
Installation Guide

Advanced Authentication - Mac OS X 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
How to Set a DNS for Server Discovery	11
How To Bind Mac To Active Directory	14
How To Configure Mac Recovery	15
Using a Specific Advanced Authentication Server	16
Configuration Settings for Multitenancy	16
Customizing a Logo	16
Configuring Timeout for Card Waiting	17
Working in Offline Mode	17
Selecting an Event	17
How To Show Other User on Login Screen in Non-Domain Mode	18
Creating a Mobile Account	18
Configuration for Verification of Server Certificates	18
Configuration to Enable the Authentication Agent Chain	19
Configuring the Enforced Cached Logon	19
3 Installing and Uninstalling Mac OS X Client	21
Installing Mac OS X Client	21
Upgrading Mac OS X Client from 5.4 to 6.0	22
Uninstalling Mac OS X Client	22
4 Troubleshooting	23
Collecting Debug Logs	23
Using Diagnostic Tool	23
Manual	24
Endpoint Not Found	24
Domain Users are Unable to Create Network Account on Mac OS 10.13	25
Domain Users are Unable to Unlock the Preferences Pane in the Offline Mode	25

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 Mac OS X Client Installation Guide is designed for all users and describes the system requirements and the installation procedure for Advanced Authentication Mac OS Client.

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, the native authentication form is displayed.

1

System Requirements

IMPORTANT: Installing and removing Mac OS X Client requires root privileges.

The following system requirements should be fulfilled:

- ♦ Apple Mac OS 10.12 (Sierra), 10.13 (High Sierra).
- ♦ DNS is properly configured for Advanced Authentication Server discovery (see [How to Set a DNS for Server Discovery](#)) or a specific Advanced Authentication server must be specified in the [configuration file](#).
- ♦ It's recommended to have the recovery configured for the Mac. For more information, see [How To Configure Mac Recovery](#).

2 Configuring the Preliminary Settings

This chapter contains sections about the pre-configuration settings on Mac OS Client.

- ♦ You need to setup an interaction between Mac OS Client and Advanced Authentication server.
 - ♦ To make Mac OS Client interact with Advanced Authentication servers through DNS, see [“How to Set a DNS for Server Discovery”](#).
- Or
- ♦ To manually specify a custom Advanced Authentication server, see [“Using a Specific Advanced Authentication Server”](#).
- ♦ To configure the Mac recovery, see [“How To Configure Mac Recovery”](#).
- ♦ **Optional Settings:**
 - ♦ To change a default Card waiting timeout, see [“Configuring Timeout for Card Waiting”](#).
 - ♦ 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”](#).
 - ♦ If you use Multitenancy, you must point Mac OS Client to a specific tenant. For more information, see [“Configuration Settings for Multitenancy”](#).
 - ♦ To bind Mac to an Active Directory, see [“How To Bind Mac To Active Directory”](#).
 - ♦ To customize a logo for Mac OS Client, see [“Customizing a Logo”](#).
 - ♦ To configure the verification of server certificates for LDAP connection, see [“Configuration for Verification of Server Certificates”](#).
 - ♦ To force offline login manually for users, see [“Working in Offline Mode”](#).
 - ♦ To display the user on the login screen in the non-domain mode, see [“How To Show Other User on Login Screen in Non-Domain Mode”](#).
 - ♦ To create a mobile account, see [“Creating a Mobile Account”](#).
 - ♦ To enable Authentication Agent chain in the Mac OS Client, see [“Configuration to Enable the Authentication Agent Chain”](#).
 - ♦ To configure the Cached Login for Mac OS client unlock, see [““Configuring the Enforced Cached Logon” on page 19”](#).

How to Set a DNS for Server Discovery

Question:

I would like to set DNS for server discovery. How can I do it and what is its workflow?

Answer:

To set a DNS for the Server Discovery, perform the following steps:

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:
 - a. In the console tree, right-click the forward lookup zone that includes your domain name and click **New Host (A or AAAA)**.
 - b. Specify a DNS name for the Advanced Authentication Server in **Name**.
 - c. 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).
 - d. 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.

- a. For Advanced Authentication servers from a primary Advanced Authentication site (a site with Global Master server):
 - i. In the console tree, locate **Forward Lookup Zones** and right-click on a node with domain name and click **Other New Records**.
 - ii. In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.
 - iii. Click **Service** and then specify **_aav6**.
 - iv. Click **Protocol** and then specify **_tcp**.
 - v. Click **Port Number** and then specify **443**.
 - vi. In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.
 - vii. Click **OK**.
- b. For Advanced Authentication servers from other Advanced Authentication sites:
 - i. 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**.
 - ii. In the **Select a resource record type** list, click **Service Location (SRV)** and then click **Create Record**.
 - iii. Click **Service** and then specify **_aav6**.
 - iv. Click **Protocol** and then specify **_tcp**.
 - v. Click **Port Number** and then specify **443**.
 - vi. In **Host offering this service**, specify the FQDN of the server that is added. For example, `authsrv.mycompany.com`.
 - vii. Click **OK**.

Repeat steps 2 to 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 present 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 side

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 features is not supported in Windows Client.

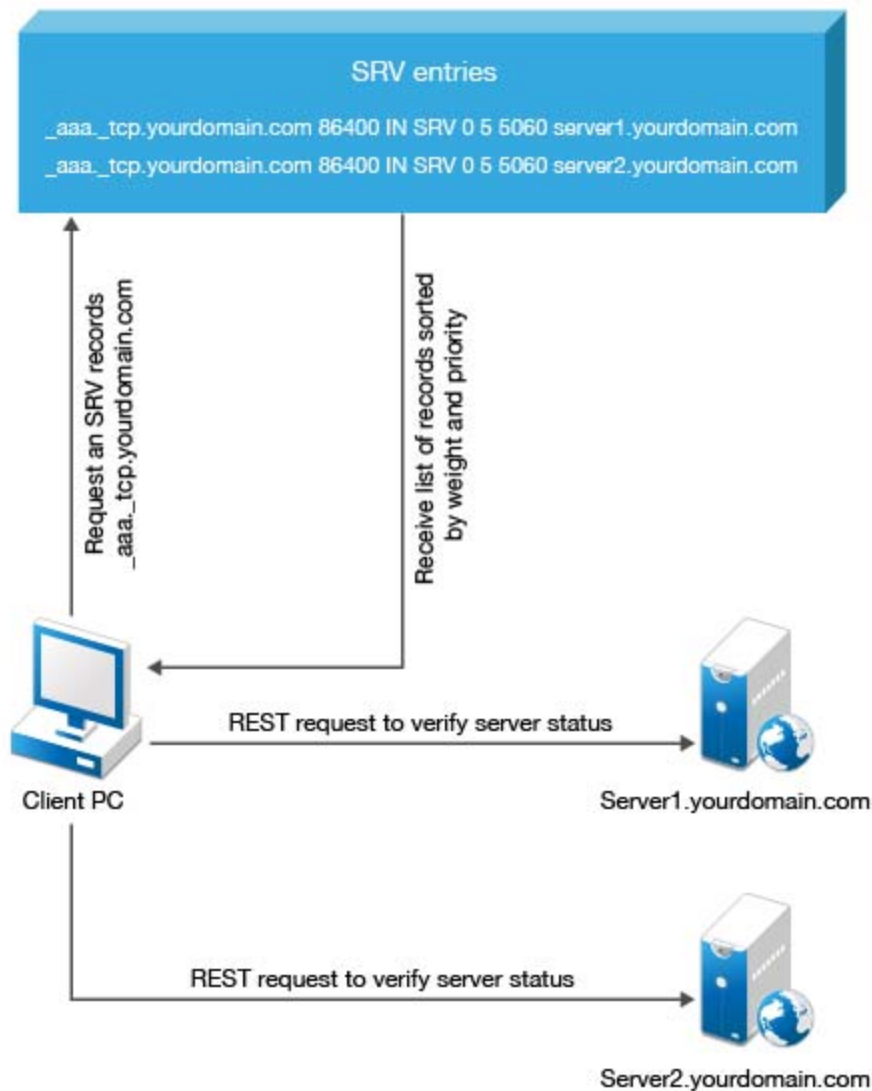
Mac OS X Client/ Linux PAM module

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:

- ♦ **Mac OS X 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.



How To Bind Mac To Active Directory

Binding Mac to Active Directory is preliminary required to get the Advanced Authentication Client working. To do it follow the steps:

1. Click Apple icon in left top corner, select **System Preferences...**
2. Click Network icon.
3. Click **Advanced...** button.
4. Switch to **DNS** tab.
5. In **DNS Servers** section double click an existing record to edit it. If it's not possible click + button.
6. Enter IP address of your DNS server. E.g. 192.168.0.200.
7. Click + button in **Search Domains** section.
8. Enter FQDN of your domain. E.g. company.com.
9. Click **OK**.
10. Click **Apply** in Network window.

11. Switch back to the **System Preferences...** menu.
12. Click **Users & Groups** icon.
13. Select **Login Options** item.
14. Click lock icon in bottom part of the window to unlock making changes.
15. Enter local admin's **Username** and **Password** and click **Unlock**.
16. Click **Join...** next to the **Network Account Server** text.
17. In **Server** field enter the address of an Active Directory Domain. E.g. company.com.
18. Fill the **AD Admin User** and **AD Admin Password** fields.
19. Click **OK**.
20. In some seconds you will see a green icon near your domain name, next to the **Network Account Server** text.
21. Click **Edit...**
22. Click **Open Directory Utility...**
23. Click lock icon in bottom part of the **Directory Utility** window to unlock making changes.
24. Enter local admin's **Username** and **Password** and click **Modify Configuration**.
25. Double check the **Active Directory** item.
26. Expand **Show Advanced Options**.
27. Switch to **Administrative** tab.
28. Check the **Allow administration by** option.
29. Click **OK**.
30. Click lock icon in bottom part of the **Directory Utility** window to prevent further changes.
31. Close the **Directory Utility** and **Users & Groups** windows.

To check the binding follow the steps:

1. Run **Terminal**.
2. Execute the command: `login <UsernameOfActiveDirectoryUser>`. E.g. `login pjones`.
3. Enter the user's password. The console should switch to the user.
4. Execute the command: `exit`. Close the Terminal.
5. Click **Apple** icon in left top corner, select **Log Out <username>...**
6. In user selection screen you will see the **Other...** icon.
7. Click it and try to log on as the domain user.

How To Configure Mac Recovery

It's recommended to configure recovery for Mac before the installation of Advanced Authentication Mac OS X Client. To do it follow the steps:

1. Click the **Apple** icon in left top corner, select **System Preferences...**
2. Click **Sharing** icon.
3. Enable **Remote Login** option.
4. Remember the ssh login. It should be a string like: `pjones@192.168.0.112`.
5. Try to log on to the Mac using ssh.

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 Mac OS X Client is not joined to a domain.

In the `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.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>`.

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.

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: `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.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`.

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 configuration file `aucore_login.conf`.
4. Restart the computer.

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 `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf` file.
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.

Working in Offline Mode

To use Advanced Authentication in offline (cached) mode, mobile accounts has to be created. Perform the following steps to enable working in offline mode:

1. Click the **Apple** icon in left top corner, select **System Preferences...**
2. Click **Users & Groups** icon.
3. Select **Login Options** item.
4. Click **Lock** icon in bottom part of the window to unlock marking changes.
5. Enter local administrator's Username and Password and then click **Unlock**.
6. Click **Edit...** next to the **Network Account Server** text.
7. Click **Open Directory Utility...**
8. Click **Lock** icon in bottom part of the window to unlock marking changes.
9. Enter local administrator's Username and Password and then click **Unlock**.
10. Double click Active Directory.
11. Expand the hidden section of the window.
12. Select **Create mobile account at login** option.
13. Click **OK**.

Selecting an Event

By default Mac OS 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:

```
/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/  
aucore_login.conf
```

How To Show Other User on Login Screen in Non-Domain Mode

To show **Other User** on login screen in non-domain mode, execute the following in Terminal:

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

Creating a Mobile Account

For offline login, it is required to create a mobile account for a domain user. To create mobile account for a domain user, perform following steps:

- 1 Login to domain user.



- 2 Click the Apple icon in the upper left corner and select **System Preferences**.
- 3 Click **Users & Group**.
- 4 Click **Click the lock to make changes**.
- 5 Select preferred domain user.
- 6 Select **Create Mobile Account for the User**.
- 7 Click **Create**.

The system gets logged off automatically.

Configuration for Verification of Server Certificates

You can secure connection between a workstation and Advanced Authentication Servers with a valid self-signed SSL certificate, thus preventing any attacks on the connection and ensuring safe authentication.

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

- 1 Navigate to `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/` and open `aucore_login.conf` file.
If the configuration file does not exist, create a new file.
- 2 Specify `verifyServerCertificate=true` in the configuration file.
- 3 Place the server certificate in the **Keychain**.

NOTE: Ensure that the server certificate is in .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](#).

Configuration to Enable the Authentication Agent Chain

You must select **Authentication Agent** in the Chains list of Mac Client to initiate the authentication process on Windows computer where the Authentication Agent is installed. To enable the Authentication Agent chain in the Mac Client, perform the following steps:

- 1 Navigate to `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/` and open `aucore_login.conf` file.
If the configuration file does not exist, create a new file.
- 2 Specify `verifyServerCertificate=true` in the configuration file.
- 3 Click **Save**.
- 4 Restart your computer.

Configuring the Enforced Cached Logon

When the network connection is slow or unstable, the client logon or unlock process can 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 not used and the Client will always try to connect to Advanced Authentication Server to validate credentials.

Perform the following steps to allow users to use the enforced cached logon:

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) in the `aucore_login.conf` file.
3. Save the configuration file.
4. Restart the system.

3 Installing and Uninstalling Mac OS X Client

In this chapter:

- ♦ [Installing Mac OS X Client](#)
- ♦ [Uninstalling Mac OS X Client](#)

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

You can find the Mac OS X Client in the Advanced Authentication Enterprise Edition distributive package.

IMPORTANT: After upgrading the Mac OS X, you may have to reinstall the NetIQ Mac OS X Client.

Installing Mac OS X Client

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

The `naaf-macclient.pkg` and `uninstall` files are displayed.

2. Double click the file `naaf-macclient.pkg`.
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 window is displayed to specify the local administrator credentials to install the software.
7. Specify **Username** and **Password**.
8. Click **Install Software**.
9. Click **Close**.

NOTE: After the Mac OS X client is installed, ensure to [create a mobile account for domain user](#) on the Mac OS X Client.

IMPORTANT: You must set **Require admin password to register endpoint/workstation** to **OFF** in the Endpoint management options on the Advanced Authentication Administrative Portal. Otherwise the required endpoint is not created. For more information, see [Endpoint Management Options](#) in the [Sever Administrator guide](#).

Upgrading Mac OS X Client from 5.4 to 6.0

To upgrade Mac OS X Client from 5.4 to 6.0, perform the following steps:

- 1 Run `sudo /Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/bin/uninstall` in the terminal.
- 2 Reboot Mac OS X Client.
- 3 Delete `aucore_login.bundle` from the `/Library/Security/SecurityAgentPlugins` folder.
- 4 Reboot Mac OS X Client.
- 5 Delete the endpoint in the Advanced Authentication Administration portal.
- 6 Install 6.0 Mac OS X Client.

Uninstalling Mac OS X Client

You can uninstall Mac OS X client in two ways:

- ♦ [Using Uninstall Script](#) (recommended)
- ♦ [Manual](#)

Using Uninstall Script

- 1 Double click the file `naaf-macclient-macos-release-<version>.dmg`.
The `naaf-macclient.pkg` and `uninstall` files are displayed.
- 2 Click the `uninstall` file.
- 3 Specify sudo password.

Manual

- 1 Open the **Terminal** application.
- 2 Run the command `cd /Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/bin/` to navigate to the directory.
- 3 Run the command `sudo ./uninstall`.
- 4 Reboot Mac OS X client.
- 5 Delete the file `aucore_login.bundle` from the path `/Library/Security/SecurityAgentPlugins`.
- 6 Reboot Mac OS X client.

NOTE: When you uninstall Mac OS X client in the Manual way, ensure to remove the corresponding endpoint manually on Advanced Authentication Server. We recommend you to uninstall Mac OS X client using the `uninstall` script that performs complete uninstallation.

4 Troubleshooting

This chapter contains following topics:

- ♦ [“Collecting Debug Logs” on page 23](#)
- ♦ [“Endpoint Not Found” on page 24](#)
- ♦ [“Domain Users are Unable to Create Network Account on Mac OS 10.13” on page 25](#)
- ♦ [“Domain Users are Unable to Unlock the Preferences Pane in the Offline Mode” on page 25](#)

Collecting Debug Logs

Advanced Authentication provides a Diagnostic Tool that allows you to collect the debug logs for Mac OS X Client and Device Service. The Debug logs helps 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 Diagnostic Tool](#)
- ♦ [Manual](#)

Using Diagnostic Tool

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 system.

- 2 Repeat the scenario.
- 3 Run the file `DiagTool.app` again.
All logs are displayed.
- 4 Click **Save** in the **Debug logs** tab.

A file that contain 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 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 Fully Qualified Domain Name (FQDN) to enable the Diagnostic tool to find and retrieve the respective record.

Manual

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 `config.properties` file: `logEnabled=True` that ends with a line break.
- 3 Create a directory named `Logs` in the `/Library/Logs/NetIQ/` directory.
- 4 Restart the system.
- 5 Repeat the scenario.
- 6 Compress the logs located in `/Library/Logs/NetIQ/Logs/` directory to a `.zip` format.

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 `/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/etc/aucore_login.conf`
3. Reboot.

Domain Users are Unable to Create 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 is not responding after the user specifies the credentials.
- ♦ Home directory is not created for that specific user.

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

Workaround: As a solution to this issue, [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 is not getting unlocked to change the settings. This issue occurs when the user has not been granted the administrator privileges.

Workaround: As a solution to this issue, perform the following steps:

- 1 Login as a domain user and [create a mobile account](#).
- 2 Launch **System Preferences** and navigate to **Users & Groups**.
- 3 Select the preferred mobile account.
- 4 Select **Allow user to administer this computer** option.
- 5 Restart your system.

