# Installation Guide

## Advanced Authentication - Mac OS X Client

**Version 5.5**

MICRO FOCUS

## 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 © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.**

# Contents

**About NetIQ Corporation** **5**
**About this Book** **7**

**1 System Requirements** **9**

**2 Preliminary configuration** **11**

2.1 How to Set a DNS for Server Discovery . . . . . 11
2.2 How To Bind Mac To Active Directory. . . . . 14
2.3 How To Configure Mac Recovery. . . . . 15
2.4 Using a Specific Advanced Authentication Server . . . . . 15
2.5 Configuration Settings for Multitenancy . . . . . 15
2.6 Working in Offline Mode . . . . . 16
2.7 Selecting an Event . . . . . 16
2.8 How To Show **Other User** on Login Screen in Non-Domain Mode . . . . . 16

**3 Installing and Uninstalling Mac OS X Client** **17**

3.1 Installing Mac OS X Client . . . . . 17
3.2 Uninstalling Mac OS X Client . . . . . 17

**4 Troubleshooting** **19**

4.1 Endpoint Not Found . . . . . 19

# 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 Windows 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:** Only the users from Active Directory repository can be used for login purpose.

**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: 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.

**NOTE:** In the **Login Options** of the **System Preferences** for Mac, you can select the **Display login window as List of users** option only. The option **Name and password** is not supported.

# 1 System Requirements

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

The following system requirements should be fulfilled:

- Apple Mac OS X 10.11 (El Capitan).
- 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.
- Only the Active Directory users can be used for login. Other repositories are not supported.
- It's recommended to have the recovery configured for the Mac. For more information, see How To Configure Mac Recovery.

# 2 Preliminary configuration

The chapter contains articles about required pre-configuration.


- Section 2.1, “How to Set a DNS for Server Discovery,” on page 11
- Section 2.2, “How To Bind Mac To Active Directory,” on page 14
- Section 2.3, “How To Configure Mac Recovery,” on page 15
- Section 2.4, “Using a Specific Advanced Authentication Server,” on page 15
- Section 2.5, “Configuration Settings for Multitenancy,” on page 15
- Section 2.6, “Working in Offline Mode,” on page 16
- Section 2.7, “Selecting an Event,” on page 16
- Section 2.8, “How To Show **Other User on Login Screen in Non-Domain Mode,” on page 16**


## 2.1 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:
   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 **_aaa**.

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 **_aaa**.

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.

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:

- `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 15 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.

## 2.2 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 marking 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 marking 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.

## 2.3 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.

## 2.4 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.

---

## 2.5 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.`

---

## 2.6 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**.

## 2.7 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
```

## 2.8 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
```

# 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`.

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

## 3.1 Installing Mac OS X Client

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

   A system warning is displayed that the package cannot be opened because it is from an unidentified developer.
2. Click the Apple icon in the top left corner and select **System Preferences...**.
3. Click the **Security & Privacy** icon.
4. Click **Open Anyway** on the **General** tab.
5. Click **Continue** on the **Introduction** step.
6. Read and accept the License Agreement.
7. Select the disk where you want to install the Mac OS Client and click **Continue**.
8. Click **Install**.

   A window is displayed requesting you to enter the local administrator credentials to install the software.
9. Enter a valid **Username** and **Password** and click **Install Software.**
10. Click **Close**.

**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**.

## 3.2 Uninstalling Mac OS X Client

1. Open the **Terminal** application.

2. Run the command `cd /Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/Resources/bin/` to switch to the directory.
3. Run the command `sudo ./uninstall`.

---

**NOTE:** Do not remove the `aucore_login.bundle` as it might break Mac OS X.

The endpoint must be manually removed on Advanced Authentication - Administrative Portal.

---

If the login is broken, the above method can be used to uninstall the Mac OS Client with the ssh console from another machine (only if Mac recovery is configured).

# 4 Troubleshooting

To investigate the issues, you may be asked to collect the debug logs. The logs are located in the folder:

`/Library/Security/SecurityAgentPlugins/aucore_login.bundle/Contents/var/log`

## 4.1 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.