NetIQ Advanced Authentication Framework - MacOS Client

Installation Guide

Version 5.2.0

Table of Contents

Introduction

About This Document

Purpose of the Document

This Windows Client Installation Guide is intended for all user categories and describes system requirements that should be fulfilled before the installation of NetIQ Advanced Authentication Framework Windows Client.

Document Conventions

This document uses the following conventions:

Warning. This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

Important notes. This sign indicates important information you need to know to use the product successfully.

Notes. This sign indicates supplementary information you may need in some cases.

Tips. This sign indicates recommendations.

- Terms are italicized, e.g.: ***Authenticator***.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

About MacOS Client

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

MacOS Client 5.2 supports only log on, unlock is not supported. It means that the user will be able to unlock Mac by password only.

Usage of single factor FIDO U2F chain is not supported in Mac OS Client. It should be always combined with LDAP Password and the FIDO U2F method should be last in the used chain, i.e. LDAP Password+FIDO U2F.

System Requirements

Installing and removing MacOS Client requires **root** privileges.

The following system requirements should be fulfilled:

- Apple MacOS X 10.10.5 (Yosemite).
- The machine must be bound to Active Directory. Check the related article.
- DNS is properly configured for NetIQ Advanced Authentication Server discovery. Check the related article.
- Only users of Active Directory repository can be used for log on. Other repositories are not supported.
- It's recommended to have the recovery configured for the Mac. Check the related article.

Preliminary configuration

The chapter contains articles about required pre-configuration.

- How to set DNS for server discovery.
- How to bind Mac to Active Directory.
- How to configure Mac recovery.

How to set 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 DNS for server discovery:

1. Open DNS Manager. To open DNS Manager, click **Start**, point to **Administrative Tools**, and then click **DNS**.
2. Set **Reverse Zone Lookup**:
    a. Go to the **Reverse Zone Lookup** folder icon, right click it and select **New Zone**.
    b. After **New Zone Wizard** opens, click **Next**.
    c. Select **Primary Zone** as the **Zone Type**. Click **Next**.
    d. Type the first three octets of your network IPV4 address range like 192.168.1. Click **Next**.
3. Add Host A or AAAA record and PTR record:
    a. In the console tree, right-click the forward lookup zone which includes your domain name, and click **New Host (A or AAAA)**.
    b. In the **Name** text field, type a DNS name of the NetIQ Advanced Authentication Server.
    c. In the **IP address** text field, type the IP address for the NetIQ Advanced Authentication Server. You can type 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 the **Create associated pointer (PTR) record** check box to create an additional pointer (PTR) resource record in a reverse zone for this host, based on the information that you entered in Name and IP address
4. Add SRV record:
    a. In the console tree, right-click the forward lookup zone which includes your domain name, and click **Other New Records**.
    b. In the **Select a resource record type** list , click **Service Location (SRV)**, and then click **Create Record**.
    c. Click **Service**, and then type **_aaa**.
    d. Click **Protocol**, and then type **_tcp**.
    e. Click **Port Number**, and then type **443**.
    f. In **Host offering this service**, type the FQDN of the server that is added (e.g., authsrv.mycompany.com).
    g. Click **OK**.

Repeat the actions described in points 3-4 for DB Slave and Member servers. You may vary the Priority and Weight values for different servers to prioritize them.

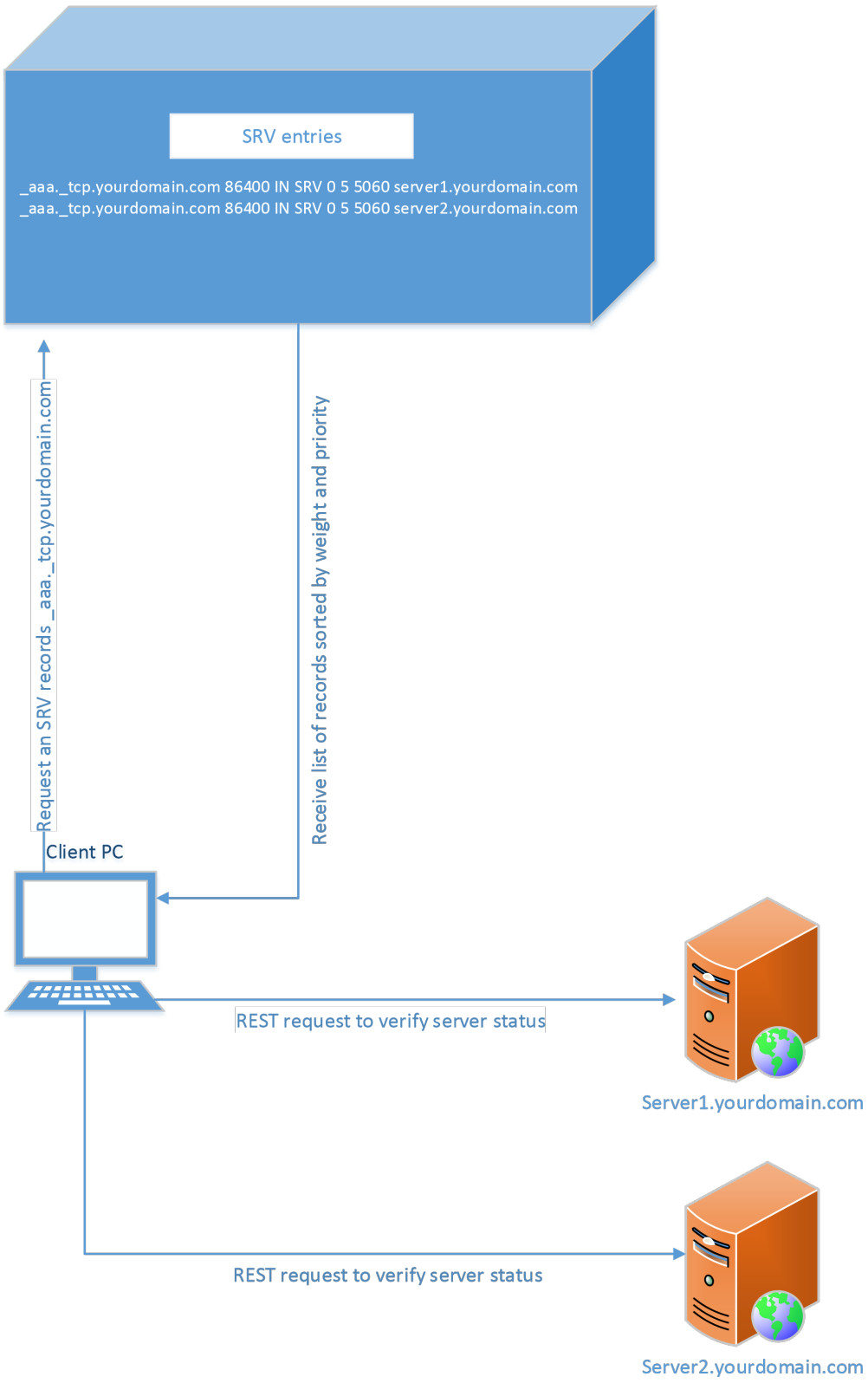
DNS server contains SRV entries _service._proto.name TTL class SRV priority weight port target, where:

- **Service** - symbolic name of an applicable service.
- **Proto** - transport protocol of an applicable service; usually either TCP or UDP.
- **Name** - domain name for which this record is valid; ends with 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 means more preferred.
- **Weight** - a relative weight for records with the same priority; higher value means more preferred.
- **Port** - TCP or UDP port on which the service is located.
- **Target** - canonical hostname of the machine providing the service; ends with dot.

Server discovery workflow is the following:

1. Client sends request through TCP protocol (port 443) to get the list of all entries _aaa._tcp.yourdomain.com.
2. Client receives the sorted list by weight and priority.
3. Since the priority field determines the precedence of use of the record's data, client always uses SRV record with the lowest-numbered priority value first.
4. Client sends https request to check server availability status. If the first connection to the server fails, then client will fall back to other records of equal or higher value. If service has multiple SRV records with the same priority value, client will use the weight field to determine which server to use.

The diagram below shows server discovery workflow graphically.


SRV entries
_aaa._tcp.yourdomain.com 86400 IN SRV 0 5 5060 server1.yourdomain.com
_aaa._tcp.yourdomain.com 86400 IN SRV 0 5 5060 server2.yourdomain.com
Request an SRV records _aaa._tcp.yourdomain.com
Receive list of records sorted by weight and priority
Client PC
REST request to verify server status
Server1.yourdomain.com
REST request to verify server status
Server2.yourdomain.com

How To Bind Mac To Active Directory

Binding Mac to Active Directory is preliminary required to get the NetIQ 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.

How To Configure Mac Recovery

It's recommended to configure recovery for Mac before the installation of NetIQ MacOS Client. To do it follow the steps:

1. Click **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.

Installing and Removing MacOS Client

In this chapter:

Installing MacOS Client

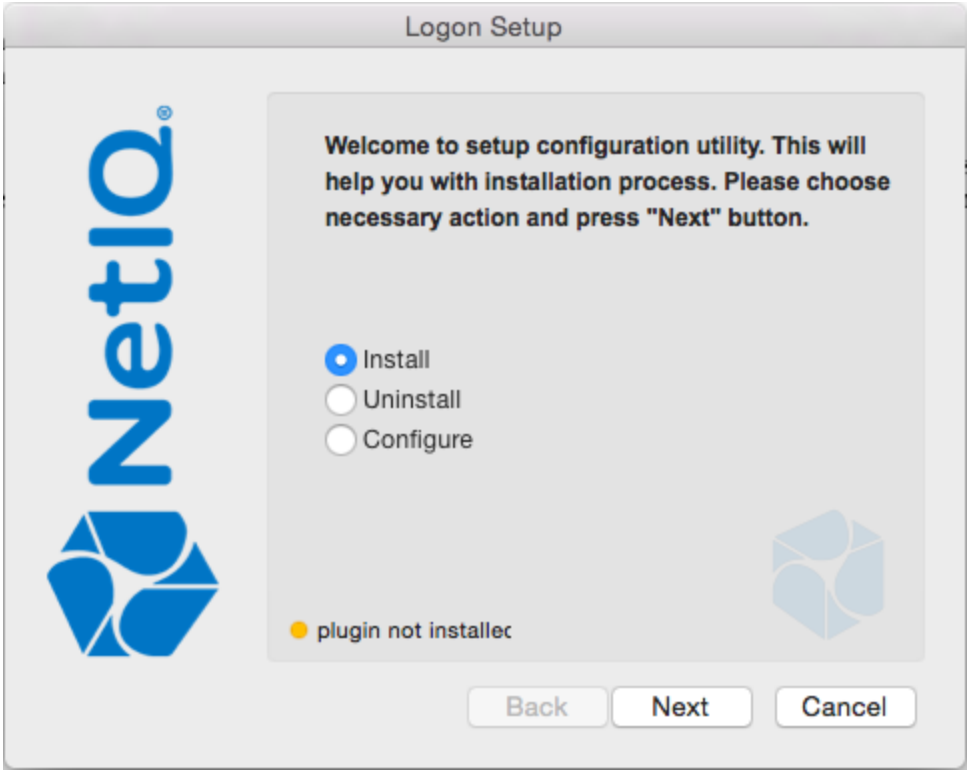
To install MacOS Client follow the instruction:

1. Double click the **NAAFMacOSClient-<version>.dmg** to mount the installation package.

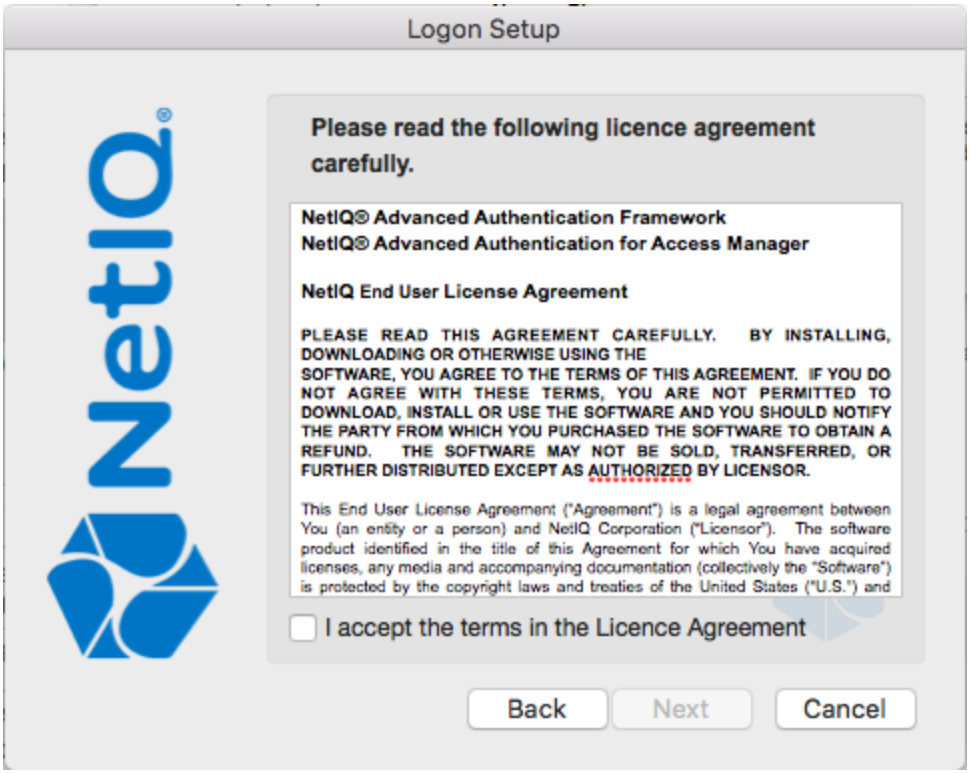
2. Drag the **LogonScreen** folder to the **Applications**.

3. Open **Launchpad** and click **NetIQ MacOS Client** icon.

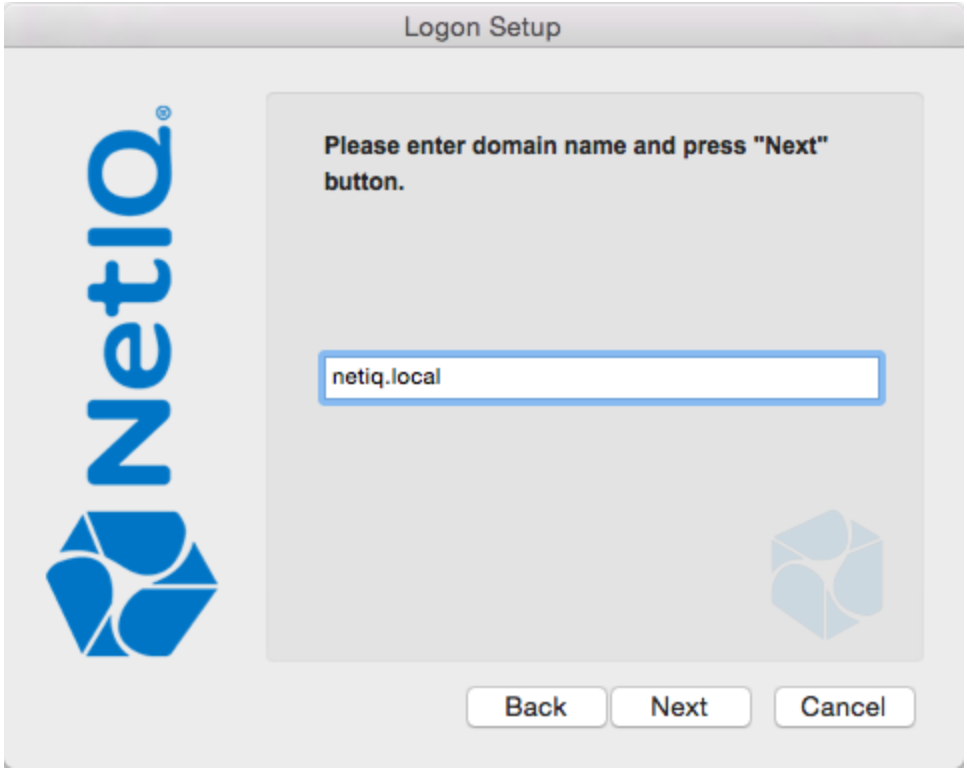
4. Select**Install** and click **Next** to continue.



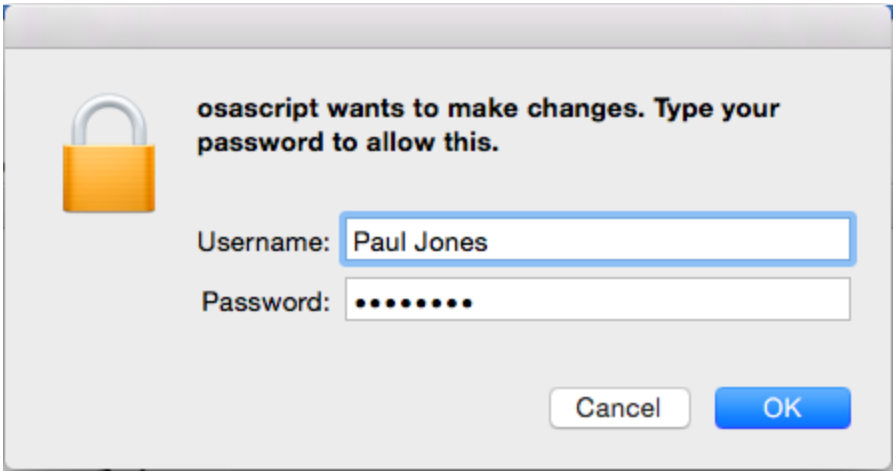
5. Read the **License Agreement**. Select the **I accept the terms in the License Agreement** checkbox and click **Next**.



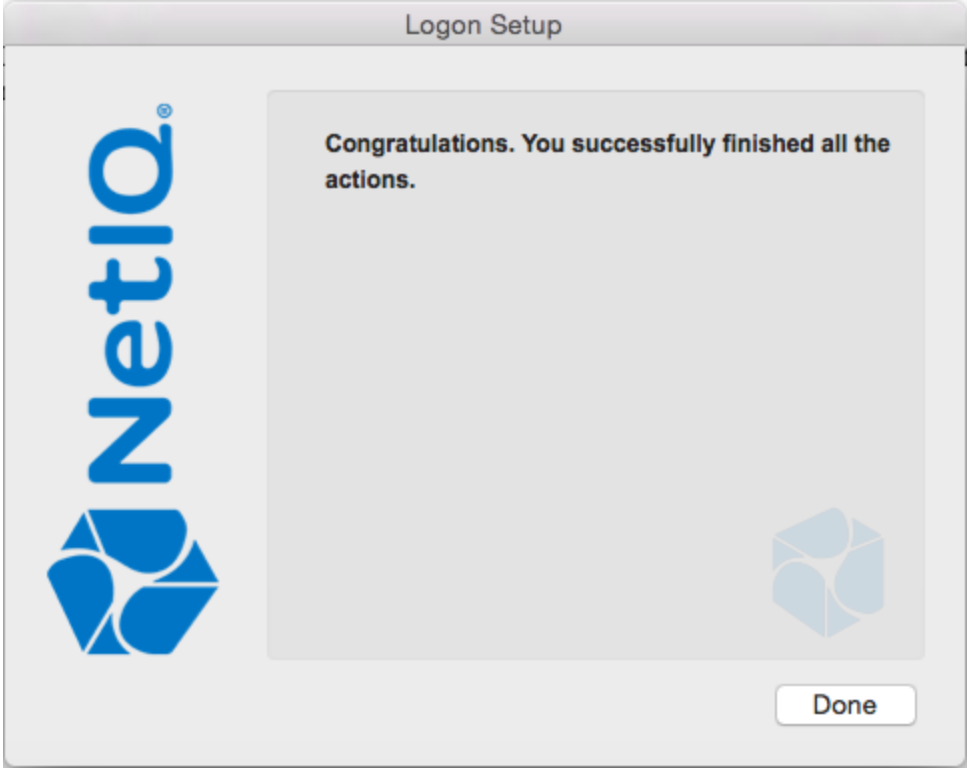
6. Enter an FQDN of your domain and click **Next**.



7. Provide local administrators credentials and click **OK**.



8. Click **Done** to close the wizard.

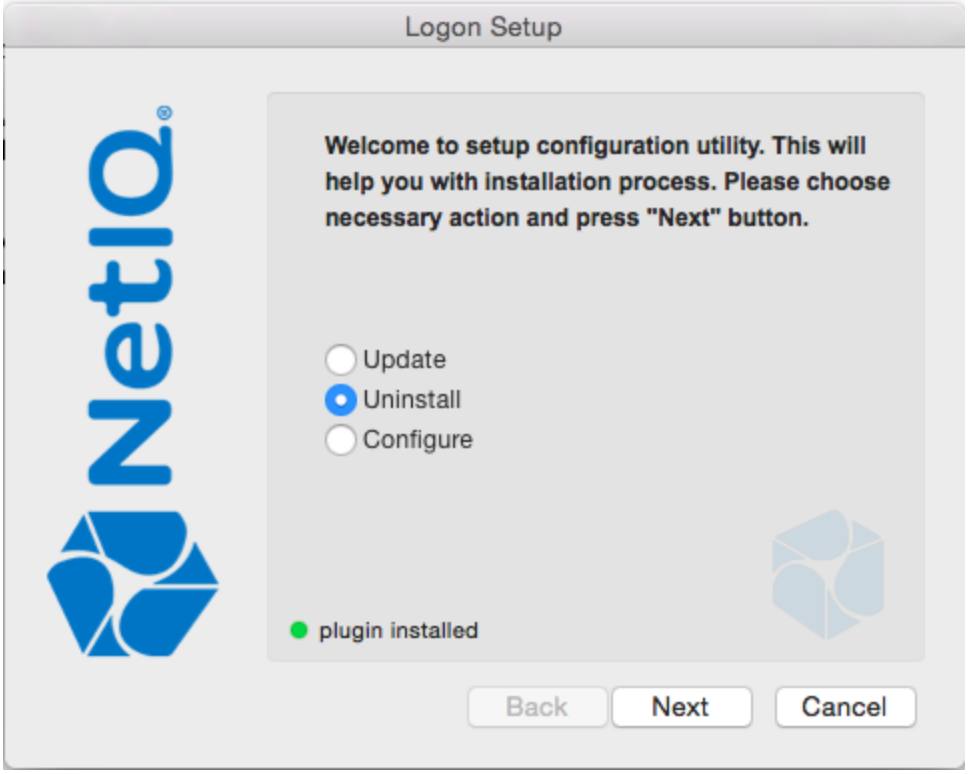


It is required to set **Require admin password to register endpoint/workstation** to **OFF** in **Endpoint management options** on NetIQ Advanced Authentication Administrative Portal. Otherwise the required endpoint won't be created.

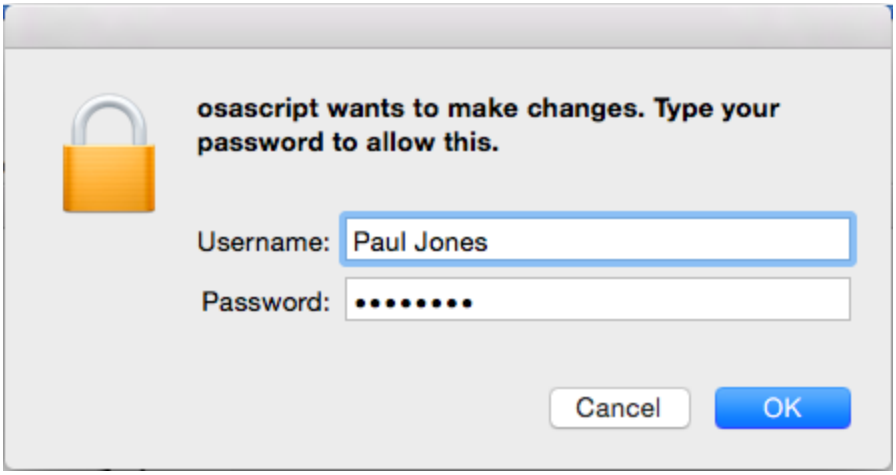
Removing MacOS Client

MacOS Client can be removed using the following way:

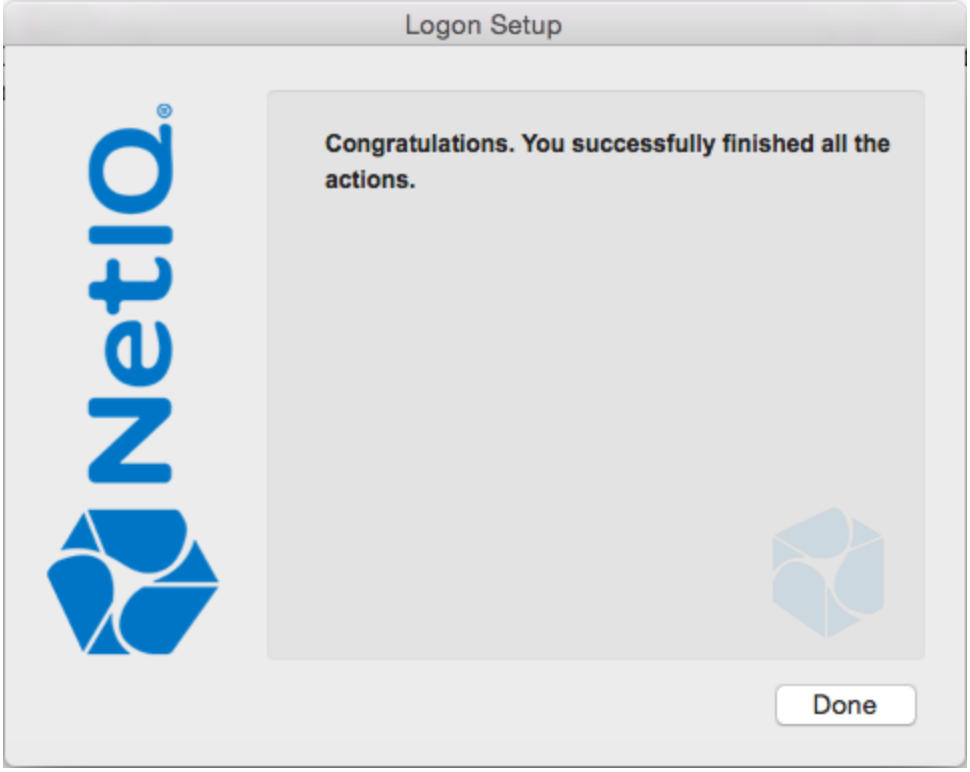
1. Open **Launchpad** and click **NetIQ MacOS Client** icon.
2. Select **Uninstall** and click **Next** to continue.



3. Provide local administrators credentials and click **OK**.



4. Click **Done** to close the installation wizard.



Troubleshooting

To investigate the possible issues you may be asked to collect the debug logs.

To get access to debug logs for Client component in MacOS, follow the steps:

- Open **Launchpad**.
- Click **Other**.
- Click **Console**.
- In left side of the Console window click the **system.log** file.
- In **Search** section enter **[libauth]**.

How To Recover Mac

If MacOS logon was broken and you are not able to log on to uninstall the NetIQ MacOS Client, please follow the steps to perform the Mac recovery:

1. Log on to the Mac using ssh.
2. Switch to the folder: */Applications/LogonScreen/data/scripts/*.
3. Run the *recovery.sh* script.

Index