Advanced Authentication 6.2

Linux PAM Client Installation Guide

February 2019

Legal Notices

Contents

About This Book 5
About NetIQ Corporation 7

1 System Requirements 9

2 Securing SSH 11

3 Offline Support for Linux PAM Client 13

4 Configuring the Preliminary Settings 15

Configuring the Mandatory Settings 15
Using a Specific Advanced Authentication Server in Non-DNS Mode 15
Setting-up a DNS for Advanced Authentication Server Discovery 16
Preparing Linux for Installing Linux PAM Client 20
Preinstalling the Configuration on Ubuntu 16 20
Configuring Optional Settings 21
Configuration Settings for Multitenancy 22
Selecting an Event 22
Configuring Timeout for Card Waiting 23
Configuring Timeout for the U2F Authentication 23
Enabling Logs on Linux Client 23
Configuring Verification of Server Certificates 24
Enabling the Authentication Agent Chain 25
Configuring the Enforced Cached Login 25

5 Installing and Uninstalling Linux PAM Client 27

Installing and Uninstalling Linux PAM Client on CentOS and Red Hat Enterprise Linux 28
Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server 28
Installing and Uninstalling Linux PAM Client on Ubuntu and Debian 9 29

6 Troubleshooting 31

Endpoint Not Found 31
Endpoint Already Exists 31
Users Are Unable to Log In with a Domain Account After Booting 31
Domain Users Are Unable to Log In Even After Authenticating All the Methods In a Chain 32

About This Book

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

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

Ensure to meet the following system requirements:

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

Requirement	Detail
Operating System	◆ CentOS 7 with KDE or Gnome desktop environment ◆ SUSE Linux Enterprise Desktop 12 Service Pack 3 (64-bit) ◆ SUSE Linux Enterprise Desktop 15 ◆ SUSE Linux Enterprise Server 11 Service Pack 4 (64-bit) ◆ SUSE Linux Enterprise Server 12 Service Pack 3 (64-bit) ◆ SUSE Linux Enterprise Server 15 ◆ Red Hat Enterprise Linux Workstation 7.5, 7.6 ◆ Red Hat Enterprise Linux Server 7.5, 7.6 ◆ Debian 9.6 ◆ Ubuntu 16, 18
Login Setting	Set Gnome Display Manager (GDM) as the login manager in CentOS.

2 Securing SSH

To use Advanced Authentication in the SSH (Secure Shell) mode, configure the following parameters in the file `/etc/ssh/sshd_config`:

- Set `PasswordAuthentication` to no
- Set `ChallengeResponseAuthentication` to `yes`

To apply the changes in the file `sshd_config`, you must restart the SSH Service. To restart the SSH Service, run the command `sudo service sshd restart` in the terminal.

Advanced Authentication secures SSH by providing multi-factor authentication only for the methods that do not require Advanced Authentication Device Service.

NOTE: You can use the Authentication Agent to use methods such as fingerprint and card to secure SSH. For more information, see “Enabling the Authentication Agent Chain”.

IMPORTANT: Advanced Authentication does not support the multi-factor authentication to a Terminal or SSH for the domain users when Linux machine is used in a non-domain mode.

---

3 Offline Support for Linux PAM Client

You can log in to the Advanced Authentication Linux PAM Client in the offline mode (when the Advanced Authentication server is not available) for non-local accounts of the authentication chains. The authentication methods that support the offline mode are:

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

4 Configuring the Preliminary Settings

This chapter contains the following sections about the pre-configuration settings in Linux Client:

- "Configuring the Mandatory Settings" on page 15
- "Configuring Optional Settings" on page 21

Configuring the Mandatory Settings

You must perform the following tasks based on different distributions of the Linux operating system:

- To set up an interaction between Linux Client and the Advanced Authentication server, perform one of the following:
  - Configure Advanced Authentication server lookup in non-DNS mode by manually specifying a custom Advanced Authentication server. For more information, see "Using a Specific Advanced Authentication Server in Non-DNS Mode".

    Or
  - Allow Linux Client to interact with the Advanced Authentication servers through the DNS and configure the DNS for Advanced Authentication server lookup. For more information, see "Setting-up a DNS for Advanced Authentication Server Discovery".
- To prepare Linux for installing the Linux PAM Client, see "Preparing Linux for Installing Linux PAM Client".
- To prepare Ubuntu 16 for installing the Linux PAM Client, see "Preinstalling the Configuration on Ubuntu 16".

Prerequisite for Advanced Authentication Server discovery

Ensure that the DNS is configured appropriately for Advanced Authentication server discovery (see Setting-up 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 Non-DNS 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 domain based entry for a specific workstation and use the settings specified in the `pam_aucore.conf` file.

To configure Linux Client to discover a specific Advanced Authentication server without a DNS, perform the following steps:

1 Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.

2 Specify `discovery.host: <IP_address|domain_name>`.

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

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

3 (Optional) Specify `discovery.port = <portnumber>` to configure the port number for the Client-server communication.

4 Restart the system.

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

Setting-up a DNS for Advanced Authentication Server Discovery

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

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

- "Adding a Host in DNS" on page 16
- "Adding an SRV Record" on page 17
- "Configuring Authentication Server Discovery in Client" on page 19

Adding a Host in DNS

1 Click **Start > Administrative Tools > DNS** to open the DNS Manager.

2 Add Host A or AAAA record and PTR record:

2a Right-click your domain name and click **New Host (A or AAAA)** under **Forward Lookup Zone** in the console tree.

2b Specify a DNS name of the Advanced Authentication server in **Name**.

2c Specify the IP address of 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 using the details 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 in the 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 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** and click **Create Record**.
3. Specify **_aav6** in **Service** of **New Resource Record** dialog box.
4. Specify **_tcp** in **Protocol**.
5. Specify **443** in **Port Number**.
6. Specify the full qualified domain name (FQDN) of the server that is added in **Host offering this service**.

   For example, `authsrv.mycompany.com`.
7. Click **OK**.

Adding an SRV Record from Other Advanced Authentication Sites

To add an SRV record for the Advanced Authentication servers from other Advanced Authentication sites, perform the following steps:

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** and click **Create Record.**
4. Specify **_aav6** in **Service** of **New Resource Record** dialog box.
5. Specify **_tcp** in **Protocol**.
6. Specify **443** in **Port Number**.
7. Specify the FQDN of the server in **Host offering this service**.

   For example, `authsrv.mycompany.com`.
8. Click **OK**.

You must add a host and SRV records in the DNS for all the authentication servers. The **Priority** and **Weight** values for different servers may vary.

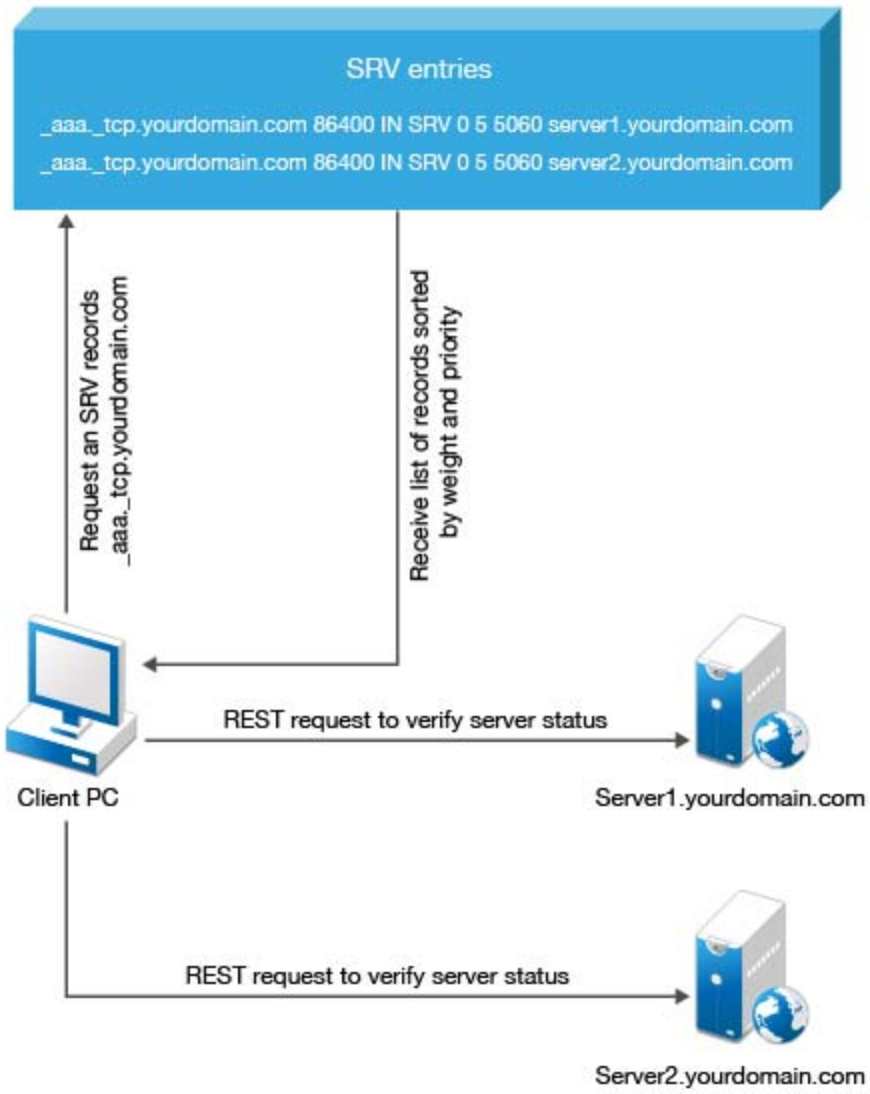
DNS Server Entries

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 describes these elements present in an SRV record:

Element	Description
Service	Symbolic name of an applicable service.
Protocol	Transport protocol of an applicable service. Typically, TCP or UDP.
Domain	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 (set as IN, by default).
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 Linux Client by using the following parameters in the `pam_aucore.conf` file:

Parameter	Description
`discovery.Domain`	DNS name of the domain.
`discovery.host`	Option to specify the port number for the client-server interaction.
`discovery.port`	Option to specify the DNS name or the IP address of an Advanced Authentication server.
`discovery.subDomains`	Lists additional sub-domains separated by a semicolon.

Parameter	Description
discovery.useOwnSite	Set the value to True to use the local site (Windows Client only).
discovery.dnsTimeout	Set the 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 Linux Client.
discovery.wakeupTimeout	Time out after the system starts or resumes from sleep. The default value is 10 seconds.
discovery.skipAlreadyTriedPeriod	A delay for which the Linux 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.

You can find the configuration file pam_aucore.conf in the path /opt/pam_aucore/etc/.

Preparing Linux for Installing Linux PAM Client

You can add Linux Client to a specific domain and configure the network, by setting **Search Domains** with FQDN.

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

Preinstalling the Configuration on Ubuntu 16

Before installing the Linux PAM Client on Ubuntu 16, you must configure lightdm to achieve the following:

- Allow manual login
- Hide the user list
- Disable guest login

For more information about lightdm, see LightDM.

To configure lightdm on Ubuntu 16, perform the following steps:

1. Navigate to /usr/share/lightdm/lightdm.conf.d.
2. Double click the 50-ubuntu.conf file and add the following parameters:
   - [SeatDefaults]
   - greeter-show-manual-login=true

- `greeter-hide-users=true`
- `allow-guest=false`

3 Click **Save**.

Configuring Optional Settings

The following table describes the optional settings that you can configure for Linux Client:

Setting	Description
tenant_name	If you use Multitenancy, you must point Linux Client to a specific tenant. For more information, see Configuration Settings for Multitenancy.
event_name: <CustomEventName>	If you want to use both domain-joined and non-domain machines, you can use a custom event for the specific machines. For more information, see Selecting an Event.
card.timeout: X	To change a default Card waiting timeout. For more information, see Configuring Timeout for Card Waiting.
u2f.timeout: X	To configure the timeout for authentication with the U2F token, see Configuring Timeout for the U2F Authentication.
logEnabled: true	Enable the logs of Linux Client for debugging. For more information, see Enabling Logs on Linux Client.
verifyServerCertificate	To configure the verification of server certificates for LDAP connection. For more information, see Configuring Verification of Server Certificates.
authentication_agent_enabled	Enables the **Authentication Agent** chain in Linux Client. For more information, see Enabling the Authentication Agent Chain.
forceCachedLogon	To enforce the cached login for unlocking the Client. For more information, see Configuring the Enforced Cached Login.
default_repo	

NOTE: A separator between the setting and its value can be either equal (=) or colon (:).

Configuration Settings for Multitenancy

If the Multitenancy option is enabled, you must add the parameter `tenant_name` with a tenant name as the value in the `pam_aucore.conf` file.

To configure a specific tenant name, perform the following steps:

1. Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.
2. Specify `tenant_name: <name of tenant>`

   For example, `tenant_name: TOP` for the TOP tenant.

   If the configuration file does not exist, create a new file.
3. Save the changes.
4. Restart the system.

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

Creating a Linux Endpoint When the Tenant Name Matches the Domain

In the Multitenancy mode, by default a new endpoint gets mapped to the tenant name that has the same name as the domain name. You can also add an endpoint to a preferred tenant that does not have the same name as the domain.

To add an endpoint to specific tenant in the Multitenancy mode, perform the following steps:

1. Install the PAM Client.
2. Edit the configuration file `pam_aucore.conf`, set the `tenant_name` parameter with the preferred tenant name.

   For example, TOP.
3. Run an activation script for the domain mode.
4. Save the changes.
5. Restart the system.

Selecting an Event

By default, Linux Client uses the **Linux 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-DNS joined workstations.

To configure custom event for Linux Client, perform the following steps:

1. Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.
2. Specify `event_name: <CustomEventName>`

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

3 Save the changes.

4 Restart the system.

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. Subsequently, the user login selection screen is displayed.

To configure the timeout for card waiting, perform the following steps:

1 Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.

2 Specify `card.timeout: X`.

x is the timeout value in seconds. The card timeout value is set to 60 seconds, by default.

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

3 Save the changes.

4 Restart the 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 `opt/pam_aucore/etc/pam_aucore.conf`.

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

2 Specify `u2f.timeout: X` in the `aucore.conf` file. X is the timeout value in seconds.

3 Save the configuration file.

4 Restart the operating system.

Enabling Logs on Linux Client

You can enable the logs of Linux Client to view the logs for debugging.

To enable the logs of Linux Client, perform the following steps:

1 Run the following command to edit the configuration file:

```
sudo vi /opt/pam_aucore/etc/pam_aucore.conf
```

2 Specify `logEnabled:true`.

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

3 Save the changes.

4 Restart the system.

The logs are generated in the path `/opt/pam_aucore/var/log/`.

Configuring Verification of Server Certificates

You can secure the connection between Linux Client and the Advanced Authentication servers with a valid SSL certificate. This prevents any attacks on the connection and ensures safe authentication.

You can enable verification of a server certificate on Linux platforms in the following ways:

- Using PAM Certificate Path
- Using OS Specific Certificate Path

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.

Using PAM Certificate Path

To enable verification of a server certificate in the PAM certificate path on any Linux platform, perform the following steps:

1. Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.
2. Specify `verifyServerCertificate:true`.

   If the configuration file does not exist, create a new file.
3. Place the trusted certificates in the path `/opt/pam_aucore/certs`.

   If the certificates are not available in `/opt/pam_aucore/certs`, the PAM module searches for an OS specific certificate directory.

   NOTE: Ensure that the server certificates are in `.cert` or `.crt` format.

   ---
4. Run the command `sudo chmod 644` to set permission for certificates.
5. Restart the system.

Using Operating System Specific Certificate Paths

To enable verification of a server certificate in the operating system (OS) specific certificate path, perform the following steps:

1. Navigate to `/opt/pam_aucore/etc` and open the `pam_aucore.conf` file.
2. Specify `verifyServerCertificate:true`.

   If the configuration file does not exist, create a new file.
3. Place the trusted certificates in the OS specific path of the respective Linux platform. Following are the OS specific paths of the Linux platforms:
   - **CentOS 7.x, Red Hat** - `/etc/pki/ca-trust/source/anchors`
   - **SUSE 11.x** - `/etc/ssl/certs`
   - **SUSE 12.x** - `/etc/pki/trust/anchors`
   - **Ubuntu 16.x, Debian 8.x** - `usr/local/share/ca-certificates`
4. Run the command `sudo chmod 644` to set the permission for the certificates.

5 Run the command specific to the platform to update the certificates:

- **CentOS 7.x, Red Hat** - `sudo update-ca-trust`
- **SUSE 11.x** - `sudo c_rehash /etc/ssl/certs`
- **SUSE 12.x** - `sudo update-ca-certificates`
- **Ubuntu 16.x, Debian 8.x** - `sudo update-ca-certificates`

6 Restart the system.

Enabling the Authentication Agent Chain

You can enable the Authentication Agent chain in the Linux Client to allow users to authenticate with the Authentication Agent on a Windows system and get seamless access to the Linux Client that does not support the external devices. To perform such authentication, users must select the **Authentication Agent** chain from the **Chains** list of Linux Client to initiate the authentication process on the Windows system where the Authentication Agent is installed.

To enable the **Authentication Agent** chain in the Linux Client, perform the following steps:

1 Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.

2 Specify `authentication_agent_enabled: true`.

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

3 Save the changes.

4 Restart the system.

Configuring the Enforced Cached Login

When the network connection is slow or unstable, the Client logon or unlock process might take several minutes. A solution to this is to enforce the cached logon. The Client connects to the Advanced Authentication server to validate the credentials in the background after the cached login. By default, the enforced cached logon is disabled and the Client will always try to connect to Advanced Authentication Server to validate the credentials.

To enforce cached login for Linux Client, perform the following steps:

1 Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.

2 Specify `forceCachedLogon: true`.

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

3 Save the changes.

4 Restart the system.

5 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 and Red Hat Enterprise Linux
- Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server
- Installing and Uninstalling Linux PAM Client on Ubuntu and Debian 9

IMPORTANT

- To use Advanced Authentication in the SSH (Secure Shell) mode, configure the following parameters in the file `/etc/ssh/sshd_config`:
  - Set `PasswordAuthentication` to no
  - Set `ChallengeResponseAuthentication` to `yes`

  To apply the changes in the file `sshd_config`, you must restart the SSH Service. To restart the SSH Service, run the command `sudo service sshd restart` in the terminal.
- Advanced Authentication secures SSH by providing multi-factor authentication only for the methods that do not require Advanced Authentication Device Service.
- Advanced Authentication does not support the multi-factor authentication to a Terminal or SSH for the domain users when Linux machine is used in a non-domain mode.

NOTE: You cannot upgrade Linux PAM Client from Advanced Authentication 5.x to 6.x. To install the latest version of Client, perform the following steps:

1. Uninstall the previous version of the Client.

   NOTE: You must run a deactivation script during the uninstallation process of the Client. For example, to uninstall the 5.x version of the Client from RHEL Workstation and Server 7, perform the following steps:

   1. Run the following command to deactivate 5.x Client on RHEL Workstation and Server 7:

      `/opt/pam_aucore/bin/deactivate.sh`
   2. Run the following command to remove the `pam_aucore` package:

      `rpm -e pam_aucore`
2. Navigate to **Advanced Authentication Administration portal > Endpoints**.
3. Search and remove the endpoint of the Linux PAM Client.
4. Install the latest version of Client.

For more information about how to install Linux Client, see Installing and Uninstalling Linux PAM Client.

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

Installing and Uninstalling Linux PAM Client on CentOS and Red Hat Enterprise Linux

To install Linux PAM Client on CentOS, RHEL Workstation, and Server 7, perform the following steps:

1. Run the following command:

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

2. Run one of the following commands:
   - Non-domain joined Linux machine
     - `sudo chmod +x /opt/pam_aucore/bin/bind-to-nondomain.sh`
     - `sudo /opt/pam_aucore/bin/bind-to-nondomain.sh`

     NOTE: Ensure to set **Event type** as **OS logon (local)** in the **Linux logon** event for the Linux machine that is not joined to a domain.
   - Domain joined Linux machine
     - `sudo chmod +x /opt/pam_aucore/bin/bind-to-ad.sh`
     - `sudo /opt/pam_aucore/bin/bind-to-ad.sh mycompany.com`

       where `mycompany.com` is your FQDN.

     NOTE: Ensure to set **Event type** as **OS Logon (domain)** in the **Linux logon** event for the Linux machine that is joined to a domain.

To uninstall Linux PAM Client on CentOS, run the following command:

```
sudo rpm -e pam_aucore
```

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

NOTE: Before installation, it is recommended to import the public key from the package using the following command:

```
rpm --import netiq-provo-build-key.public
```

This prevents the error message `Package is not signed` from being displayed if you have not imported the public key.

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

1 Run the following command:

```
rpm -ivh Suse<OS version>PAMClientInstaller-Release-<version>.rpm
```

2 Run one of the following commands:

- Non-domain joined Linux machine

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

  NOTE: Ensure to set **Event type** as **OS logon (local)** in the **Linux logon** event for the Linux machine that is not joined to a domain.

- Domain joined Linux machine

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

  where mycompany.com is your FQDN.

  NOTE: Ensure to set **Event type** as **OS Logon (domain)** in the **Linux logon** event for the Linux machine that is joined to a domain.

WARNING: Ensure that the event name in the configuration file `aucore.conf` corresponds to the appropriate event name configured in the Administration portal. Do not change the default domain name in the `aucore.conf` file.

To uninstall Linux PAM Client on SUSE Linux Enterprise Desktop and server, run the following command:

```
sudo rpm -evh pam_aucore
```

Installing and Uninstalling Linux PAM Client on Ubuntu and Debian 9

NOTE: Before installing Linux PAM Client on Ubuntu, ensure to configure `lightdm`. For more information, see Preinstalling the Configuration on Ubuntu 16.

To install Linux PAM Client on Ubuntu and Debian 9, perform the following steps:

1 Run the following command:

```
sudo dpkg -i naaf-linuxpamclient-debian-release-<version>.deb
```

2 Run one of the following commands:

- Non-domain joined Linux machine

  ```
  sudo chmod +x /opt/pam_aucore/bin/activate-nondomain.sh
  sudo /opt/pam_aucore/bin/activate-nondomain.sh
  ```

  NOTE: Ensure to set **Event type** as **OS logon (local)** in the **Linux logon** event for the Linux machine that is not joined to a domain.

- Domain joined Linux machine

  ```
  sudo chmod +x /opt/pam_aucore/bin/activate.sh
  sudo /opt/pam_aucore/bin/activate.sh mycompany.com
  ```

  where mycompany.com is your FQDN.

NOTE: Ensure to set **Event type** as **OS Logon (domain)** in the **Linux logon** event for the Linux machine that is joined to a domain.

To uninstall Linux PAM Client on Ubuntu and Debian 9, run the following command:

```
sudo dpkg --purge pam_aucore
```

6 Troubleshooting

This chapter contains the following sections:

- "Endpoint Not Found" on page 31
- "Endpoint Already Exists" on page 31
- "Users Are Unable to Log In with a Domain Account After Booting" on page 31
- "Domain Users Are Unable to Log In Even After Authenticating All the Methods In a Chain" on page 32

To enable logs for Linux Client, see Enabling Logs on Linux Client.

Endpoint Not Found

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

Reason: This issue occurs when an endpoint of the Client does not exist in the Administration portal.

Workaround:

1. Boot the system in Safe mode and remove the parameters `endpoint_id` and `endpoint_secret` from the `pam_aucore.conf` file located in the path `/opt/pam_aucore/etc/`.
2. Reboot the system.

Endpoint Already Exists

Issue: If a Linux Client has lost the Endpoint ID and Secret and tries to register an endpoint for the Client again in the Advanced Authentication server, an error message `Endpoint already exists?` is displayed.

Reason: This issue occurs when an endpoint of the Client is already registered in the Administration portal.

Workaround: Remove the existing endpoint entry of the Client from the **Endpoints** section of the Administration portal.

Users Are Unable to Log In with a Domain Account After Booting

Issue: After booting the Linux Client, an error message `Only local user can logon` is displayed.

Reason: This issue is due to the less start-up timeout value set to the Client service.

Workaround: To increase the timeout, perform the following steps:

1. Run the following command to edit the configuration file:

   ```
   sudo vi /opt/pam_aucore/etc/pam_aucore.conf
   ```

2. Specify `pam.serviceStartupTimeout=X`. `X` is timeout value in seconds. The default timeout value is set to 10.

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

3. Save the changes.

Domain Users Are Unable to Log In Even After Authenticating All the Methods In a Chain

Issue: When an Active Directory user logs in to the SUSE Linux PAM Client and passes all the authentication methods in the chain, authentication fails and an error message `Sorry that didn't work` is displayed.

Workaround:

1. After joining the SLES 12 Service Pack 3 to the windows domain, navigate to Yast and search for the **Windows Domain Membership**.
2. Select the following in the **Windows Domain Membership** window:
   - Use SMB Information for Linux Authentication
   - Create Home Directory on Login
   - Offline Authentication
3. Click **NTP configuration** in the lower part of the window.
4. Select **Now and on Boot** in the **Advanced NTP Configuration** > **General Settings** tab.
5. Click **Add**.
6. Select the **Type** as **Server** from the **New Synchronization** window and click **Next**.
7. Specify the host or IP address of the NTP server in **Address**.
8. Click **Test** to test the server settings.
9. Click **OK** to apply the Windows Domain Membership settings.

   A list of packages are displayed.
10. Ensure to install all the packages that are prompted in the list.
11. Reboot your system.