Installation Guide

Advanced Authentication - Logon Filter

Version 5.5

Legal Notices

Contents

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

About this Book

The 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 which should be installed on the Domain Controllers. It increases security by forbidding logging in of users without the Advanced Authentication solution. Password Filter is a feature which automatically updates the password for the appliance whenever the password is changed or reset in the Active Directory.

1 System Requirements

IMPORTANT: Installing and removing Logon Filter requires Domain Admin privileges.

The following system requirements should be fulfilled:

- Domain controllers based on Microsoft Windows Server 2008 R2/ Microsoft Windows Server 2012 R2/Microsoft Windows Server 2016.

2 Installing and Removing Logon Filter

In this chapter:

- Installing Logon Filter
- Removing Logon Filter

2.1 Installing Logon Filter

NOTE: Logon Filter must be installed on all domain controllers in the domain.

To install Logon Filter via Setup Wizard:

1. Run `NAAF-logonfilter-x64-<version>.msi`.
2. Click **Next** to continue.
3. Read the **License Agreement**. Select the **I accept the terms in the license agreement** checkbox and click **Next**.
4. Click **Next** to install to the default folder or click **Browse** to choose another.
   - To change the destination folder, click the **Change** button and select an applicable destination.
   - To continue, click **Next**.
5. Click **Install** and wait until the component is installed.
6. Click **Finish** to close the Wizard.
7. Click **Yes** to restart the operating system.

NOTE: Before you install 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.

2.2 Removing Logon Filter

Logon Filter can be removed via Setup Wizard or Control Panel.

To remove Logon Filter via Setup Wizard, follow the steps:

1. Right-click the Start button and select **Control Panel** > **Programs** > **Programs and Features.**
2. Select **NetIQ Logon Filter** and click **Uninstall.**
3. Confirm the removal.
4. Wait for a few seconds until the removal is completed.
5. Open Advanced Authentication Administrative Portal and switch to **Endpoints** section. Find and remove an endpoint for the uninstalled Logon Filter instance.

3 Configuring Logon Filter

Logon Filter is a component which should be installed on the Domain Controllers. It increases security by forbidding logging in of users without the Advanced Authentication solution.

Perform the following steps to configure Logon Filter:

1. Install the Advanced Authentication Logon Filter component on all Domain Controllers.
2. Enable Logon Filter through the Advanced Authentication - Administrative Portal: **Policies** section > **Logon filter for AD** > switch to **ON**.
3. Create the following two groups in Active Directory:
   - Legacy logon – add all users to the group (you can just add the Domain Users group to its members).
   - MFA logon – this should be an empty group.

   (you can use any names for the groups)
4. Navigate in the Advanced Authentication - Administrative Portal:

   Repositories > specify a used Active Directory repository > scroll down > expand **Advanced settings** > scroll to the bottom.
5. 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 should point to an empty group in Active Directory. When a user logs in, Logon Filter checks the user’s authentication. If the user uses the Advanced Authentication, then the user is automatically moved to the group specified in the MFA logon tag field
6. Scroll up and enter a Password in the Repository Settings.
7. Scroll down and click **Save.**
8. Wait for a minute.
9. Ensure that Advanced Authentication Windows Client is installed on all required workstations.
10. When you are ready to prohibit logon on all workstations which do not have the AA Windows Client installed, configure the Microsoft policy **Allow log on locally** in the Default Domain Policy or a custom GPO to allow logon for only MFA logon group using the following steps:.
    a. On a Domain Controller, open Group Policy Management Editor by entering gpmc.msc in the search box.
    b. Double-click the name of the forest, double-click Domains, and then double-click the name of the domain in which you want to join a group.
    c. Right-click **Default Domain Policy,** and then click **Edit.**
    d. In the console tree, expand and navigate to **Computer Configuration** > **Policies** > **Windows Settings** >**Security Settings** > **Local Policies** > **User Rights Assignment.**
    e. In the right pane, double-click **Allow Log on Locally.**
    f. Click **Add User** or **Group.**

g. Specify a group which is pointed in the MFA logon tag.
h. Click **OK.**
i. Click **OK** in the **Allow log on locally** Properties dialog box.

NOTE: The above steps prohibits the users without NetIQ Windows Client installed (only on workstations joined to the domain) from logging on to the workstations. 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.

4 Configuring 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.

Perform the following steps to configure Password Filter:

1. Install the Advanced Authentication Logon Filter component on all Domain Controllers.
2. Enable Password Filter for AD through the Advanced Authentication - Administrative Portal: **Policies section** > **Password Filter for AD.**
3. Set **Update password on change** option to **ON**, to enable updating of the LDAP password in Advanced Authentication, when it is changed in the Active Directory. This helps you authenticate without getting any prompt to sync 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 he/she changed his/her password where the user will need to enter an actual password.
4. Set **Update password on reset** option to **ON**, to enable updating 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 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 administrator has reset the user's password where the user will need to enter an actual password.

NOTE: Endpoint for Password Filter should be trusted. To set this option, open the Advanced Authentication - Administrative Portal > **Endpoints** section, edit an endpoint of the Password Filter, set **Is trusted** flag to **ON** and add a description. Save the changes.

5 Troubleshooting

This chapter provides information about troubleshooting the Logon filter.

- Section 5.1, "Incorrect Username Saved By Remote Desktop Connection," on page 17

5.1 Incorrect Username Saved By Remote Desktop Connection

When the Logon Filter is used 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 Administrative portal.

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