Installation Guide

Advanced Authentication - Linux PAM Client

Version 6.0

NetIQ

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Contents

About NetIQ Corporation

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

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

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

Enabling critical business services, better and faster

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

Our Philosophy

Selling intelligent solutions, not just software

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

Driving your success is our passion

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

Our Solutions

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

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, contact our Technical Support team.

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

Contacting Documentation Support

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

Contacting the Online User Community

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

About this Book

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: 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 Terminal and SSH by providing multi-factor authentication for only the methods that do not require Advanced Authentication Device Service. The Smartphone method is supported in out-of-band (online) mode. Advanced Authentication does not support the multi-factor authentication for a Terminal or SSH for the domain users when Linux machine is used in a non-domain mode.

---

1 System Requirements

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

The following system requirements must be met:

- Ensure that anyone of the following operating system is installed.
  - CentOS 7 with KDE or Gnome desktop environment
  - SUSE Linux Enterprise Desktop 12 Service Pack3
  - SUSE Linux Enterprise Server 11 Service Pack4
  - SUSE Linux Enterprise Server 12 Service Pack2 and Service Pack3
  - Red Hat Enterprise Linux Client 7.4
  - Red Hat Enterprise Linux Server 7.4
  - Debian 9.4
  - Ubuntu 16, 18
- 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

2 Configuration

This chapter contains the following information:

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 **_aav6.**

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 **_aav6**.

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 Step 2 to Step 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. You must add the parameters in the `config.properties` file.

- `discovery.Domain`: DNS name of the domain. For 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 Mac OS X 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`: 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 Windows and Linux Clients and `True` for Mac Client.
- `discovery.wakeupTimeout`: Timeout after the system starts or resumes from sleep. The default value is 10 seconds.

Authentication Server Discovery Flow

Windows Client

The feature is not supported in Windows Client.

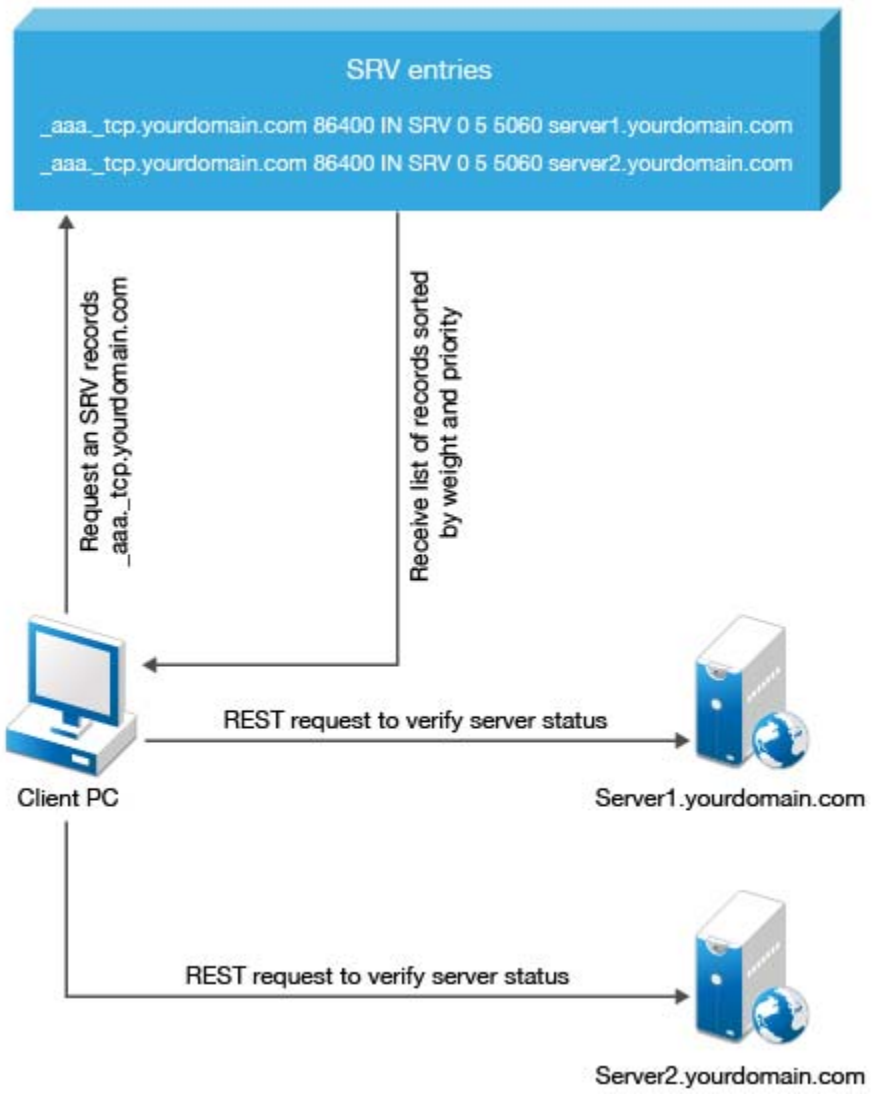
MacOS Client/ Linux PAM Module

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.



Preparing Linux for Installing Linux PAM Client

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`.

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>`.

The Advanced Authentication server receives the client connections through the port 443 by default. However, if the port redirection is configured on the network between the client and server then you can customize the port number manually. In the `config.properties` file of the client, you must use `discovery.port` parameter to enable the client to discover and pair with the Advanced Authentication server.

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.

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.`

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`

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 timeout period, the `Hardware timeout` message is shown and then the card waiting dialog is closed and user login selection screen is displayed.

By default the card timeout is 60 seconds.

To configure the timeout for card waiting, 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. Enter `card.timeout: X` in the config.properties file. X is the timeout value in seconds.
3. Save the configuration file.
4. Restart the operating system.

Preinstalling Configuration on Ubuntu 16

Before installing the Linux PAM client on Ubuntu 16, you must complete the preinstallation process to configure `lightdm` to accomplish 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**.

Enabling Logs on Linux Client

You can enable logs for Linux Client to enable viewing the logs for debugging.

To generate logs for Linux Client, perform the following steps:

1. Run the following command:

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

2. Add `logEnabled=true` to the configuration file. If the configuration file does not exist, you must create it.

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

Configuration for Verification of Server Certificates

You can secure the connection between a workstation and Advanced Authentication servers with a valid SSL certificate, thus preventing any attacks on the connection and ensuring 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 all Linux platforms, perform the following steps:

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

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

   If the certificates are not available in `/opt/pam_aucore/certs`, PAM module searches 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.

Using OS Specific Certificate Paths

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

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

   If the configuration file does not exist, create a new file.
3. Place the trusted certificates in the OS specific path of 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 permission for 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`

Configuration to Enable the Authentication Agent Chain

The Authentication Agent allows you to authenticate on one computer where all the devices required for authentication are connected to get authorized access to another computer or z/OS mainframe, where one of the following condition is true:

- It is not possible to redirect the authentication devices.
- It does not support devices that are used for authentication.

The Authentication Agent can be installed only on the Windows computer.

You must select **Authentication Agent** in the Chains list of Linux Client to initiate the authentication process on Windows computer 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 `pam_aucore.conf` file.
2. Specify `authentication_agent_enabled = true` in the configuration file.

   If the configuration file does not exist, you must create it.
3. Click **Save**.
4. Restart your computer.

An Example Scenario of Using the Authentication Agent

This scenario describes how you can perform authentication on Windows computer and auto-sign in to Linux computer using the Authentication Agent.

Mark uses the SSH to access Linux computer. But, the devices required for authentication such as FIDO U2F token and card reader are not supported in SSH. He cannot get authenticated to Linux computer because it is not possible to redirect the authentication devices. In this case, Mark can use Authentication Agent to perform authentication on Windows computer and get seamless access to Linux computer.

Consider the following setup:

- Windows computer is installed with the Authentication Agent and is connected with the devices used for authentication such as FIDO U2F token and card reader.
- Linux computer is where the Authentication Agent chain is enabled using the `config.properties` file and is not connected with the authentication devices.

The following sequence describes the authentication process using the Authentication Agent:

1. Specify **user name** and the chain number corresponding to the Authentication Agent chain in Linux computer.
2. The Authentication Agent on Windows computer launches a restricted browser.
3. Select the preferred chain to log in to Linux computer in the restricted browser.
4. Perform the authentication using the FIDO U2F token and card reader in the restricted browser.

   Mark is logged in to Linux computer automatically.

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
- 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: If you want to use Advanced Authentication in the SSH (Secure Shell), configure the following parameters in the file `/etc/ssh/sshd_config`:

- `PasswordAuthentication no`
- `ChallengeResponseAuthentication 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 6.0. To install the latest client, you must do the following:

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 5.4 version of the client perform the following steps:

   1. Deactivate 5.4 client with the following command:

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

   2. Remove the `pam_aucore` package:

      ```
      rpm -e pam_aucore
      ```

2. Open the **Advanced Authentication Administration portal > Endpoints**.
3. Find and remove the endpoint for the Linux PAM Client instance.
4. Install the new client.

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

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

Installing and Uninstalling Linux PAM Client on CentOS, Red Hat Enterprise Linux Client and Server 7

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

1. Run the following command:

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

2. Run the following configuration scripts:
   - If Linux machine is not bound to a domain, ensure that you select **OS logon (local)** type as the **Linux logon** event:

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

   - If your Linux workstation is bound to a domain, ensure that you select **OS Logon (domain)** as the **Event type**:

     ```
     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.

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

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 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 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 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 the following command:

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

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

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

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

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

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

   where mycompany.com is your FQDN.

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

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

4 Troubleshooting

To investigate the possible issues, analyze the debug logs.

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

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

The logs are also recorded in the files:

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

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.