specify IP address or host name of the Proxy server in `proxy.host`.
- Specify a port number for the client-server interaction in `proxy.port`.
- Specify the timeout in seconds for the Proxy server response in `proxy.timeout`.

  The default timeout value is 10 seconds.

- (Optional) Specify the username to login to the Proxy server in `proxy.username`.
- (Optional) Specify the password to login to the Proxy server in `proxy.password`.

NOTE: You can skip specifying Proxy username and password. If the Proxy username or password are not specified or wrong, the user will be asked for the proxy credentials during next login.

For local users, the proxy credentials are ignored and you are allowed to login.

---

3 Save the `config.properties` file and restart the Windows operating system.

4 Installing and Uninstalling Windows Client

This chapter contains information about how to install and uninstall Windows Client:

NOTE:

- When you upgrade from Windows Client 5.2, the endpoints are not removed automatically. The administrator must remove the endpoints manually.
- 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. Navigate to **System properties** (**Control Panel > All Control Panel Items > System**) to identify your **System type**.
2. Run `naaf-winclient-x86-release-<version>.msi` for a 32-bit operating system or `naaf-winclient-x64-release-<version>.msi` for a 64-bit operating system.

   To install Windows Client Support Assisted Logon mode, run the following command:

   `msiexec -i naaf-winclient-x86|x64-release-<version>.msi ASSISTANCE_LOGON=1`.
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 or when Advanced Authentication as a Service is used, 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 in a Non-Domain Mode" to specify an Advanced Authentication server.

NOTE: If the Windows Client installation hangs or fails, this might be due to the unavailability of a port for the Windows Client Cache Service. To resolve this issue, you can configure a specific port that manages the Windows Client Cache Service. For more information, see Configuring the Port for Windows Client Cache Service.

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 the administrator must 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 the deletion.

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 double-click **Programs and Features**.
2. Select **NetIQ Windows Client** and click **Uninstall**.

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**.

Microsoft Windows 10

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

5 Support Assisted Logon

The Support Assisted Logon feature is for the users who do not use multi-factor authentication and forget the password. Using Support Assisted Logon, a helpdesk administrator can log in as the user with the Helpdesk Administrator's credentials.

For example, Bob is a top official in his organization. He forgot his password, and he is not able to access his Windows workstation. In this situation, Bob is the managed user who needs to open the workstation. If authenticators of Helpdesk Administrator are shared with the Managed user's (Bob) account, perform the following steps to access Bob's Windows workstation:

1. Bob is required to click the Support Assisted logon link on the login screen and specify his username in the **Managed User Name** in Support Assisted Logon prompt.
2. Tom, the Helpdesk Administrator, needs to specify his username.
3. Tom is required to select the required chain with the shared authenticator and authenticate.

Following are the users involved in Support Assisted Logon:

- **Managed user:** The user who forgets the password and needs to access the workstation.
- **Helpdesk Administrator:** The person whose authenticators are shared with the Managed user. The Helpdesk Administrator can access the Managed user's workstation using the Helpdesk Administrator's authenticators.

- "Prerequisites" on page 43
- "Enabling Support Assisted Logon" on page 44
- "Disabling Support Assisted Logon" on page 44

Prerequisites

Ensure the following prerequisites are met before you enable Support Assisted Logon:

- Create a chain with any of the methods that support the **Sharing Authenticator** feature (TOTP, HOTP, Password, Fingerprint, Card, Flex OTP, FIDO U2F, and RADIUS Client.) and assign the chain to **Windows Logon** event.

  NOTE: The LDAP Password method does not support **Sharing Authenticator** feature.

- Support User (Helpdesk Administrator) must have enrolled for each method in the created chain.
- Share each enrolled method of Support User with Managed User in **Shared Authenticators** of Help desk. For more details about Shared Authenticators, see Sharing Authenticators.
- The user does not use multi-factor authentication. To let Advanced Authentication know the user's password, create a new custom event **LDAP Password AutoUpdate**, and assign an **LDAP Password** only chain to the event.

Enabling Support Assisted Logon

Perform the following actions to enable Support Assisted Logon:

1. Navigate to `C:\Program files\NetIQ\Windows Client` path.
2. Open `AssistanceLogonOn.reg` file.
3. Click **OK**.

NOTE: Enabling the Support Assisted Logon disables the multi-factor authentication.

Disabling Support Assisted Logon

Perform the following actions to disable Support Assisted Logon:

1. Navigate to `C:\Program files\NetIQ\Windows Client` path.
2. Open `AssistanceLogonOff.reg` file.
3. Click **OK**.

6 Support Windows Hello for Business

Advanced Authentication enhances security on the domain-joined Windows 10 workstations by providing an additional request for the Windows Hello authentication with PIN. It is required to have the Windows Hello for Business configured in the domain to allow users to authenticate with Windows Hello PIN. The Windows Hello PIN is asked separately as one more factor after the regular authentication.

NOTE: Windows Hello does not require configuration and cannot be disabled.

7 Client Login Extension Support for Windows Client

You can reset your password through the 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 must be displayed for the **LDAP password** method page in the Windows Client.

Prerequisites

Ensure that the following prerequisites are met before you use CLE 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.

8 Troubleshooting for Windows Client

This chapter contains the following sections on troubleshooting:

Debugging Logs for Advanced Authentication

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, clear **Use v6 DNS lookup**.

5. Click **Search**.

NOTE: If you configure the 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 the Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.

You can collect the logs for Advanced Authentication in the following ways:

- Using a Diagnostic Tool
- Manual

Using a Diagnostic Tool

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 Windows operating 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.
9. Click **Save** to save the logs.
10. Click **Disable** to disable the logging.
11. Click **Clear All**.

Manual

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`.

Enabling the Profiling Tool

You can configure the Windows Client to enable the profiling for Web server logs of the Advanced Authentication server. Profiling tool helps in tracking the performance, memory allocation, and CPU utilization of each REST API calls that are processed including the background programs that are initiated by the call. In case of an issue, it facilitates in identifying the cause.

Enabling the profiling tool appends `&profiling=true` parameter to API calls sent to the server. Before enabling profiling, ensure to set **Debugging Logs** to **ON** in the Administration portal. After enabling the Profiling tool, you can track the detailed logs in **Logs > Web server** in the Administration portal.

To enable the Profiling tool, 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 `rest_profiling:true` (default value is false) in the `config.properties file`.
3. Save the configuration.

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 describes list of events:

Event Id	Severity	Description
1	Success	Connection with XXX server was established
2	Warning	Failed to establish connection with server XXX
3	Error	Server not found
4	Success	User XXX was logged on successfully on server YYY. Used chain: ZZZ
5	Success	User XXX was logged on successfully via cache. Used chain: ZZZ
6	Error	User XXX failed to log in with the YYY chain on the server ZZZ. For example, User **FOCUS\bob** failed to log in with the LDAP Password only chain on the server **aa.focus.com:443**
7	Error	User XXX failed to log in with the YYY chain via cache. For example, User **FOCUS\bob** failed to log in with the LDAP Password only chain via cache.

Chain Icons Cannot be Updated

Issue: A system administrator has applied the new icons for the authentication chains, but the icons are not updated on the Windows Client.

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

Endpoint Not Found

Issue: After installing the Windows Client and rebooting, the client reports `Endpoint not found` error and it is not possible to log in.

Reason: An endpoint for the client exists on the server or in the configuration file of the client.

Workaround:

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

Password Synchronization Does Not Work On Standalone Workstations

Issue: A message `Wrong password` is displayed when the password is not synchronized while logging in to a standalone workstation.

Workaround:

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 the Active Directory, and users try to log in 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 the Active Directory, the account is able to log in successfully.

Reason: This issue happens when using the LDAP Password method, Advanced Authentication tries to bind to the Domain Controller to validate the password and it fails.

Workaround:

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. To prevent that user from accessing the Domain Controllers, go to **Group Policy Management > Domain Controllers > Default Domain Controller policy > Edit**.
4. In 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 Log In Due to JSON Parsing Error

Issue: Users are unable to log in to a workstation because the debug log files of Windows Client contain the JSON syntax or 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:

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 resolving the IP address, which is disabled by default on Windows.

Issue With the Login When an Endpoint Exists on the Server

Issue: While logging in to Windows Client, an error `Cannot add or change the endpoint (same name or software_name already exist?)` is displayed on the workstation.

Reason:

1. Windows Client is installed on the machine. After the first reboot an endpoint is created. You can find the local data in the path: `%ProgramData%\NetIQ\Windows Client\config.properties`. It is possible that the `config.properties` file is deleted or overwritten, but the endpoint is still available on the Advanced Authentication server.

   Workaround: You must remove the endpoint from the Advanced Authentication server (**Administration portal > Endpoints** section).

2. Multiple machines are rolling out from a single gold image. They have the same machine SID. The endpoint is generated based on the SID.

   Workaround: The SID must be unique to ensure the Windows Client works on multiple workstations.

Issue with the Windows Client Credential Provider When the McAfee Disk Encryption is Installed

Issue: When the McAfee Disk Encryption is installed on a Windows workstation that has the Advanced Authentication Windows Client installed, after rebooting, the Windows Client's Credential Provider does not appear. User can authenticate with the Password method only.

Workaround: Modify the DE/EEPC `EpePcCp.ini` file. For more information, see the McAfee support page (https://kc.mcafee.com/corporate/index?page=content&id=KB85612).

Black Login Screen Is Displayed When a Laptop Is Connected to a Docking Station

Issue: A black login screen is displayed when users try to log in to a Windows 7 laptop or workstation that is connected to a docking station. No authentication prompt is displayed.

Workaround: Perform the following steps:

1. Open the configuration file `C:\ProgramData\NetIQ\Windows Client\config.properties`.
2. Add `gfx_layer:1`.
3. Save the `config.properties` file and restart the Windows operating system.

However, when you set `gfx layer:1`, there could be a considerable lag while typing on the login screen where the resolution is high.

Prevent Multi-Factor Authentication bypassing on the Login Screen for VPN connectivity

The user can bypass MFA in case of VPN authentication configured on the login screen. To prevent MFA bypassing for VPN authentication, perform the following steps:

1. Navigate to `%appdata%\Microsoft\Network\Connections\Pbk` directory.
2. Open the `.pbk` file in Notepad.
3. Set the parameter `UseRasCredentials` to `1.` (default value is `0`).
4. Save the changes and close the file

Windows Client Freezes When A User Authenticates to an Application with UAC

Issue: While authenticating to Windows User Account Control (UAC) prompt, the Windows Client freezes in the `Please wait screen` after providing the username.

Reason: This issue happens only in Windows machines with external Nvidia Quadro graphics cards and their drivers installed.

Workaround: 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 `gfx_unfreeze: true`

   The default value of `gfx_unfreeze` is `false`.
3. Save the configuration file.