
Installation Guide

Advanced Authentication - Linux PAM Client

Version 6.1

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/>.

Copyright © 2018 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About NetIQ Corporation	5
About this Book	7
1 System Requirements	9
2 Configuring the Preliminary Settings	11
Configuring the Mandatory Settings	11
Setting a DNS for Server Discovery	11
Configuring a Specific Advanced Authentication Server	14
Preparing Linux for Installing Linux PAM Client	15
Preinstalling Configuration on Ubuntu 16	15
Configuring Optional Settings	15
Configuration Settings for Multitenancy	16
Selecting an Event	17
Configuring Timeout for Card Waiting	17
Enabling Logs on Linux Client	17
Configuring Verification of Server Certificates	18
Enabling the Authentication Agent Chain	19
Configuring the Enforced Cached Logon	19
Emulating ppc64le Hardware	20
3 Installing and Uninstalling Linux PAM Client	21
Installing and Uninstalling Linux PAM Client on CentOS, Red Hat Enterprise Linux	21
Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server	22
Installing and Uninstalling Linux PAM Client on Ubuntu and Debian 9	23
4 Troubleshooting	25
Endpoint Not Found	25
Issue While Unlocking the Screen	25
Users Unable to Log In with a Domain Account After Booting	26
Domain Users Unable to Log In Even After Authenticating All the Methods In a Chain	26

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: Bluetooth, 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.

Ensure that the following requirements are met:

- ♦ One of the following operating system is installed:
 - ♦ 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
 - ♦ Red Hat Enterprise Linux Server 7.5
 - ♦ Debian 9.5
 - ♦ Ubuntu 16, 18
- ♦ Gnome Display Manager (GDM) is set as the login manager
- ♦ DNS is configured for Advanced Authentication Server discovery (for more information, see [Setting a DNS for Server Discovery](#)) or a specific Advanced Authentication server must be specified in the Client configuration file (for more information, see [Configuring a Specific Advanced Authentication Server](#))

2 Configuring the Preliminary Settings

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

- ♦ [“Configuring the Mandatory Settings” on page 11](#)
- ♦ [“Configuring Optional Settings” on page 15](#)

Configuring the Mandatory Settings

- ♦ To setup a connection between Linux Client and the Advanced Authentication server, perform one of the following:
 - ♦ To make Linux Client communicate with the Advanced Authentication servers through DNS, see [“Setting a DNS for Server Discovery”](#).
 - Or
 - ♦ To manually specify a custom Advanced Authentication server, see [“Configuring a Specific Advanced Authentication Server”](#).
- ♦ 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 Configuration on Ubuntu 16”](#).

Setting a DNS for Server Discovery

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

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

- ♦ [“Adding a Host in DNS” on page 11](#)
- ♦ [“Adding a SRV Record” on page 12](#)
- ♦ [“Configuring Authentication Server Discovery in Client” on page 13](#)
- ♦ [“Authentication Server Discover Flow” on page 14](#)

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 then click **New Host (A or AAAA)** under **Forward Lookup Zone** in the console tree.
 - 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 using the details that you have provided in **Name** and **IP address**.

Adding a SRV Record

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

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

To add a SRV record for the Advanced Authentication servers in the primary Advanced Authentication site (a site with Global Master server), perform the following steps:

- 1 Right-click on a node with 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** then 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**.

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

- 1 Expand the preferred domain name node then select `_sites` in the **Forward Lookup Zones** of the console tree.
- 2 Right-click on the preferred site name then click **Other New Records**.
- 3 Select **Service Location (SRV)** from **Select a resource record type** then 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 that is added in **Host offering this service**.
For example, `authsrv.mycompany.com`.
- 8 Click **OK**.

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

The DNS server contains the following elements:

Element	Description
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 hostname of the machine providing the service. It ends with a dot.

Configuring Authentication Server Discovery in Client

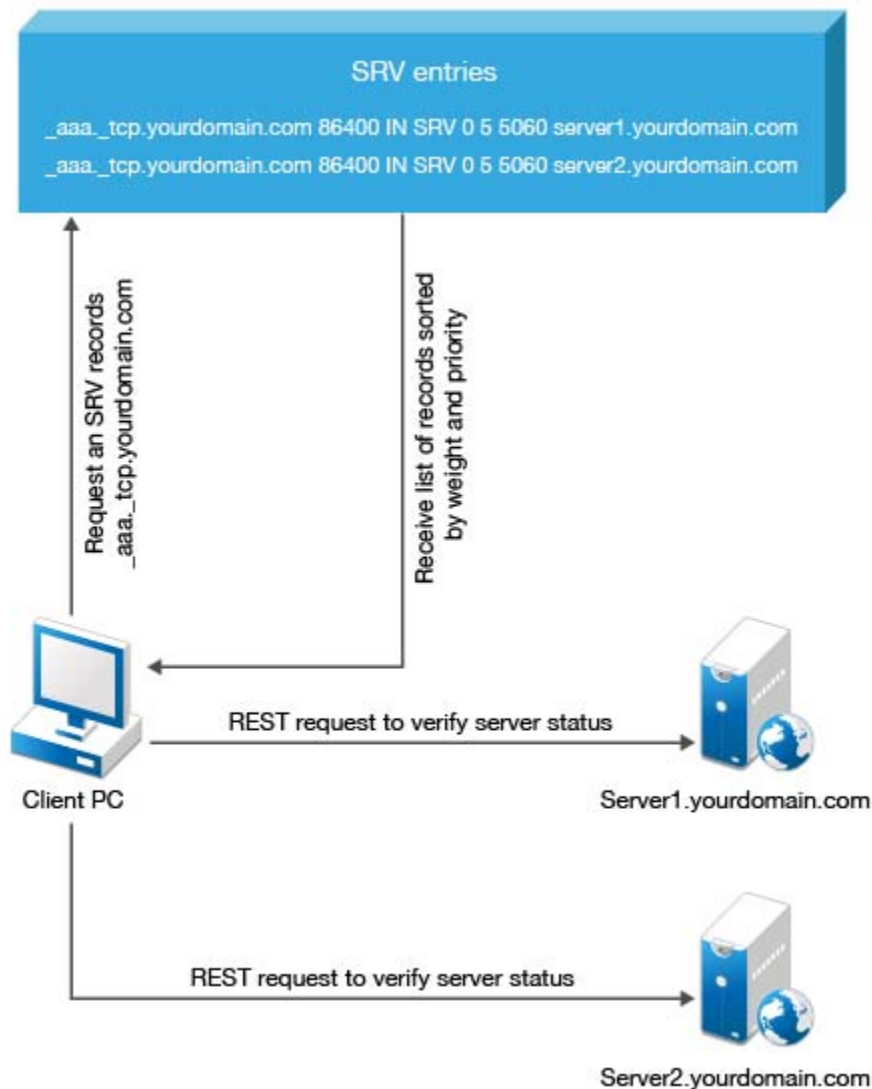
You can configure server discovery in Linux Client by using the following parameters in the `config.properties` file:

Parameter	Description
<code>discovery.Domain</code>	DNS name of the domain. For Windows Client, this value is used if workstation is not connected to the domain.
<code>discovery.subDomains</code>	To list additional sub domains separated by a semicolon. You can also use the parameter on Mac OS X Client to list the AD sites.
<code>discovery.useOwnSite</code>	Set the value to <code>True</code> to use the local site (Windows Client only).
<code>discovery.dnsTimeout</code>	Set time out for the DNS queries. The default value is 3 seconds by default.
<code>discovery.connectTimeout</code>	Time out for the Advanced Authentication server response. The default value is 2 seconds.
<code>discovery.resolveAddr</code>	Set the value to <code>False</code> to skip resolving the DNS. By default the value is set to <code>False</code> for Linux Client.
<code>discovery.wakeupTimeout</code>	Timeout after the system starts or resumes from sleep. The default value is 10 seconds.

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

Authentication Server Discover Flow

The following diagram illustrates the server discovery workflow.



Configuring a Specific Advanced Authentication Server

You can configure a specific Advanced Authentication server on a workstation that is used when the workstation is not joined to a domain. You can also use this option to enforce a connection to a specific Advanced Authentication server when a workstation with Linux Client is joined to a domain.

To configure a Advanced Authentication server in Linux Client, 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.

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

NOTE: To use Linux Client in non-domain joined workstations, set **Event type** as **OS Logon (local)** for the **Linux logon** event in the Administration console.

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 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**.

Configuring Optional Settings

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

Setting	Description
tenant_name	To point Linux Client to a specific tenant. For more information, see Configuration Settings for Multitenancy .
event_name: <CustomEventName>	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 .

Setting	Description
<code>card.timeout: X</code>	To configure the time for which the card waiting dialog is displayed, when the user authenticates using the card method. For more information, see Configuring Timeout for Card Waiting .
<code>logEnabled</code>	To view the logs of Linux Client for debugging. For more information, see Enabling Logs on Linux Client .
<code>verifyServerCertificate</code>	To configure the verification of server certificates for LDAP connection. For more information, see Configuring Verification of Server Certificates .
<code>authentication_agent_enabled</code>	To enable the Authentication Agent chain in Linux Client. For more information, see Enabling the Authentication Agent Chain .
<code>forceCachedLogon</code>	To enforce the cached logon to Linux Client. For more information, see Configuring the Enforced Cached Logon .

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

Configuration Settings for Multitenancy

If the Multi-tenancy feature is enabled in the Administration console, you can configure a specific tenant name to Linux Client.

To configure specific tenant name, perform the following steps:

1. Navigate to `/opt/pam_aucore/etc/` and open `pam_aucore.conf` file.
2. Specify `tenant_name: <name of tenant>`
For example, `tenant_name: TOP` for the TOP tenant.
If the 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

New endpoint gets mapped to the tenant name that has a name similar to the domain name in the Multitenancy mode by default. You can also add an endpoint to a preferred tenant that is not named 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

You can log in to Linux Client using the Linux login event, by default. However, you can also create a custom event when required and map the event to a specific workstation.

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.

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

1. Navigate to `/opt/pam_aucore/etc/` and open `pam_aucore.conf` file.
2. Specify `event_name: <CustomEventName>`
If the file does not exist, create a new file.
3. Save the changes.
4. Restart the system.

Configuring Timeout for Card Waiting

When using Card method for authenticating to Linux Client, you can configure the time duration till when the card waiting dialog is displayed to the user to authenticate. If the user does not present the card before the timeout period, a message `Hardware timeout` is displayed and the card waiting dialog is closed then the user is prompted with the authentication methods list for login.

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

1. Navigate to `/opt/pam_aucore/etc/` and open `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 file does not exist, create a new file.
3. Save the changes.
4. Restart the system.

Enabling Logs on Linux Client

You can enable logs for Linux Client to view 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. Specify `logEnabled:true` to the configuration file.
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 `/opt/pam_aucore/var/log/pam_aucore` folder.

Configuring 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`.
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.
- 5 Restart the system.

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`.
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`
 - 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 **Authentication Agent** chain from the **Chains** list of Linux Client to initiate the authentication process on Windows system where the Authentication Agent is installed.

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

Configuring the Enforced Cached Logon

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. In this case the Client will connect to Advanced Authentication Server to validate the credentials in background after the cached logon. By default, the enforced cached logon is disabled and the Client will always try to connect to Advanced Authentication Server to validate credentials.

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

1. Navigate to /opt/pam_aucore/etc/ and open `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.

Emulating ppc64le Hardware

Installing Linux PAM client on ppc64le requires a third part installer. The following sections contain the information to install Linux PAM client on ppc64le.

Emulating ppc64le on Microsoft Windows

Perform the following steps to install Linux PAM client on Windows running on ppc64le:

- 1 Go to [QEMU Binaries for Windows \(64 bit\) \(https://qemu.weilnetz.de/w64/\)](https://qemu.weilnetz.de/w64/) to download and install the latest QEMU version for Windows.
- 2 Download an ISO that supports PPC. In this configuration OpenSuse is used as an example.
Go to [OpenSuse Index \(http://mirror.linux-ia64.org/opensuse/ports/ppc/distribution/leap/\)](http://mirror.linux-ia64.org/opensuse/ports/ppc/distribution/leap/) to download OpenSuse ISO.
- 3 Perform the following steps to install OpenSuse on QEMU.
 - 3a Run the following command to create a hard disk:

```
qemu-img create -f qcow2 PATH_TO_IMAGE/opensuse.qcow 20G
```
 - 3b Run the following command to install and configure the operating system:
 1. `qemu-system-ppc64 -hda image/opensuse.qcow -boot d -cdrom iso/openSUSE-Leap-42.3-NET-ppc64le-Build0130-Media.iso -m 4G -net nic -net user`
 2. `qemu-system-ppc64 -hda image/opensuse.qcow -m 8G -net nic -net user`
- 4 See [“Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server” on page 22](#) to install the Linux PAM client on OpenSuse.

Emulating ppc64le on Linux

Perform the following steps to install Linux PAM client on Linux running on ppc64le:

- 1 Go to [QEMU for Virtualization \(https://software.opensuse.org/download.html?project=Virtualization&package=qemu\)](https://software.opensuse.org/download.html?project=Virtualization&package=qemu) and click **SLE** to download and install SLE. In this configuration SLE12 is used as an example.
- 2 Run the following as root:
 1. `zypper addrepo https://download.opensuse.org/repositories/Virtualization/SLE_12/Virtualization.repo`
 2. `zypper refresh`
 3. `zypper install qemu qemu-ppc`
- 3 Perform the following steps to install OpenSuse on QEMU.
 - 3a Run the following command to create a hard disk:

```
qemu-img create -f qcow2 PATH_TO_IMAGE/opensuse.qcow 20G
```
 - 3b Run the following command to install and configure the operating system:
 1. `qemu-system-ppc64 -hda image/opensuse.qcow -boot d -cdrom iso/openSUSE-Leap-42.3-NET-ppc64le-Build0130-Media.iso -m 4G -net nic -net user`
 2. `qemu-system-ppc64 -hda image/opensuse.qcow -m 8G -net nic -net user`
- 4 See [“Installing and Uninstalling Linux PAM Client on SUSE Linux Enterprise Desktop and Server” on page 22](#) to install the Linux PAM client on OpenSuse.

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](#)
- ♦ [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

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 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

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 an error message `Package is not signed` that you may get 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 the following command:

If the 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
```

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.

If the 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, you can enable logs for Linux Client. For more information, see [“Enabling Logs on Linux Client”](#).

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

The logs are also recorded in the following files:

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

This chapter contains the following sections:

- ♦ [“Endpoint Not Found” on page 25](#)
- ♦ [“Issue While Unlocking the Screen” on page 25](#)
- ♦ [“Users Unable to Log In with a Domain Account After Booting” on page 26](#)
- ♦ [“Domain Users Unable to Log In Even After Authenticating All the Methods In a Chain” on page 26](#)

Endpoint Not Found

Issue: After you install the Linux Client and reboot the system, an error message `Endpoint not found` error is displayed and you are unable to log in to the Client.

Reason: This issue occurs when an endpoint for the Client already exists either in the server or in the configuration file of the Client.

Workaround: Perform the following steps:

1. Remove the endpoint for the Client from the **Endpoints** section of the Administration Portal (if it exists).
2. Boot the system in Safe mode and remove `endpoint_id`, `endpoint_name` and `endpoint_secret` parameters from the `pam_aucore.conf` file located in the `/opt/pam_aucore/etc/` path.
3. Reboot the system.

Issue While Unlocking the Screen

Issue: When a user tries to unlock the screen on Linux Client by specifying the password and a message `Please wait` is displayed, the screen stops responding. This issue happens on SLES 12 Service Pack 1.

Workaround: Upgrade SLES 12 to Service Pack 2 or later version.

Users Unable to Log In with a Domain Account After Booting

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

Reason: This issue is due to the less startup timeout value set to the Client service.

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

- 1 Run the following command:

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

- 2 Add `pam.serviceStartupTimeout=X`, to the configuration file, where X is timeout value in seconds. The default value is set to 10.

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

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

Issue: When an AD user logs into the SUSE Linux PAM client, pass all the authentication methods in the chain, authentication fails and an error message `Sorry that didn't work` is displayed.

Workaround: Perform the following steps:

- 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** lower bottom of the window.
- 4 Select **Now and on Boot** from 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.