Advanced Authentication 6.3

Logon Filter Installation Guide

December 2019

Legal Notices

Contents

About this Book

The Logon Filter Installation Guide has been designed for domain administrators and describes the system requirements and the installation procedure for Logon Filter.

Intended Audience

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

About Logon Filter

Logon Filter is a component that you must install on the Domain Controllers. Logon Filter allows you to automatically update group membership if you log in with the Advanced Authentication Windows Client. You can use the Logon Filter to prevent users to log in without the Advanced Authentication Windows Client. You can also use it to delegate specific permissions when user uses a specific chain.

Password Filter is a feature that automatically updates the password for the appliance whenever the password is changed or reset in the Active Directory.

1 System Requirements

NOTE: To install and remove the Logon Filter, you must have the domain administrator privileges.

Ensure that the following requirements are met:

- Domain controllers based on Microsoft Windows Server 2012 R2/Microsoft Windows Server 2016 are installed.

2 Configuring Preliminary Settings

This chapter contains sections about the pre-configuration settings on Logon Filter.

Configuring Settings for Multitenancy

If Multi-tenancy is enabled, you must add the parameter `tenant_name` with a tenant name as the value in the configuration file: `C:\ProgramData\NetIQ\LogonFilter\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`.

Setting the Logon Filter Parameters

The following configuration allows to improve authentication speed when Logon Filter is used. You can configure the Logon Filter configuration file to decide that how often the logon filter connects to the Advanced Authentication server to update cache and cookie. Perform the following steps to configure the configuration file:

1. Go to `ProgramData\NetIQ\LogonFilter\`
2. Open the `config.properties` file.
3. Specify the following parameters in the configuration file:
   - `config_cache_ttl_sec = 300`

     NOTE: In Advanced Authentication 6.0 and previous versions, Logon Filter queues the server configuration (repositories, MFA tags etc.) on every logon. From Advanced Authentication 6.1, Logon Filter queues the server configuration as per the specified value (by default 300 seconds). When the Advanced Authentication configuration is completed (all the Advanced Authentication Servers in cluster are configured, the MFA tags group are specified, the new repositories are not planned to be added), the value can be increased up to 3600 seconds.

   - `cookie_cache_ttl_sec = 60`

     NOTE: In Advanced Authentication 6.0 and previous versions, Logon Filter validates cookies on Advanced Authentication Server on every logon. It can cause performance issues. From Advanced Authentication 6.1, Logon Filter supports caching of information provided by cookies. The default caching period is 60 seconds. It is sufficient for common

deployment scenarios. In environments where the network connection is slow, the value can be increased. In this case, the administrator must monitor the memory usage because Logon Filter stores the cached cookies in RAM and that causes increased RAM usage.

4 Restart the operating system.

3 Installing and Removing the Logon Filter

This chapter contains the following sections:

Installing the Logon Filter

NOTE: You must install the Logon Filter on all the domain controllers in the domain.

You can find the Logon Filter in the Advanced Authentication Enterprise Edition or Remote Access Edition distributive package.

To install Logon Filter, perform the following steps:

1. Run the `NAAF-logonfilter-x64-<version>.msi` file.
2. Click **Next**.
3. Read and accept the **License Agreement**.
4. Click **Next** or click **Browse** to choose another folder.
   - To change the destination folder, click **Change** and select an applicable destination.
   - To continue, click **Next**.
5. Click **Install**.
6. Click **Finish**.
7. Click **Yes** to restart the operating system.

NOTE: Before you install the Logon Filter, if you have enabled Multitenancy you must specify a tenant name. This is required because an endpoint can be created in a wrong tenant. For more information on configuring the Multitenancy setting, see "Configuration Settings for Multitenancy" in the *Advanced Authentication - Windows Client* guide.

Uninstalling the Logon Filter

1. Right-click **Start** and select **Control Panel** > **Programs** > **Programs and Features.**
2. Select **NetIQ Logon Filter** and click **Uninstall.**
3. Open the Advanced Authentication Administration portal and goto to **Endpoints**. Find and remove an endpoint for the Logon Filter instance that you have uninstalled.

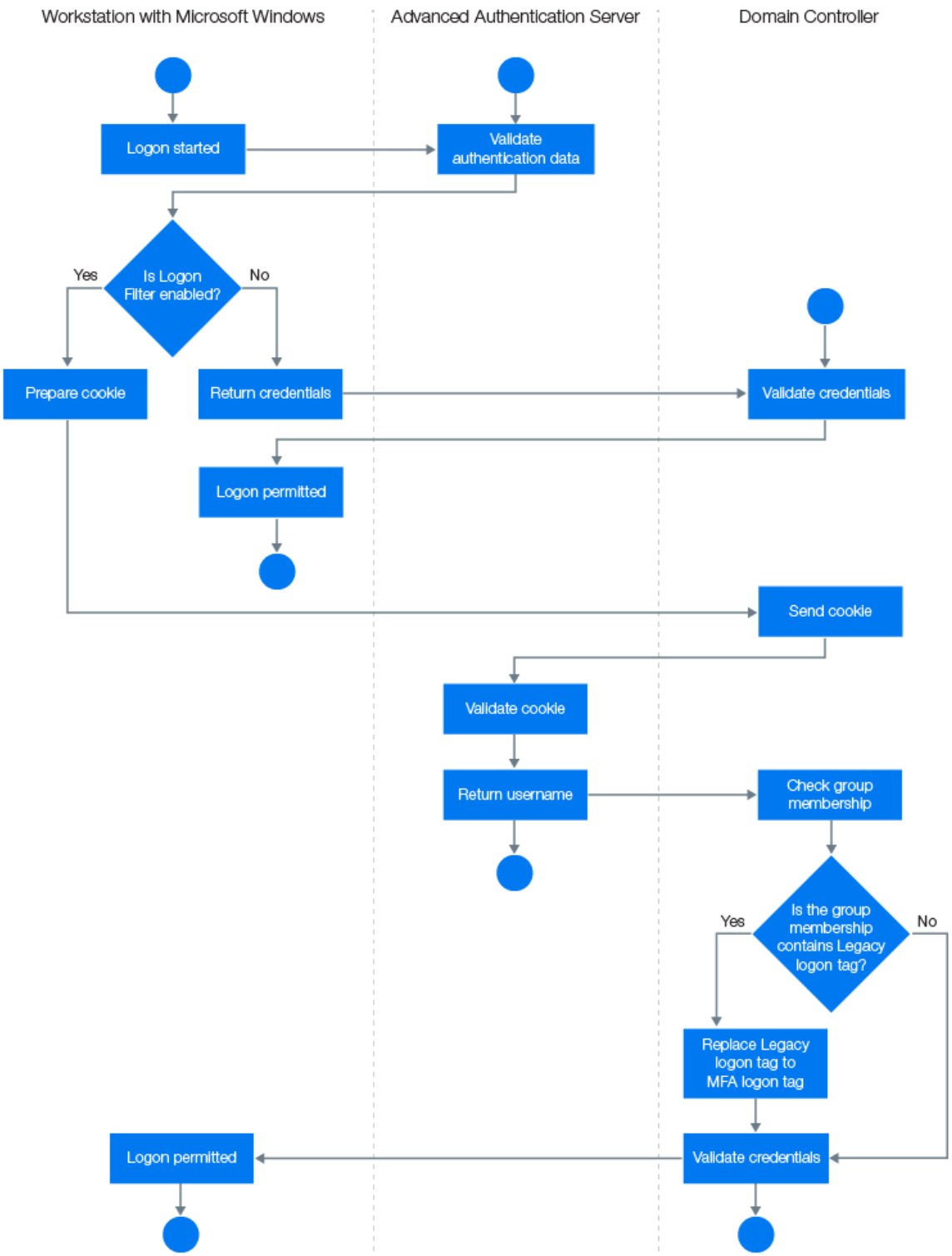
4 Configuring Logon Filter

Logon Filter is a component that you must install on the Domain Controllers. It allows to update the group membership temporarily if you login with Advanced Authentication Windows Client. The change in member does not reflect in Active Directory Users and Computers. The Logon Filter can be used to prevent users to login without the Advanced Authentication Windows Client or to delegate specific permissions when user uses a specific chain.

NOTE: To check the group membership, run the following power shell command:

```
WHOAMI /GROUPS
```

The following diagram illustrates the architecture of the Logon Filter.



This chapter contains the following sections:

Configuring the Logon Filter

1. Install the Advanced Authentication Logon Filter component on all the Domain Controllers.
2. Enable Logon Filter through the Advanced Authentication Administration portal **Policies** > **Logon filter for AD**.
3. Create the following two groups using the **Global** type in Active Directory:
   - **Legacy logon:** Add all users to the group (you can add the **Domain Users** group to its members).
   - **MFA logon:** This group must be an empty group.

   You can use any names for the groups.
4. In the Advanced Authentication Administration portal **Repositories** section, specify an **Active Directory repository**.
5. Expand the **Advanced settings**.
6. Point Legacy logon tag to the Legacy logon group and MFA logon tag to the MFA logon group.

   NOTE: Legacy logon tag must point to a group in the Active Directory that must include all the users. It should be a custom group. The built-in groups like Domain Users are not supported. The users can be members of the group directly or you can add another custom group with users to the group. MFA logon tag must point to an empty group in the Active Directory.

   When a user logs in to Windows and the Logon Filter is enabled, Advanced Authentication Windows Client prepares a cookie, which is sent to the Domain Controller, and then is validated on the Advanced Authentication server. After the validation, Advanced Authentication server returns a username to the Domain Controller that verifies the group membership. If the group membership contains Legacy logon tag, the group is replaced with an MFA logon tag.

   ---
7. Specify a **Password** in the **Repository** settings.
8. Click **Save.**
9. You can configure MFA tags per chain. To do this, specify the MFA tags in the **Advanced settings** of the chain settings. For example, if you specify a **Card users** group from Active Directory in MFA tags for **LDAP Password+Card chain**, then the users who use the chain will be moved from the **Legacy logon** group to the **Card users** group.
10. Ensure that Advanced Authentication Windows Client is installed on all the required workstations.

NOTE: During the login, a user with the NetIQ Windows Client installed will be automatically moved from a group pointed to the Legacy logon tag to a group pointed to the MFA logon tag.

The group specified in the MFA logon tag is added to the user token, so all Kerberos tickets will have it no matter what the service is requested.

The MFA tag does not work while connecting to Remote Desktop, if the user credentials were saved with **Remember my credentials**.

Configuring to Prevent Login Without the Windows Client Installed

If you want to prevent users to log in on all the workstations that do not have the Advanced Authentication Windows Client installed, configure the Microsoft policy **Allow log on locally** in the default **Domain Policy** or a custom GPO. This allows login for only the MFA logon group.

The following procedure helps you to achieve this:

1. On a Domain Controller, open the **Group Policy Management** Editor by specifying `gpmc.msc` in the search box.
2. Double-click the name of the forest, double-click Domains, and double-click the name of the domain in which you want to join a group.
3. Right-click **Default Domain Policy** and click **Edit.**
4. In the console tree, expand and navigate to **Computer Configuration** > **Policies** > **Windows Settings** >**Security Settings** > **Local Policies** > **User Rights Assignment.**
5. In the right pane, double-click **Allow Log on Locally.**
6. Click **Add User** or **Group.**
7. Specify a group which is pointed in the MFA logon tag.
8. Click **OK.**
9. Click **OK** in the **Allow log on locally Properties** dialog box.

Securing Access to File Share on Windows Using the Logon Filter

Perform the following to secure access to file shares on Microsoft Windows with the Logon Filter:

1. Open the properties of a shared folder.
2. Click the **Security** tab.
3. Click **Edit**.
4. Click **Add**.
5. Specify a group that is pointed in the **MFA logon tag.**
6. Click **OK**.
7. Set the required permissions for the added group.
8. Click **OK**.
9. Click the **Sharing** tab.
10. Click **Advanced Sharing.**
11. Click **Permissions**.

12. Click **Add**.
13. Specify a group that is pointed in the **MFA logon tag**.
14. Click **OK**.
15. Set the required permissions for the group.
16. Click **OK**.

If members of Domain Admins or Enterprise Admins groups are using the shared folder, add the **Domain Admins/ Enterprise Admins** group to Members of a group that is pointed in the MFA logon tag to skip the Logon Filter for users of those groups. This is required because for Domain Admins and Enterprise Admins, by default, Microsoft Windows uses the NTLM authentication. Here, the authentication is required every time, but the Logon Filter requires the Kerberos authentication where a single Kerberos ticket obtained during the login to operating system is used instead of communicating to the Domain Controller every time.

NOTE: When a file share is secured by the Logon filter, the file share cannot be accessed. For a solution, see "A File Share Cannot be Accessed When Secured by the Logon Filter".

---

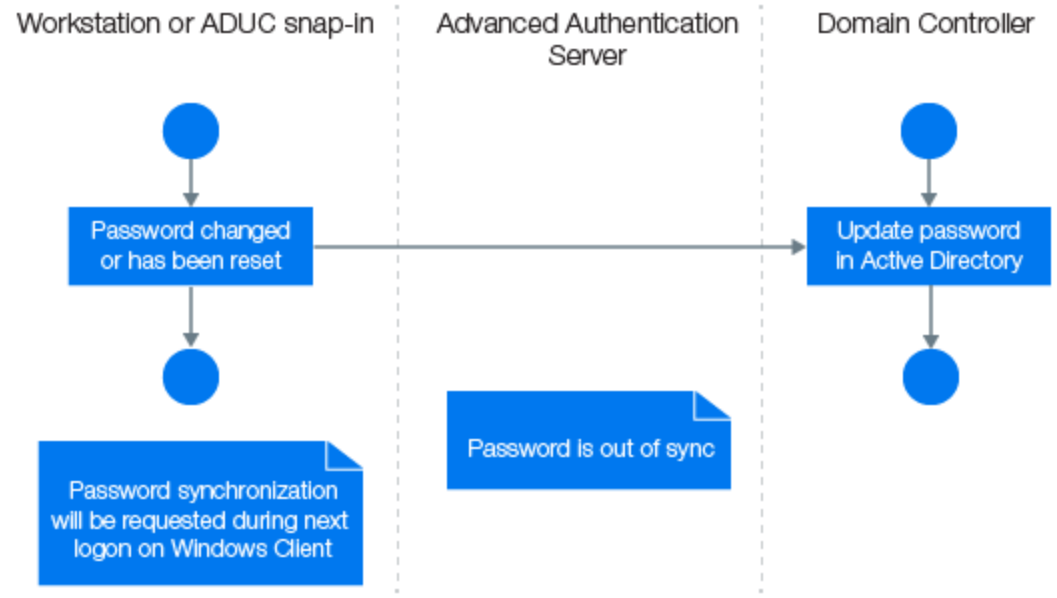
5 Configuring the Password Filter

Password Filter automatically updates the LDAP Password stored inside Advanced Authentication, whenever the password is changed or reset in the Active Directory. This helps you to authenticate without getting any prompt to synchronize the password after it is changed or reset.

NOTE: If you do not include the LDAP Password method in a chain, a prompt to perform a synchronization is displayed. Set **Save LDAP password** to **ON** in the LDAP Password method, the prompt is displayed only for the first time until the password is changed or reset. If you set this option to OFF, a prompt for synchronization is displayed each time.

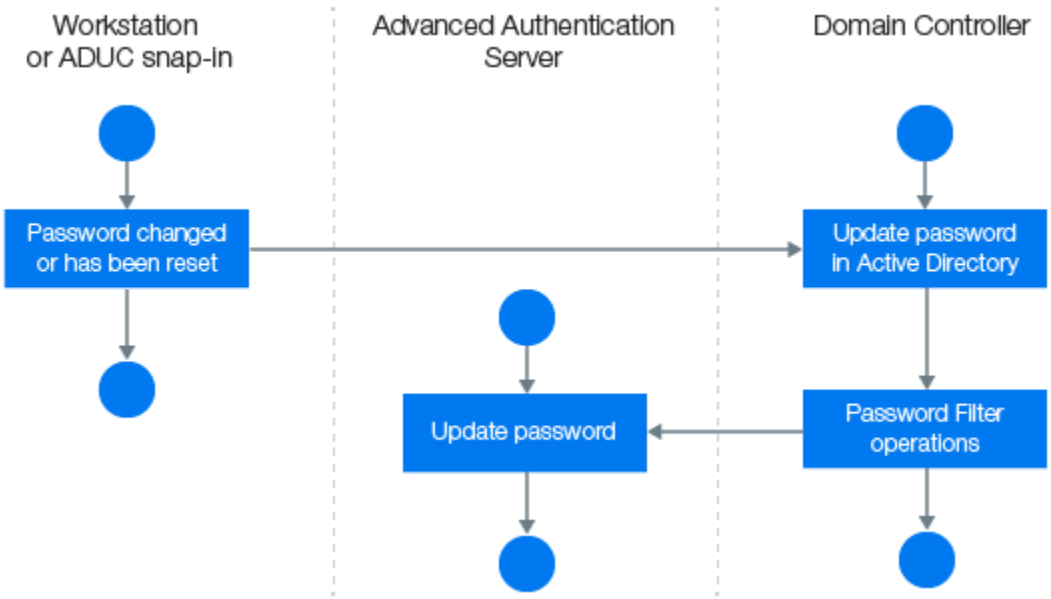
The Figure 5-1 illustrates the situation when you do not use the Password Filter.

Figure 5-1



The Figure 5-2 illustrates the situation when you use the Password Filter.

Figure 5-2



Perform the following steps to configure the Password Filter in the Advanced Authentication Administration portal:

1. Install the Advanced Authentication Logon Filter component on all Domain Controllers.
2. Open the Advanced Authentication Administration portal.
3. Goto to **Endpoints**.
4. Edit the endpoints for all the Domain Controllers one-by-one and set **Is trusted** option to **ON.** Add a Description to save the changes.
5. Enable the Password Filter through the Advanced Authentication Administration portal in **Policies** > **Password filter for Active Directory.**
6. Set **Update password on change** to **ON**, to enable updating of the LDAP password in Advanced Authentication, when the password is changed in the Active Directory. This helps you to authenticate without getting any prompt to synchronize the password after it is changed. If **Update password on change** is set to **OFF**, user will get a request to synchronize the password while logging in to Windows, if the user has changed the password.
7. Set **Update password on reset** to **ON**, to enable automatic update of the LDAP password in Advanced Authentication, when it is reset in the Active Directory. This helps you to authenticate without getting any prompt to sync the password if it is reset. If **Update password on reset** is set to **OFF**, user will get a request to synchronize the password while logging in to Windows, if the administrator has reset the user's password.

NOTE: If **Enable local caching** is set to **ON** in the Cache Options and **forceCachedLogon** parameter is set to **True**, when the password is changed or reset in the Active Directory. Then, a user is prompted to synchronize the password while logging in to Windows Client irrespective of the status of the following **Password Filter for AD** settings:

- **Update password on change**
- **Update password on reset**

If **forceCachedLogon** set as **False**, the Password Filter works according to the settings configured in the **Password Filter for AD** policy

If **Enable local caching** is set to **OFF**, the Password Filter works according to the settings configured in the **Password Filter for AD** policy.

NOTE: Endpoint for Password Filter must be trusted. To set this option, open the Advanced Authentication Administration portal > **Endpoints**, edit an endpoint of the Password Filter, set **Is trusted** flag to **ON**. Save the changes.

6 Troubleshooting

This chapter contains the following troubleshooting for the Logon Filter:

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” on page 24
- “Manual” on page 24

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`.

Incorrect Username Saved By the Remote Desktop Connection

Issue: When the Logon Filter is enabled and if a user selects **Remember my credentials** while connecting to a terminal server with the Remote Desktop Connection, a wrong username is saved. When the user tries to login the next time, the wrong username is prompted. This issue happens when the **Logon Filter for AD** policy is enabled in the Administration portal.

Workaround: Do not select the option **Remember my credentials** while connecting to Remote Desktop.

A File Share Cannot be Accessed When Secured by the Logon Filter

Issue: When a file share is secured by the Logon filter, the file share cannot be accessed.

Solution: Perform the following steps:

1. Execute the **whoami /groups** after logging in to the operating system to ensure that the user is in the group that is pointed in the MFA logon tag.
2. Use the **Security** event log on the Domain Controller to ensure that the NTLM is not used for the authentication.