Advanced Authentication 6.4

Mac OS X Client Installation Guide

July 2022

Legal Notices

Contents

About this Book 5

1 System Requirements 7

2 Offline Support for Mac OS X Client 9

3 Configuring the Preliminary Settings 11

Configuring the Mandatory Settings . . . 11
Setting-up a DNS for Advanced Authentication Server Discovery . . . 11
Using a Specific Advanced Authentication Server in the Non-DNS Mode . . . 15
Enabling Remote Login . . . 16
Configuring the Optional Settings . . . 16
Disabling 1:N . . . 17
Configuration Settings for Multitenancy . . . 18
Customizing a Logo . . . 18
Configuring Time-Out for Card Waiting . . . 18
Configuring Time-Out for the U2F Authentication . . . 19
Selecting an Event . . . 19
Configuring to Verify Server Certificates . . . 20
Enabling the Authentication Agent Chain . . . 20
Configuring the Enforced Cached Logon . . . 21
Binding Mac to Active Directory . . . 21
Enabling the Offline Mode . . . 22
Displaying Other User on the Login Screen in Non-Domain Mode . . . 23
Creating a Mobile Account for the Offline Mode . . . 23
Displaying the Authentication Window on Unlock Screen . . . 23
Disabling Linked Chains for Offline Login . . . 24
Enabling the Profiling Tool . . . 24
Localizing the Messages for Clients . . . 25
Changing the Locale of Mac OS Client without Changing the Locale of the Operating System . . . 26
Configuring the TLS Version . . . 26
Configuring in Case of Advanced Authentication as a Service . . . 27
Configuring to Connect Via HTTP Proxy . . . 27
Disabling the Local Accounts . . . 29

4 Installing and Uninstalling Mac OS X Client 31

Installing Mac OS X Client . . . 31
Uninstalling Mac OS X Client . . . 31
Uninstalling Mac OS Client with dmg File . . . 32
Uninstalling Mac OS Client without dmg File . . . 32

5 Upgrading Mac OS X Client **33**

6 Troubleshooting **35**

Debugging the Logs 35
Using the Diagnostic Tool to Debug the Logs 35
Manually Debugging the Logs 36
Endpoint Not Found 36
Domain Users are Unable to Create a Network Account on Mac OS 10.13 37
Domain Users are Unable to Unlock the Preferences Pane in the Offline Mode 37

About this Book

This guide has been designed for users and describes the system requirements and the installation procedure for the Advanced Authentication Mac OS Client. Mac OS Client enables you to log in to Mac system in a more secure way by using the authentication chains configured in Advanced Authentication.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

About Mac OS X Client

Mac OS X Client replaces standard way of log on to Apple Mac OS X by a more secure using the authentication chains configured in Advanced Authentication.

NOTE: Mac OS X Client supports offline logon (when the Advanced Authentication Server is not available) for non-local accounts for authentication chains that contain the following methods: Bluetooth, LDAP Password, Password, HOTP, TOTP, Smartphone (offline mode), Card, FIDO U2F, and PKI.

In cases with fast user switching (FUS), the multi-factor authentication window for Client is displayed.

IMPORTANT: When a domain user (user1) is bound to a local user (local1) and if the domain user user1 logs in and switches to the local user local1 using FUS, the local1 user's credentials are prompted instead of the domain user's credentials.

---

1 System Requirements

For system requirements of Mac OS X Client, see Mac OS X Client.

IMPORTANT: You must have root privileges to install and uninstall Mac OS X Client.

2 Offline Support for Mac OS X Client

You can log in to the Advanced Authentication Mac OS X 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: For fast user switching (FUS), the built-in authentication form of Mac OS is displayed.

IMPORTANT: When a domain user (user1) is bound to a local user (local1) and if the domain user user1 logs in and switches to the local user local1 using FUS, the local1 user's credentials are prompted instead of the domain user's credentials.

3 Configuring the Preliminary Settings

This chapter contains the following pre-configuration settings for the Mac OS Client:

- "Configuring the Mandatory Settings" on page 11
- "Configuring the Optional Settings" on page 16
- "Configuring in Case of Advanced Authentication as a Service" on page 27

Configuring the Mandatory Settings

Following are the mandatory settings for Mac OS Client:

- To setup communication between Mac OS Client and the Advanced Authentication server, perform one of the following:
  - Allow Mac OS 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".

    Or
  - Configure the 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 the Non-DNS Mode".
- To configure the Mac recovery, see "Enabling Remote Login".

Setting-up a DNS for Advanced Authentication Server Discovery

You can configure a DNS to allow the Mac OS X 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 11
- "Adding an SRV Record" on page 12
- "Configuring Authentication Server Discovery in Client" on page 14

Adding a Host in DNS

1. Click **Start > Administrative Tools > DNS** to open the DNS Manager.
2. Perform the following steps to 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 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 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 the 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**.
3. Click **Create Record**.
4. Specify `_aav6` in **Service** of the **New Resource Record** dialog box.
5. Specify `_tcp` in **Protocol**.
6. Specify 443 in **Port Number**.
7. Specify the Fully Qualified Domain Name (FQDN) of the server that is added in **Host offering this service**. For example, `authsrv.mycompany.com.service`.
8. Click **OK**.

Adding an SRV Record from Other Advanced Authentication Sites

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**.
4. Click **Create Record**.
5. Specify `_aav6` in **Service** of **New Resource Record** dialog box.
6. Specify `_tcp` in **Protocol**.
7. Specify 443 in **Port Number**.

8 Specify the FQDN of the server that is added in **Host offering this service**. For example, `authsrv.mycompany.com`.

9 Click **OK**.

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

DNS Server Entries

DNS server contains the following elements in an SRV record:

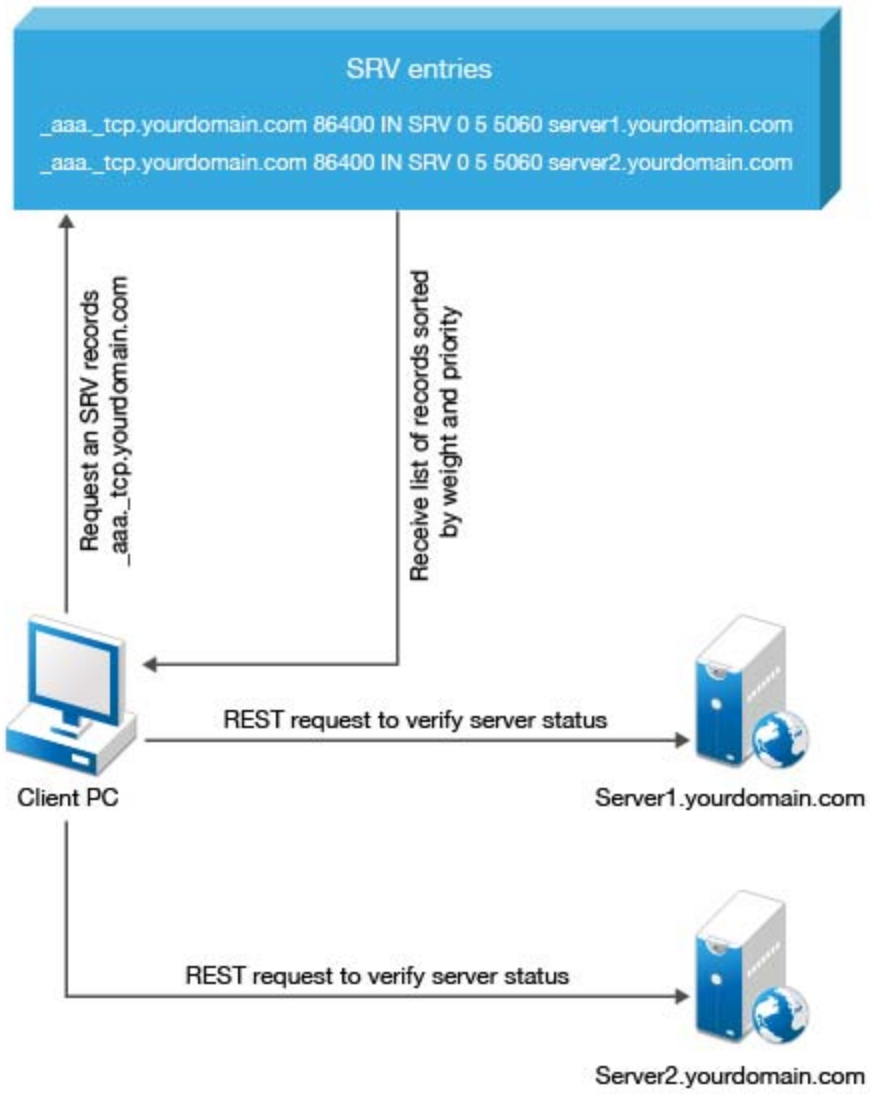
```
SRV entries _service._proto.name TTL class SRV priority weight port target
```

The following table defines 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.
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 (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 Mac OS Client by using the following parameters in the `aucore_login.conf` file that is located in the `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/` path:

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.

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 True for Mac OS 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 Mac OS 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.

Using a Specific Advanced Authentication Server in the Non-DNS Mode

You can achieve the following requirements with this setting:

- Enforce a connection to a specific workstation where the DNS is not available.
- Override a domain based entry for a specific workstation and use the settings specified in the aucore_login.conf file.

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

1. Navigate to /Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/ and open the aucore_login.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 operating system.

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

Enabling Remote Login

You must enable the remote login before installing Advanced Authentication Mac OS X Client. Perform the following steps to enable the remote login:

1. Click the Apple icon in the upper-left corner.
2. Click **System Preferences... > Sharing**.
3. Enable **Remote Login**.
4. Log in to Mac using the ssh login.

   For example, `pjones@192.168.0.112`

Configuring the Optional Settings

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

Setting	Description
disable_1N: true	To disable the automatic detection of username for Card and PKI methods. For more information, see Disabling 1:N.
tenant_name	To use Multitenancy, you must point Mac OS Client to a specific tenant. For more information, see Configuration Settings for Multitenancy.
logo_path: <custom_logo_path>	To customize a logo for Mac OS Client. For more information, see Customizing a Logo.
card.timeout: X	To change a default Card waiting time-out duration. For more information, see Configuring Time-Out for Card Waiting.
u2f.timeout: X	To configure the time-out duration for authentication with the U2F token. For more information see, Configuring Time-Out for the U2F Authentication.
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.
verifyServerCertificate: true	To configure the verification of server certificates for LDAP connection. For more information, see Configuring to Verify Server Certificates.
authentication_agent_enabled: true	To enable the Authentication Agent chain in Mac OS X Client. For more information, see Enabling the Authentication Agent Chain.
forceCachedLogon: true	To enforce the cached login for unlocking the Client. For more information, see Configuring the Enforced Cached Logon.
keep_window_on_unlock: false	To display the authentication window on the Mac OS Client unlock screen, see Displaying the Authentication Window on Unlock Screen.
enableLinkedChainsOffline:false	To disable linked chains for offline login. For more information, see Disabling Linked Chains for Offline Login.

Setting	Description
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.
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 Mac OS 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 Mac OS 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 (:).

Following are the other optional settings:

- To bind Mac to an Active Directory, see "Binding Mac to Active Directory".
- To force offline login manually for users, see "Enabling the Offline Mode".
- To display the user on the login screen in the non-domain mode, see "Displaying Other User on the Login Screen in Non-Domain Mode".
- To create a mobile account, see "Creating a Mobile Account for the Offline Mode".
- To localize the Advanced Authentication resources for your language with the instructions, see Localizing the Messages for Clients.

Disabling 1:N

You can disable the 1:N feature that allows you to detect the user name automatically while authenticating with the Card and PKI methods.

For example, Bob can place the card on the reader to log in to Mac system and authenticate with the Card method automatically without specifying his user name.

To disable the 1:N feature, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Add the parameter **disable_1N: true** in the file.
3. Save the changes.
4. Restart the operating system.

Configuration Settings for Multitenancy

If the Multi-tenancy option is enabled, you must add the parameter `tenant_name` with a tenant name in the `aucore_login.conf` file.

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

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf.`

   If the configuration file does not exist, create a new file.
2. Specify `tenant_name: <name of tenant>`

   For example, `tenant_name: TOP` for the TOP tenant.
3. Save the changes.
4. Restart the operating system.

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

Customizing a Logo

You can customize the logo of Mac OS Client according to your requirement. The format of the logo must meet the following requirements:

- **Image format**: `png, jpg, gif`
- **Resolution**: `400x400px`
- **Maximum file size**: `100Kb`

To customize the logo, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify the path of the folder where the image file is stored, in the following format:

   `logo_path: /Users/<username>/<path_of_the_file>/<file_name>.png`
3. Save the changes.
4. Restart the operating system.

Configuring Time-Out for Card Waiting

You can configure the duration 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 time-out period, the `Hardware timeout` message is displayed and the card waiting dialog is closed. Then, the user login selection screen is displayed.

By default, the card timeout is 60 seconds.

To configure time-out for card waiting, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `card.timeout: X`. X is the timeout value in seconds.
3. Save the changes.
4. Restart the operating system.

Configuring Time-Out for the U2F Authentication

You can configure the duration after which the authentication fails if the user does not touch U2F token for authentication. The default timeout is 60 seconds.

To configure the timeout for U2F authentication, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `u2f.timeout: X` in the file. X is the timeout value in seconds.
3. Save the changes.
4. Restart the operating system.

Selecting an Event

By default, Mac OS X Client uses the **Mac OS 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 type `Generic` for the non-domain joined workstations.

To configure custom event for Mac OS X Client, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `event_name: <CustomEventName>`
3. Save the changes.
4. Restart the operating system.

Configuring to Verify Server Certificates

You can secure connection between Mac OS X Client and Advanced Authentication servers with a valid self-signed SSL certificate. This prevents any attacks on the connection and ensures safe authentication.

To enable verification of the server certificates, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/open aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `verifyServerCertificate=true` (default value is `false`).
3. Save the changes.
4. Place the server certificate in the **Keychain Access**.

NOTE: Ensure that the server certificate is in the `.p12` format.

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.

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 Mac OS X Client to allow users to authenticate with the Authentication Agent on a Windows system. This helps users to get authorized access to the Mac OS X Client that does not support the external devices. To perform such authentication, users must select the Authentication Agent chain from the Chains list of Mac OS X Client to initiate the authentication process on the Windows system, where the Authentication Agent is installed.

To enable the Authentication Agent chain on the Mac OS X Client, perform the following steps:

1. Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `authentication_agent_enabled:true`.
3. Save the changes.
4. Restart the operating system.

Configuring the Enforced Cached Logon

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

To enforce cached login for Mac OS X Client, perform the following steps:

1. Open the configuration file `\Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `forceCachedLogon: true` (default value is `false`).
3. Save the changes.
4. Restart the operating system.

Binding Mac to Active Directory

You can bind a Mac to Active Directory to enable the Mac system to access user accounts in the Active Directory domain. Domain users can use credentials stored in the Active Directory to get authorized access to Mac system. Perform the following steps to bind Mac to Active Directory:

1. Click **Apple** icon in the upper-left corner.
2. Click **System Preferences > Network**.
3. Click **Advanced > DNS**.
4. Double click an existing record to edit it or click **+** in **DNS Servers** section.
5. Specify the IP address of your DNS server.

   For example, `192.168.0.200`.
6. Click **+** in the **Search Domains** section.
7. Specify the FQDN of your domain.

   For example, `company.com`.
8. Click **OK**.
9. Click **Apply** in the **Network** window.
10. Click **System Preferences > Users & Groups**.
11. Click **Login Options** in the left pane.
12. Click the lock icon in lower-left of the screen to unlock and edit the settings.
13. Specify **Username** and **Password** of the local administrator and click **Unlock**.
14. Click **Join** adjacent to the text **Network Account Server**.
15. Specify the IP address of Active Directory domain in **Server**.

    For example, `company.com`.
16. Specify **AD Admin User** and **AD Admin Password**.
17. Click **OK**.

A green icon is displayed adjacent to your domain name indicating, that the Mac system is joined to the domain.

18 Click **Edit > Open Directory Utility**.

19 Click the lock icon in lower-left of the **Directory Utility** screen to unlock and edit the settings.

20 Specify **Username** and **Password** of local administrator.

21 Double click the **Active Directory**.

22 Click the show options icon to view the hidden options.

23 Click **Administrative**.

24 Select **Allow administration by** to grant administrative privileges for members of the Active Directory on the local Mac.

25 Click **OK**.

26 Click the lock icon to prevent further changes.

27 Close the **Directory Utility** and **Users & Groups** screens.

To verify the binding, perform the following steps:

1 Open **Terminal**.

2 Run the following command to log in as an Active Directory user:

```
login <UsernameOfActiveDirectoryUser>
```

For example, `login pjones`.

3 Specify the password. The console switches to the logged in user.

4 Run the command: `exit` to close the Terminal.

5 Click the Apple icon in upper-left corner and select **Log Out <username>**.

6 Click **Other** in the user selection screen to log in as a different domain user.

Enabling the Offline Mode

1 Click the Apple icon in upper-left corner.

2 Click **System Preferences > Users & Groups**.

3 Select **Login Options**.

4 Click the lock icon in lower-left of the window to unlock and edit the settings.

5 Specify **Username** and **Password** of the local administrator and click **Unlock**.

6 Click **Edit** next to **Network Account Server**.

7 Click **Open Directory Utility**.

8 Click the lock icon in lower-left of the window to unlock and edit the settings.

9 Specify **Username** and **Password** of the local administrator and click **Unlock**.

10 Double click **Active Directory**.

11 Click the show options icon to view the hidden options.

12 Select **Create mobile account at login**.

13 Click **OK**.

NOTE: The users must create a mobile account to use Mac OS X Client in the offline (cached) mode. For more information about creating a mobile account, see Creating a Mobile Account for the Offline Mode.

Displaying Other User on the Login Screen in Non-Domain Mode

Open the terminal and run the following command to display **Other User** on the login screen of the non-domain mode:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow
SHOWOTHERUSERS_MANAGED -bool TRUE
```

Creating a Mobile Account for the Offline Mode

To use Mac OS X Client in the offline mode, you must create a mobile account for a domain user. Perform the following steps to create the mobile account for a domain user:

1. Log in as a domain user.
2. Click the Apple icon in the upper-left corner and select **System Preferences**.
3. Click **Users & Group.**
4. Click the lock icon in lower-left of the screen to unlock and edit the settings.
5. Specify **Username** and **Password** of the local administrator and click **Unlock**.
6. Select the preferred domain user.
7. Select **Create Mobile Account for the User**.
8. Click **Create**.

   The operating system gets logged off automatically.

Displaying the Authentication Window on Unlock Screen

Sometimes, when users log in or unlock a Mac machine with the Mac Client installed, the authentication window disappears at some point during the process. If the user moves the mouse, the screen directs to the beginning of the login or unlock process. A solution to this issue, when the Mac Client is in sleep, lock, or screen saver mode, you can display an authentication window instead of blank or black screen.

Perform the following steps to display an authentication window during sleep, lock or screen saver mode:

1. Open the configuration file `\Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

   If the file does not exist, create a new file.
2. Specify `keep_window_on_unlock: true` (default value is `false`) to display the authentication window during the unlocking process until the user closes the window manually.

   With the `keep_window_on_unlock` parameter set to `false`, the authentication window disappears if user is inactive (no click on mouse or no use of keyboard) for 30 seconds. However, the authentication window does not disappear if the user is active.

3 Save the configuration file.

4 Restart the operating system.

Disabling Linked Chains for Offline Login

With a linked chain, users can authenticate to the Mac OS 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 Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

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

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

3 Save the changes.

4 Restart the operating system.

Enabling the Profiling Tool

You can configure the Mac OS X 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 serve**r in the Administration portal.

To enable the Profiling tool, perform the following steps:

1 Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

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

2 Specify `rest_profiling: true` (default value is `false`).

3 Save the changes.

4 Restart the operating 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 `Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/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 `aucore_login.pot` files, and paste it in `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/aucore/locale/<language>\LC_MESSAGES`.
5. Open the `aaacachesrv.pot`, `aucore.pot` and `aucore_login.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 `aucore_login.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 Mac OS Client without Changing the Locale of the Operating System

This option allows you to change the locale of Mac OS Client without changing the locale of the operating system.

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

To change the locale, perform the following steps:

1 Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

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 changes.

4 Restart the operating system.

Configuring the TLS Version

You can configure the TLS version that the network library of the Mac OS 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 Open the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

2 Specify `tlsVersion: value`. The values are defined as follows:

- TLSv1.3: Default and strongly recommended value.
- TLSv1.2

NOTE: If the Mac OS 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.

Configuring in Case of Advanced Authentication as a Service

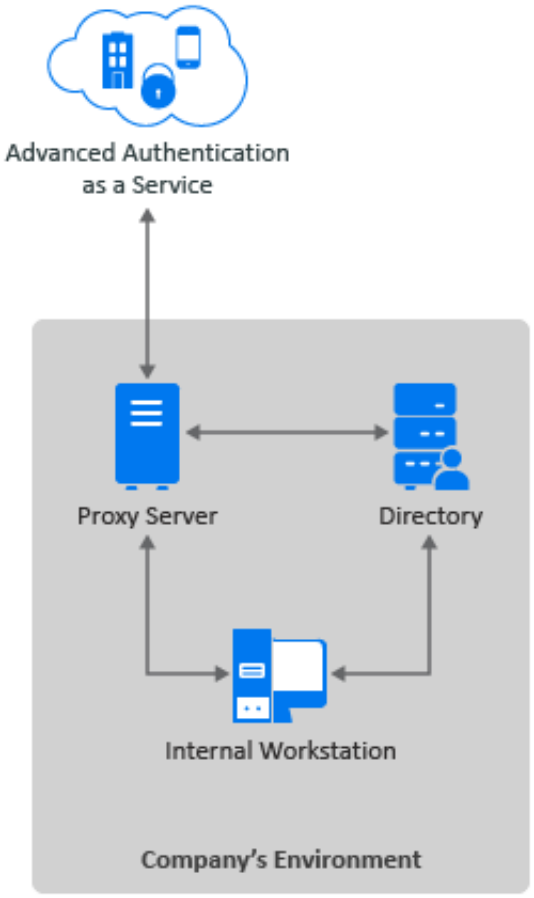
The following table describes the parameters to configure Mac OS Client in case of Advanced Authentication as a Service.

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 Mac OS 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 Mac OS Client to work with Advanced Authentication Servers via HTTP Proxy. Perform the following steps to configure the Mac OS client.



1 Navigate to `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.

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 `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.
2. Specify the following parameter:

   ```
   disable_local_accounts: true
   ```
3. Save the changes.
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.

4 Installing and Uninstalling Mac OS X Client

This chapter contains the following sections:

- Installing Mac OS X Client
- Uninstalling Mac OS X Client

NOTE: To view the installed version of Mac OS X Client, open the text file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/etc/version`.

You can find the Mac OS X Client installer in the Advanced Authentication Logon Clients distributive package.

Installing Mac OS X Client

1. Double click the `naaf-macclient-macos-release-<version>.dmg` file.

   The `naaf-macclient.pkg` and `uninstall` files are displayed.
2. Double click the `naaf-macclient.pkg file`.
3. Click **Continue**.
4. Read and accept the license agreement.
5. Select the disk where you want to install the Mac OS Client and click **Continue**.
6. Click **Install**.

   A prompt to specify the local administrator credentials is displayed.
7. Specify **Username** and **Password**.
8. Click **Install Software.**

NOTE: After the Mac OS X Client is installed, ensure to create a mobile account for a domain user. For more information, see Creating a Mobile Account for the Offline Mode.

IMPORTANT: You must set **Require admin password to register endpoint or workstation** to **OFF** in the **Endpoint management options** on the Advanced Authentication Administration portal. Otherwise, the required endpoint is not created. For more information, see Endpoint Management Options in the **Sever Administration guide**.

Uninstalling Mac OS X Client

Following are the ways to uninstall Mac OS Client:

- “Uninstalling Mac OS Client with dmg File” on page 32
- “Uninstalling Mac OS Client without dmg File” on page 32

Uninstalling Mac OS Client with dmg File

Perform the following steps to uninstall Mac OS Client:

1. Double click the `naaf-macclient-macos-release-<version>.dmg` file.

   The `naaf-macclient.pkg` and `uninstall` files are displayed.
2. Click the `uninstall` file.
3. Specify the local administrator credentials.

Uninstalling Mac OS Client without dmg File

Perform the following steps to uninstall Mac OS Client:

1. Navigate to `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/`.
2. Click the `uninstall` file.
3. Specify the local administrator credentials.

5 Upgrading Mac OS X Client

To upgrade Mac OS X Client to the latest version, perform the following steps:

1. Install the latest version of Mac OS X Client.
2. Reboot Mac OS X Client.

6 Troubleshooting

This chapter contains the following sections:

- "Debugging the Logs" on page 35
- "Endpoint Not Found" on page 36
- "Domain Users are Unable to Create a Network Account on Mac OS 10.13" on page 37
- "Domain Users are Unable to Unlock the Preferences Pane in the Offline Mode" on page 37

Debugging the Logs

Advanced Authentication provides a Diagnostic Tool that allows you to collect the debug logs for Mac OS X Client and Device Service. These logs help the Support team with the following:

- Investigate issues with Mac OS X Client and Device Service.
- Verify connection issues between a Mac OS X Client and DNS server.
- Identify a list of the Advanced Authentication servers on the domain.

You can collect the debug logs in two ways:

- Using the Diagnostic Tool to Debug the Logs
- Manually Debugging the Logs

NOTE: You can find the Diagnostic Tool component in the Advanced Authentication appliance distributive package.

Using the Diagnostic Tool to Debug the Logs

To collect the debug logs using the Diagnostic Tool, perform the following steps:

1. Run the file `DiagTool.app` and click **Enable**.

   NOTE: After you enable or disable the logs, it is recommended to restart your operating system.

   ---

2. Repeat your issue.
3. Run the file `DiagTool.app` again.

   All the logs are displayed.
4. Click **Save** in the **Debug logs** tab.

   A file that contains all logs is saved in the `logs-year-month-date-hour:minute:seconds.zip` format in the `/tmp` directory.

   For example, logs file is saved as `logs-2017-10-23-15:30:20.zip`.
5. Click **Save**.

You can perform the following actions in the **Debug logs** tab:

- Use **Disable** to disable the logging.
- Use **Refresh** to update the logs list.
- Use **Open** to open any specific log.
- Use **Clear All** to delete the existing logs.

To identify the Advanced Authentication servers on the domain, perform the following steps:

1. Run the file `DiagTool.app`.
2. Click **Servers**.
3. Specify **DNS Server** and **Domain**.
4. Select **Use v6 DNS lookup** to allow the Diagnostic Tool to find the Advanced Authentication server using `_aav6` records.

   You can clear **Use v6 DNS lookup**, if you want to find the Advanced Authentication server using `_aaa` records.
5. Click **Search**.

   A list of servers is displayed, if the IP is either IPv4 or IPv6.

NOTE: If you configure the IP address of the Advanced Authentication server in DNS service record, the Diagnostic tool cannot find and retrieve the respective record. Ensure that you configure the DNS service record with the Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.

Manually Debugging the Logs

If you do not have the Diagnostic Tool, you can collect the debug logs manually. To collect the debug logs manually, perform the following steps:

1. Create a text file `config.properties` in the `/Library/Logs/NetIQ/` directory.
2. Add a string to the file: `logEnabled=True` that ends with a line break.
3. Create a directory named `Logs` in the `/Library/Logs/NetIQ/` directory.
4. Restart the operating system.
5. Repeat your issue.
6. Compress the logs located in the `/Library/Logs/NetIQ/Logs/` directory to a zip file.

Endpoint Not Found

Issue: After installing Mac OS X Client and rebooting the system, the Client prompts an error message `Endpoint not found` and a user is unable to log in.

Reason: An endpoint for the client exists in the server or in the configuration file of the client.

Workaround: Perform the following steps:

1. Remove the endpoint for the client on the server in the **Endpoints** section of the Administration portal (if the endpoint specific to client exists).
2. Boot in the Safe mode and remove the `endpoint_id`, `endpoint_name`, and `endpoint_secret` parameters from the configuration file `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`.
3. Restart the operating system.

Domain Users are Unable to Create a Network Account on Mac OS 10.13

Issue: On Mac OS 10.13, when a domain user logs in for the first time to the domain joined Mac Client and tries to create a network account to enable the online mode, the following issues occurred:

- The operating system does not respond after the user specifies the credentials.
- Home directory is not created for that specific user.

These issues occur due to the restriction on the operating system.

Workaround: Create a mobile account and try to log in to Mac OS 10.13 as the domain user.

Domain Users are Unable to Unlock the Preferences Pane in the Offline Mode

Issue: On Mac OS 10.13.6, when a domain user logs in to the domain joined Mac Client in the offline mode and tries to unlock any preference pane using the lock icon  in the lower-left corner, the preference does not get unlocked to change settings. This issue occurs when the user is not granted the administrator privileges.

Workaround: Perform the following steps to grant the administrator privileges to a specific user:

1. Log in as a domain user and create a mobile account.
2. Click **System Preferences > Users & Groups**.
3. Select the preferred mobile account.
4. Select **Allow user to administer this computer**.
5. Restart the operating system.