Advanced Authentication 6.4

Linux PAM Client Installation Guide

July 2022

Legal Notices

Contents

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.

1 System Requirements

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

For system requirements of Linux PAM Client, see Linux PAM Client.

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**

  NOTE: The Bluetooth method is not available from the Advanced Authentication 6.4 Service Pack 1 release.

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

NOTE: 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.

4 Configuring the Preliminary Settings

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

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 `config.properties` 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 `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.

You can specify multiple Advanced Authentication servers separated by a semicolon (;):

```
discovery.hosts: aaf-1.domain.com;aaf-2.domain.com;....;aaf-n.domain.com
```

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 14
- “Adding an SRV Record” on page 15
- “Configuring Authentication Server Discovery in Client” on page 17

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.

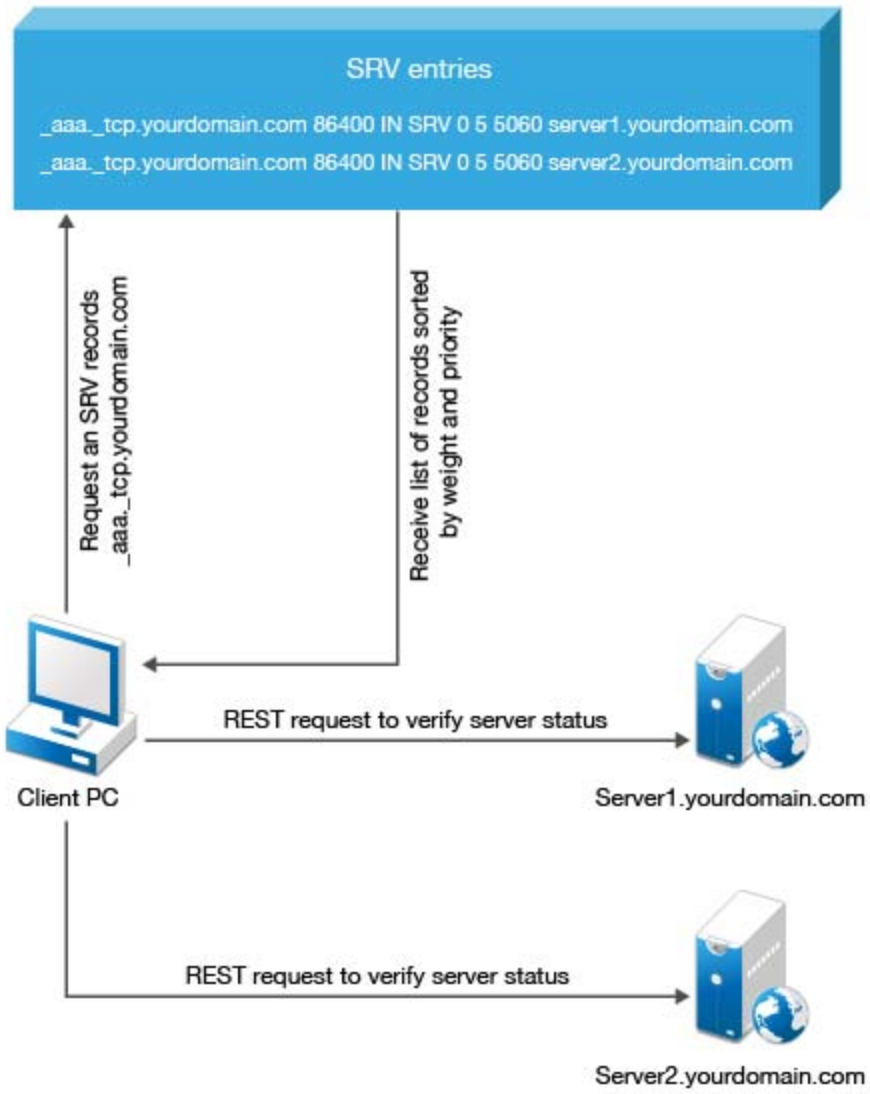
DNS Server Entries

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 `config.properties` file:

Parameter	Description
`discovery.Domain`	DNS name of the domain.
`discovery.host`	Option to specify the DNS name or the IP address of an Advanced Authentication server.
`discovery.port`	Option to specify the port number for the client-server interaction.
`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).

Parameter	Description
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.
less_verbose_services	To hide the verbose services in the PAM Client. For more information, see Configuring Less Verbose Services.
default_repo	To configure a repository as default in Linux Client for authentication. For more information, see Configuring a Default Repository on Linux PAM Client.
enableLinkedChainsOffline:false	To disable linked chains for offline login. For more information, see Disabling Linked Chains for Offline Login.
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.

Setting	Description
locale:xx	To change the client locale to a language other than the operating system's default language. For more information, see Changing the Locale of Linux PAM Client without Changing the Locale of the Operating System.
disable_local_accounts: true	To disable local accounts for the non-domain mode. For more information, see Disabling the Local Accounts.
tlsVersion: value	To configure the TLS version that the network library of the Linux PAM Client uses for establishing HTTPS connection with the Advanced Authentication server. For more information, see Configuring the TLS Version.

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

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

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 domain joined workstations, you can create a custom event with the type as Generic for the nondomain 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/`.

Enabling the Profiling Tool

You can configure the Linux PAM 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. Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.
2. Specify `rest_profiling: true (default value is false)`.

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

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

NOTE: The `authentication_agent_enabled` parameter is not required from Advanced Authentication 6.4.

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.

When you set the `forceCachedLogon` parameter to `true`. Following are different behavior of the Cache Service in Linux PAM Client:

- 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:
  - **Advanced Authentication server is available**

    A user cannot log in during the first attempt. During the subsequent login, after selecting a chain and before providing credentials, an error message that states one of the following based on the account status:
    - The user account is locked
    - The user account is expired
    - The user account is disabled
  - **Advanced Authentication server is unavailable**

    A user cannot log in during the first attempt. During the subsequent login, an error message that states unable to find the server is displayed.
- 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 Less Verbose Services

Sometimes, multiple messages that are repeated are displayed when you are log in to SSH. For example, multiple `Please wait` messages or `Enter password` messages are displayed. You can hide these verbose messages in the PAM Client by including the `less_verbose_services` parameter in the configuration file `pam_aucore.conf`. The setting supports PAM services names list or a single service name.

For example, you can disable messages that are displayed multiple times for a gnome-screensaver service on SUSE 12 by adding `less_verbose_services = gnome-screensaver` in the `/opt/pam_aucore/etc/pam_aucore.conf` file.

You can also include multiple names in the list. This list must be divided with semicolons (;) or commas (,).

NOTE: By default, the services `sshd`, `sudo`, `su`, `lightdm`, `unity`, `gnome-screensaver` are included in this list.

Configuring a Default Repository on Linux PAM Client

In multiple repositories environment, you can configure a repository as default in the Linux PAM Client irrespective of the order of repositories configured in the **Login Options** policy on the Administration portal. With a default repository, users can log in to the Linux Client without prefixing the repository name before the user name. However, the Linux Client prefixes the defined default repository with the user details in the background for validating the credentials and authenticating the user.

For example, a company has three repositories in the following order:

1. repoX

2. repoY
3. repoZ

An administrator wants to configure the repoZ as default repository on the Linux Client for authentication. Using the `default_repo` parameter, the administrator can configure a default repository in the Linux Client.

To configure a repository as default on Linux Client, perform the following steps:

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

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

2 Specify `default_repo: <NameOfRepository>`.

3 Save the changes.

4 Restart the system.

Disabling Linked Chains for Offline Login

With a linked chain, users can authenticate to the Linux 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 login with the linked chain.

To disable linked chains for offline login, perform the following steps:

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

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

2 Specify `enableLinkedChainsOffline:false`. The default value is true.

3 Save the changes.

4 Restart the 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 `/opt/pam_aucore/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 `linux_pam.pot` files, and paste it in `/opt/pam_aucore/locale/<language>\LC_MESSAGES`.
5. Open the `aaacachesrv.pot`, `aucore.pot` and `linux_pam.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 `linux_pam.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.
10. Restart the operating system.

Changing the Locale of Linux PAM Client without Changing the Locale of the Operating System

This option allows you to change the locale of Linux PAM Client without changing the locale of the operating system.

For example, if the default language of your operating system is English, you can configure Linux PAM Client to display the messages and warnings in German.

To change the locale, perform the following steps:

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

   `locale: ISO code of the preferred language.`

   NOTE: While changing the locale, keep the following points in mind:

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

     For example, if the ISO code is `fr.ca`, then the value should be `fr_ca`.

   NOTE: By default, no value is specified. If no parameter is specified in the configuration file, operating system's default locale will be picked.
3. Save the `pam_aucore.conf` file.
4. Restart the operating system.

Configuring the TLS Version

You can configure the TLS version that the network library of the Linux PAM Client uses for establishing HTTPS connection with the Advanced Authentication server. The default version is TLSv1.3.

To configure the TLS version, perform the following steps:

1. Navigate to `/opt/pam_aucore/etc/` and open the `pam_aucore.conf` file.
2. Specify `tlsVersion: value.` The values are defined as follows:
   - TLSv1.3: Default and strongly recommended value.
   - TLSv1.2

     NOTE: If the Linux PAM Client is connected to Advanced Authentication as a Service, then it is recommended to set the TLSv1.2 value for the `tlsVersion` parameter.
   - 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 TLSv1.3 is set automatically.

3 Save the changes.

4 Restart the system.

Configuring in Case of Advanced Authentication as a Service

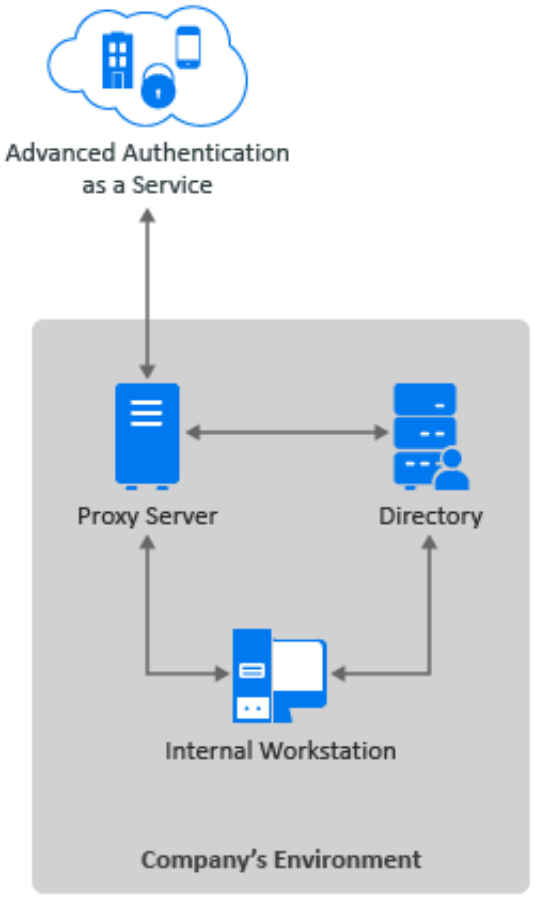
The following table describes the parameters to configure Linux PAM Client in case of Advanced Authentication as a Service.

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 configure the Linux PAM Client to work with Advanced Authentication Servers via HTTP Proxy, see Configuring to Connect Via HTTP Proxy.

Configuring to Connect Via HTTP Proxy

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



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

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 changes.

4 Restart the system

Disabling the Local Accounts

To ensure security, the Linux PAM client allows you to disable local accounts in non-domain mode.

Perform the following steps to disable local accounts:

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

   ```
   disable_local_accounts: true
   ```
3. Save the `pam_aucore.conf` file.
4. Restart the operating system.

If the local accounts for non-domain mode are not disabled, it is possible to unlock the operating system and change the password using a local account with password authentication (one factor). This may result in security issues.

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, Debian 9 and Debian 10
- Installing and Uninstalling Linux PAM Client on AIX Server

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.

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, Debian 9 and Debian 10

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, Debian 9, and Debian 10 perform the following steps:

NOTE: Before installing Linux PAM Client on Debian 10, switch to root account. Run the following command to switch to root account:

```
su -l
```

Set the root path and edit `/root/.bashrc` with the root privileges to add the following line:

```
export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

Run all commands to install Linux PAM Client without the prefix `sudo`.

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
```

To uninstall Linux PAM Client on Debian 10, run the following command without the prefix sudo:

```
dpkg --purge pam_aucore
```

Installing and Uninstalling Linux PAM Client on AIX Server

Before installing the Linux PAM Client, AIX machine must be configured to use LDAP based user accounts and user groups from an Active Directory.

Prerequisite:

It is required to define `/bin/false` as a shell on AIX machine. Navigate to `/etc/security/login.cfg` and add `/bin/false` under `shells` attribute.

To install Linux PAM Client on the AIX server:

1. Run the following command:

   ```
   rpm -ivh naaf-aixclient-aix-release-<version>.rpm
   ```

2. To enable the Linux PAM Client, perform the following:

   2a Edit the `/opt/pam_aucore/etc/pam_aucore.conf` and add `discovery.host: <AA Server ip/DNS>`

   2b Execute the following commands to restart the Cache service:

   ```
   stopsrc -s aaacache
   startsrc -s aaacache
   ```

   2c Edit the `/etc/pam.conf` file

   Comment existing `sshd` under Authentication section and add the following line to use Advanced Authentication `pam_aucore`:

   ```
   sshd auth required /opt/pam_aucore/lib/pam_aucore.so
   ```

   NOTE: Do not modify `sshd` under Account Management, Password Management, and Session Management. Retain the default settings of pam_aix.

   For more information, see Enable ssh on AIX (https://www.ibm.com/support/pages/enable-ssh-aix-use-pam).

   2d Edit `/etc/ssh/sshd_config` and add the following parameters:

   ```
   ChallengeResponseAuthentication yes
   ```

```
UsePAM yes
```

NOTE: If the parameter UsePAM is existing and set to no then modify the value to yes.

2e Edit `/etc/security/login.cfg` and set `auth_type = PAM_AUTH` instead of STD_AUTH.

2f Execute the following commands to restart sshd:

```
stopsrc -s sshd
startsrc -s sshd
```

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

```
rpm -e pam_aucore
```

NOTE: After you uninstall the Linux PAM Client, it is required to revert the changes that have been made to the following files:

- `/etc/pam.conf`
- `/etc/ssh/sshd_config`
- `/etc/security/login.cfg`

6 Troubleshooting

This chapter contains the following sections:

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.

Error While Logging with the Linux Client

Issue: After the first login to the Linux Client, when a domain or local user tries to log in again, the following error message is displayed:

```
Cannot add or change the endpoint (same name or software_name already exist?
```

Also, the deleted endpoint details exist on the Administration portal.

Reason: This issue might occur if the endpoint information is not saved in the `config.properties` file of the Linux Client.

Workaround: Before installing the Linux Client, disable the selinux. To disable selinux, perform the following steps:

1. Open `/etc/selinux/config.properties`
2. Specify `SELINUX=disabled`
3. Reboot your system.
4. Run the following command to verify the status of selinux:

   ```
   sestatus
   ```

Not Able to Login Without Repository Name

Issue: If the user tries to log in without specifying the repository name before the username, a `Sorry, it didn't work` message is displayed and login fails.

Workaround: Perform the following steps to resolve the issue:

1. Open `/etc/sssd/sssd.conf`.
2. Set `use_fully_qualified_names` parameter to `False`.
3. Reboot your system.