Installation Guide

Advanced Authentication - Linux PAM Client

Version 5.6

Legal Notices

Contents

About NetIQ Corporation **5**
About this Book **7**

1 System Requirements **9**

2 Configuration **11**

2.1 Setting a DNS for Server Discovery . . . 11
2.2 Preparing Linux for Installating Linux PAM Client . . . 15
2.3 Using a Specific Advanced Authentication Server . . . 15
2.4 Configuration Settings for Multitenancy . . . 15
2.5 Selecting an Event . . . 16

3 Installing and Uninstalling Linux PAM Client **17**

3.1 Installing and Uninstalling Linux PAM Client on CentOS, Red Hat Enterprise Linux Client, and Server 7.2 . . . 17
3.2 Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server 12 . . . 18

4 Troubleshooting **19**

4.1 Endpoint Not Found . . . 19

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

This guide describes the system requirements and installation procedure of Advanced Authentication Linux PAM Client.

Intended Audience

This book is intended for administrators who implements a secure, distributed administration model.

About Linux PAM Client

Linux PAM Client enables you to log in to Linux in a more secure way by using the authentication chains configured in Advanced Authentication.

NOTE: Only the users from Active Directory repository can be used for login purpose.

NOTE: Linux PAM Client supports offline logon (when the Advanced Authentication Server is not available) for non-local accounts for authentication chains which contains the following methods: LDAP Password, Password, HOTP, TOTP, Smartphone (offline mode), Card, FIDO U2F, and PKI.

NOTE: Advanced Authentication secures SSH by providing multifactor authentication for only the methods that do not require Advanced Authentication Device Service. The Smartphone method is supported in out-of-band (online) mode. This is supported only when Linux machine is a member of Active Directory domain and when you use Active Directory as a repository.

1 System Requirements

IMPORTANT: You must have root privileges to install and uninstall the Linux PAM Client.

Ensure that the system meets the following requirements:

- CentOS 7, SUSE Linux Enterprise Desktop 12 Service Pack1, SUSE Linux Enterprise Server 12 Service Pack1, Red Hat Enterprise Linux Client 7.2, or Red Hat Enterprise Linux Server 7.2 is installed. Gnome Display Manager (GDM) should be set as the login manager.
- DNS is configured for Advanced Authentication Server discovery (see Setting a DNS for Server Discovery) or a specific Advanced Authentication server must be specified in the configuration file.

NOTE: Only the Active Directory users can log in. Other repositories are not supported.

2 Configuration

This chapter contains the following information:

- Section 2.1, “Setting a DNS for Server Discovery,” on page 11
- Section 2.2, “Preparing Linux for Installating Linux PAM Client,” on page 15
- Section 2.3, “Using a Specific Advanced Authentication Server,” on page 15
- Section 2.4, “Configuration Settings for Multitenancy,” on page 15
- Section 2.5, “Selecting an Event,” on page 16

2.1 Setting a DNS for Server Discovery

1 Open a DNS Manager. To open the DNS Manager, click **Start**, point to **Administrative Tools**, and click **DNS**.

2 Add Host A or AAAA record and PTR record:

   2a In the console tree, right-click the forward lookup zone that includes your domain name and click **New Host (A or AAAA).**

   2b Specify a DNS name for the Advanced Authentication Server in **Name**.

   2c Specify the IP address for the Advanced Authentication Server in **IP address.** You can specify the address in IP version 4 (IPv4) format (to add a host (A) resource record) or IP version 6 (IPv6) format (to add a host (AAAA) resource record).

   2d Select **Create associated pointer (PTR) record** to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you provided in **Name** and **IP address.**

3 Add an SRV record:

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

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

   3a For Advanced Authentication servers from a primary Advanced Authentication site (a site with Global Master server):

      3a1 In the console tree, locate **Forward Lookup Zones** and right-click on a node with domain name and click **Other New Records**.

      3a2 In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.

      3a3 Click **Service** and then specify **_aaa.**

      3a4 Click **Protocol** and then specify **_tcp**.

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

3a5 In **Host offering this service,** specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.

3a6 Click **OK**.

3b For Advanced Authentication servers from other Advanced Authentication sites:

3b1 In the console tree, locate **Forward Lookup Zones**, switch to a node with domain name then to _sites node, right-click on an appropriate site name and click **Other New Records.**

3b2 In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record.**

3b3 Click **Service** and then specify **_aaa**.

3b4 Click **Protocol** and then specify **_tcp**.

3b5 Click **Port Number** and then specify **443**.

3b6 In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.

3b7 Click **OK**.

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

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

- **Service**: symbolic name of an applicable service.
- **Proto**: transport protocol of an applicable service. Mostly, TCP or UDP.
- **Name**: domain name for which this record is valid. It ends with a dot.
- **TTL**: standard DNS time to live field.
- **Class**: standard DNS class field (this is always IN).
- **Priority**: priority of the target host. Lower value indicates that it is more preferable.
- **Weight**: a relative weight for records with the same priority. Higher value indicates that it is more preferable.
- **Port**: TCP or UDP port on which the service is located.
- **Target**: canonical host name of the machine providing the service. It ends with a dot.

Configuring Authentication Server Discovery on Client

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

- `discovery.Domain`: DNS name of the domain. For a Windows Client, this value is used if workstation is not connected to the domain.
- `discovery.subDomains`: list of additional sub domains separated by a semicolon. You can use them on a MacOS Client or Linux Client to list AD sites.
- `discovery.useOwnSite`: set the value to `True` to use the local site (Windows Client only).
- `discovery.dnsTimeout`: timeout for the DNS queries. The default value is 15 seconds.

Authentication Server Discovery Flow

Windows Client

The feature is not supported in Windows Client.

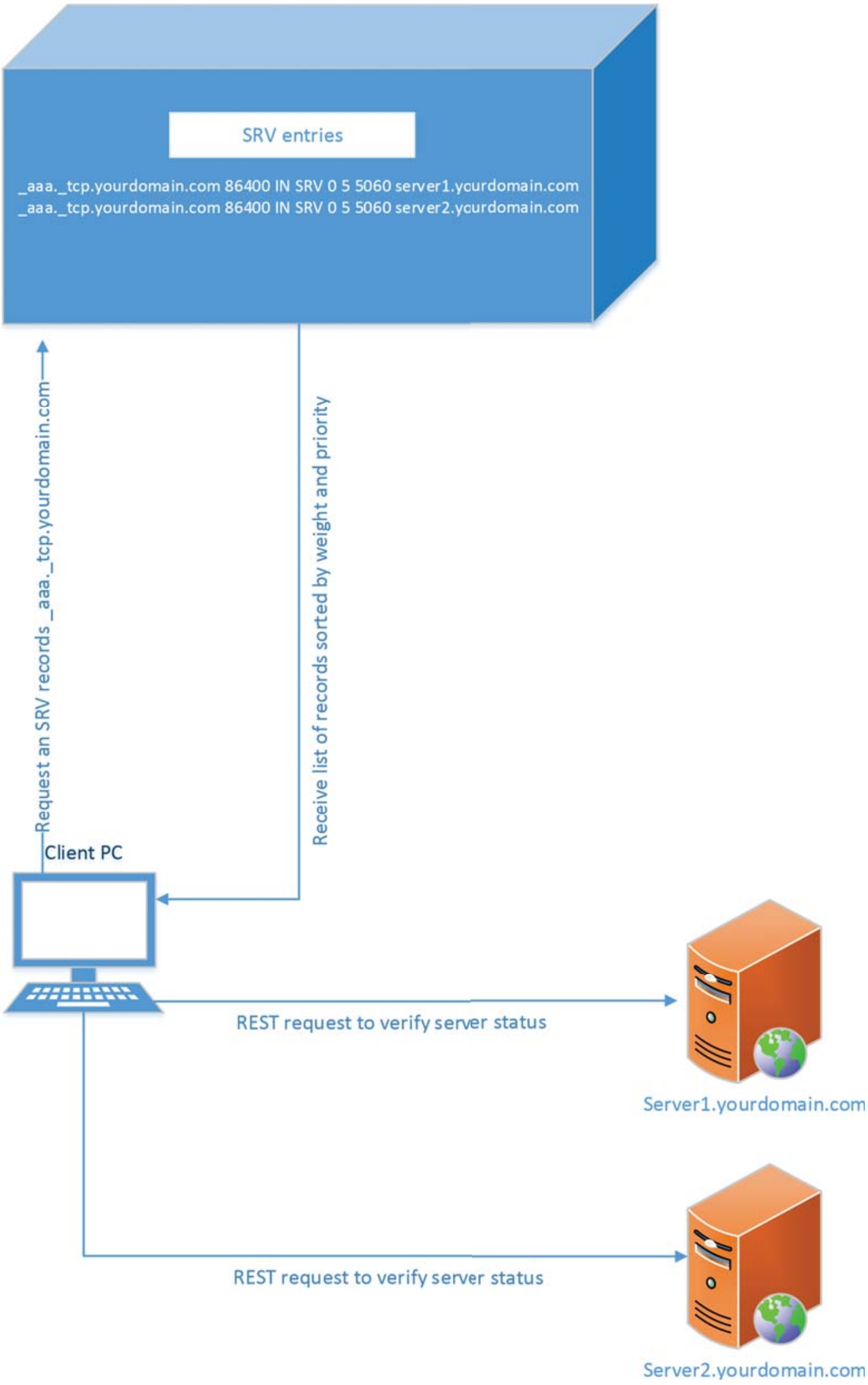
MacOS Client/ Linux PAM Module

1. Get servers from the sub domains listed in `discovery.subDomain`.
2. Get servers from the domain specified in `discovery.Domain` (global list).

Path for the configuration file is as follows:

- **MacOS Client**: `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.
- **Linux PAM module**: `/opt/pam_aucore/etc/pam_aucore.conf`.

The following diagram illustrates the server discovery workflow graphically.


SRV entries
_aaa._tcp.yourdomain.com 86400 IN SRV 0 5 5060 server1.yourdomain.com
_aaa._tcp.yourdomain.com 86400 IN SRV 0 5 5060 server2.yourdomain.com
Request an SRV records _aaa._tcp.yourdomain.com
Receive list of records sorted by weight and priority
Client PC
REST request to verify server status
Server1.yourdomain.com
REST request to verify server status
Server2.yourdomain.com

2.2 Preparing Linux for Installating Linux PAM Client

You must disable SELinux and configure networking before installing Linux PAM Client.

To disable SELinux, perform the following steps:

1. Open the configuration file `sudo nano /etc/selinux/config`.
2. Change `SELINUX=enforcing` to `SELINUX=disabled`.
3. Save the changes in the file.
4. Reboot your system.

To configure networking, perform the following steps:

1. Ensure that DNS is properly configured for server discovery.
2. Set Search Domains to `FQDN`.

   For example, in CentOS 7, you can set `/etc/sysconfig/network-scripts/ifcfg-eth0` by adding `DOMAIN=mycompany.com`.

2.3 Using a Specific Advanced Authentication Server

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

In the `/opt/pam_aucore/etc/pam_aucore.conf` file, configure `discovery.host = <IP_address|domain_name>`.

For example, `discovery.host = 192.168.20.40` or `discovery host = auth2.mycompany.local.`

You can specify a port number (optional parameter) for the client-server interaction: `discovery.port = <portnumber>`.

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

2.4 Configuration Settings for Multitenancy

If Multi-tenancy is enabled, you must add the parameter `tenant_name` with a used tenant name as value in the configuration file: `/opt/pam_aucore/etc/pam_aucore.conf.` For example, specify `tenant_name=TOP` for the TOP tenant in the file. If the configuration file does not exist, you must create it.

NOTE: If you do not add the parameter `tenant_name`, you might get an error `Tenant not found.`

2.5 Selecting an Event

By default Linux logon event is used. However, in some cases it is required to create a separate event. For example, when the predefined event is used for domain joined workstations, you can create a custom event with type `Generic` for the non-domain joined workstations. In this case you will need to point these [non-domain] workstations to the custom event using the following parameter in the `event_name: <CustomEventName>` configuration file:

```
/opt/pam_aucore/etc/pam_aucore.conf
```

3 Installing and Uninstalling Linux PAM Client

You can install and uninstall Linux PAM Client on the following platforms:

- Installing and Uninstalling Linux PAM Client on CentOS, Red Hat Enterprise Linux Client, and Server 7.2
- Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server 12

NOTE: You cannot upgrade the Linux PAM Client. To install the latest client, you must uninstall the previous version and install the new client. For more information on installing Linux Client, see Installing and Uninstalling Linux PAM Client.

You can find the Linux PAM Client in the Advanced Authentication Enterprise Edition distributive package.

3.1 Installing and Uninstalling Linux PAM Client on CentOS, Red Hat Enterprise Linux Client, and Server 7.2

To install Linux PAM Client on CentOS, RHEL Client, and Server 7.2, perform the following steps:

1. Run the following command:

   ```
   sudo yum install -y ./naaf-linuxpamclient-centos-release-<version>.rpm.
   ```

2. Run the following configuration script:

   ```
   sudo chmod +x /opt/pam_aucore/bin/bind-to-ad.sh.
   ```

   ```
   sudo /opt/pam_aucore/bin/bind-to-ad.sh MYCOMPANY mycompany.com Administrator
   ```

   where `MYCOMPANY` is your domain name and `mycompany.com` is your FQDN. Administrator is a domain account that contains permissions to integrate the machines to the domain.

3. If your Linux workstation is bound to a domain, ensure that you select **OS Logon (domain)** as the **Event type** for **Linux logon event** and you complete the configuration:

   ```
   su username
   ```

   where, username is the user name of any user account from a domain.

   Else select **OS Logon (local)** as **Event type** for the **Linux logon event**.

To uninstall Linux PAM Client on CentOS, perform the following steps:

1. Run the following command:

   ```
   cd /opt/pam_aucore/bin/sudo ./uninstall
   ```

2. Open Advanced Authentication - Administrative Portal. Switch to **Endpoints** section. Find and remove endpoint for the Linux PAM Client instance.

3.2 Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server 12

To install Linux PAM Client on SUSE Linux Enterprise Desktop and Server 12, perform the following steps:

1. Run the following command:

   ```
   rpm -i naaf-linuxpamclient-suse-release-<version>.rpm
   ```

2. Run the following command:

   If Linux machine is not bound to a domain and you select **OS logon (local)** type as the **Linux logon** event:

   ```
   sudo /opt/pam_aucore/bin/activate-nondomain.sh
   ```

   If Linux machine is bound to a domain and you select **OS logon (domain)** type as the **Linux logon** event:

   ```
   sudo /opt/pam_aucore/bin/activate.sh mycompany.com
   ```

   where mycompany.com is your FQDN.

To uninstall Linux PAM Client on SUSE Linux Enterprise Desktop, perform the following steps:

1. Run the following commands:

   ```
   sudo /opt/pam_aucore/bin/deactivate.sh
   ```

   ```
   sudo rpm -e pam_aucore
   ```

2. Open Advanced Authentication - Administrative Portal. Switch to **Endpoints** section. Find and remove endpoint for the Linux PAM Client instance.

4 Troubleshooting

To investigate the possible issues, analyze the debug logs.

The logs are placed in the `/opt/pam_aucore/var/log/pam_aucore` folder.

The logs are also recorded in the files:

- `/var/log/messages`
- `/var/log/secure`

4.1 Endpoint Not Found

Issue

After installing the client component and rebooting, the client reports `Endpoint not found` error and it is not possible to login.

Reason

An endpoint for the client already exists on server or in configuration file on the client.

Solution

1. Remove the endpoint for the client on the server in Administrative Portal - Endpoints section (if it exists).
2. Boot in Safe mode and remove endpoint_id, endpoint_name and endpoint_secret parameters from `/opt/pam_aucore/etc/pam_aucore.conf`.
3. Reboot.