Technical Report

Security hardening guide for NetApp Active IQ Unified Manager

ONTAP TME Team, NetApp
November 2022 | TR-4943

Abstract

This technical report provides guidance and configuration settings for NetApp® Active IQ® Unified Manager to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

The evolution of the current threat landscape presents an organization with unique challenges for protecting its most valuable assets: data and information. The advanced and dynamic threats and vulnerabilities we face are ever increasing in sophistication. Coupled with an increase in the effectiveness of obfuscation and reconnaissance techniques on the part of potential intruders, system managers must address the security of data and information in a proactive manner. This guide seeks to help operators and administrators in that task with the confidentiality, integrity, and availability integral to the NetApp solution.

Verifying integrity of Active IQ Unified Manager install packages

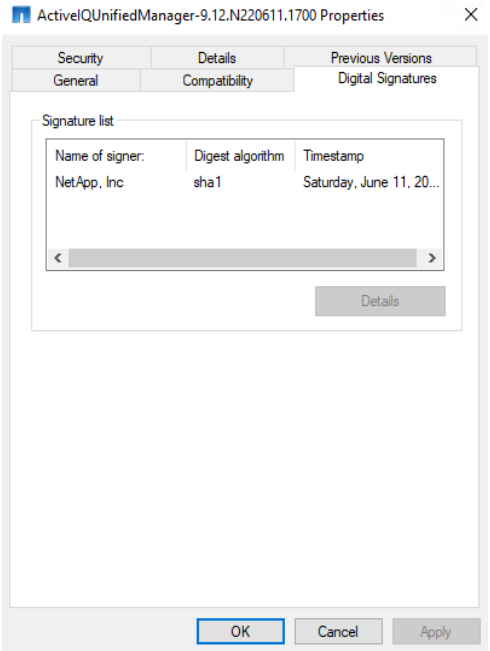
Customers can use two methods to verify the integrity of Active IQ Unified Manager install packages. They can verify the checksums and the signature of the install package.

Checksums can be found on the download page of Active IQ Unified Manager. Users must verify the checksums of downloaded packages against the checksum provided on the Active IQ Unified Manager Download Page.

Verifying the signature on Windows

Users should always verify the signature of the Windows application package executable (.exe) file after downloading it from the NetApp support site. To do so, right click on the .exe file and open properties. In the open properties window, select Digital Signatures; it should display Name of Signer as NetApp Inc as seen in Figure 1.

Figure 1) Verifying the signature on Windows



Verifying the signature on RHEL

Along with the product zip for Red Hat Enterprise Linux (RHEL), the code signing certificate is located on the product download page. From the code signing certificate, users can extract the public key as below:

```
#> openssl x509 -pubkey -noout -in netapp_cert.pem > pubkey.pem
```

Then public key is used to verify the signature for RPM product zip as below:

```
#> openssl dgst -sha256 -verify <public key> -signature <signature file>
<Binary>
example:
#> openssl dgst -sha256 -verify AIQUM-RHEL-public.key -signature
ActiveIQUnifiedManager-9.12.N220730.0329-el8.zip.sig ActiveIQUnifiedManager-
9.12.N220730.0329-el8.zip
Verified OK => response
```

Verifying the signature on vApp

The vApp install package comes in the form of a gzipped tar file. This tar file contains a root and intermediate certificate for a virtual appliance along with a README file and an Open Virtualization Appliance (OVA) package.

- While deploying a vApp (by using the OVA file, the digital signature for the vApp package can be verified on the Review Details page).
- If the downloaded vApp package is not tampered with, the Publisher column says Trusted certificate.
- If the downloaded vApp package is tampered with, the Publisher column says Invalid certificate.

You must upload the provided root and intermediate certificate on vCenter version 7.0U3E and higher. For vCenter versions between 7.0.1 and 7.0.U3E the functionality for verifying the certificate is not supported by VMware. You do not need to upload any certificate for vCenter versions 6.x.

Uploading the trusted root certificate to vCenter

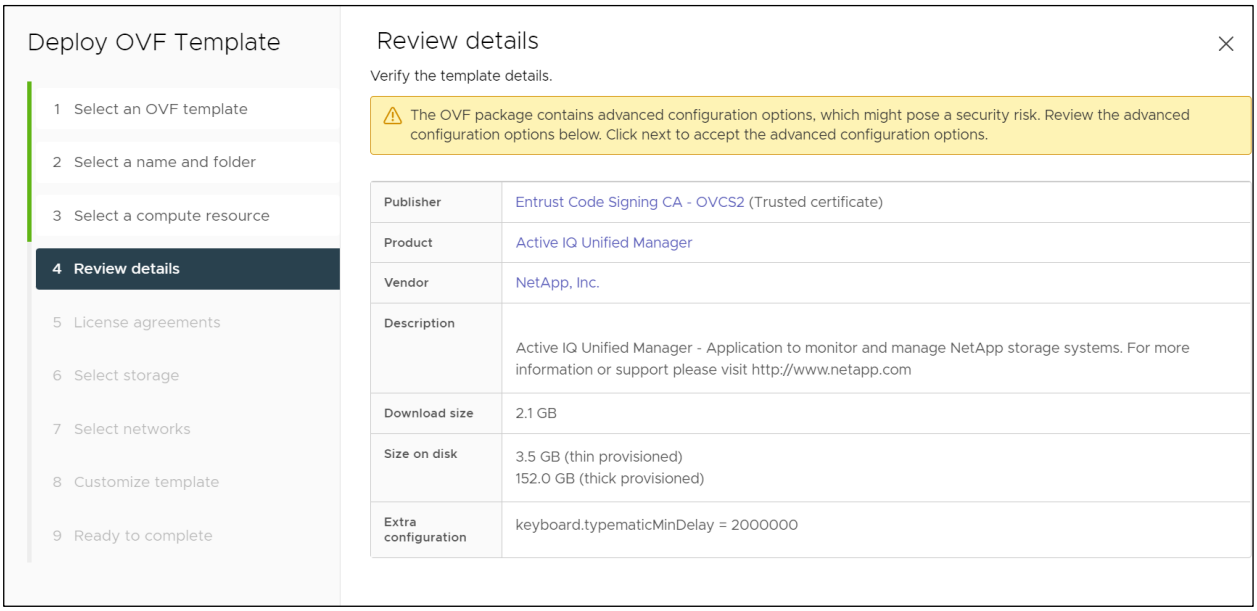
1. Log in with the vSphere Client to the vCenter Server.
2. Specify the username and password for administrator@vsphere.local or another member of the vCenter Single Sign-On Administrators group. If you specified a different domain during installation, log in as administrator@mydomain.
3. Navigate to the Certificate Management user interface.
   a. From the Home menu, select Administration.
   b. Under Certificates, click Certificate Management.
4. If the system prompts you, enter the credentials of your vCenter Server.
5. Under Trusted Root Certificates, click Add.
6. Click browse and select the location of the certificate .pem file (AIQUM-VAPP-INTER-ROOT-CERT.pem).
7. Click Add.

The certificate is added to the store.

Refer to the article Add a Trusted Root Certificate to the Certificate Store for more information.

While deploying a vApp (by using the OVA file), the digital signature for the vApp package can be verified on the Review details page. If the downloaded vApp package is genuine, the Publisher column says Trusted certificate as seen in Figure 2.

Figure 2) Verifying the signature on vApp



Ports and protocols

The required ports and protocols enable communication between a client and the Active IQ Unified Manager server and between Active IQ Unified manager and managed storage systems, servers, and other components.

Inbound and outbound ports required for Active IQ Unified Manager

The below tables list inbound and outbound ports required by Active IQ Unified Manager. Only the ports listed in Table 1 and Table 2 should be open for connections from remote machines. All other ports should be disabled for connections from remote machines.

Table 1) Inbound ports required for Active IQ Unified Manager

Interface	Protocol	Port
Unified Manager user interface	HTTP	80*
Unified Manager user interface and programs using APIs	HTTPS	443*
Maintenance console	SSH/SFTP	22
Linux command line	SSH/SFTP	22
Syslog	UDP	514
MySQL database	MySQL	3306**

* Default port, can be changed after installation

** By default, MySQL port 3306 is open for connections from localhost only. If you want to integrate Active IQ Unified Manager with OnCommand Workflow Automation (WFA) or want remote connection to a database, only then port 3306 should be open for connections from remote machines. Table 2 includes the outbound ports Active IQ Unified Manager require.

Table 2) Outbound ports required for Active IQ Unified Manager

Destination	Protocol	Port
Storage system	HTTPS	443/TCP
Storage system	NDMP	10000/TCP
AutoSupport server	HTTPS	443
Authentication server	LDAP	389
Authentication server	LDAPS	636
Mail server	SMTP	25

Changing HTTP and HTTPs ports

By default, Active IQ Unified Manager services use default HTTP and HTTPS ports 80 and 443 respectively.

Best practice

It is best security practice to run these services on non-default and non-privileged ports (port number higher than 1024). HTTP and HTTPs ports can be changed from the maintenance console as follows:

```
 [root@server bin]# maintenance_console
Active IQ Unified Manager Maintenance Console
Version: 9.12.N220531.1701-2205311701
System ID: dc006e8a-9273-4d61-870e-b76982afcb37
Status: Running
Main Menu

1 ) Support/Diagnostics
2 ) Reset Server Certificate
3 ) Backup Restore
4 ) External Data Provider
5 ) Performance Polling Interval Configuration
6 ) Disable SAML authentication
7 ) View/Change Application Ports
8 ) Debug Log Configuration
9 ) Control access to MySQL port 3306
x ) Exit
Enter your choice: 7
Maintenance console requires username & password to perform this
operation, enter administrator username & password when prompted.

Enter username: umadmin
Enter password:
Below are the application ports that can be changed, and their current values:
HTTP communication: 80
HTTPS communication: 443
Do you want to change the ports? (y/n): y
HTTP Port (Not specifying anything will set it to default 80): 7777
HTTPS Port (Not specifying anything will set it to default 443): 9999
This action will restart Active IQ Unified Manager.
Are you sure you want to change the application ports and restart Active IQ Unified Manager now?
(y/n): y
Stopping service 'Active IQ Unified Manager acquisition unit'
Stopped 'Active IQ Unified Manager acquisition unit' successfully
Stopping service 'Active IQ Unified Manager'
Stopped 'Active IQ Unified Manager' successfully
Starting service 'Active IQ Unified Manager'
Started 'Active IQ Unified Manager' successfully
Starting service 'Active IQ Unified Manager acquisition unit'
Started 'Active IQ Unified Manager acquisition unit' successfully
Active IQ Unified Manager service restart succeeded
```

```
The application ports have been changed successfully
Exit out of the maintenance console and then log back in
Press any key to continue.
Active IQ Unified Manager Maintenance Console
Version: 9.12.N220531.1701-2205311701
System ID: dc006e8a-9273-4d61-870e-b76982afcb37
Status: Running
```

Controlling remote access to MySQL port 3306

By default, MySQL port 3306 can be accessed only from localhost. The MySQL port should be open for remote connections only when you want to integrate Active IQ Unified Manager with WFA or you need to access the Active IQ Unified Manager database remotely.

Best practice

It is a security best practice to keep the MySQL port closed for remote connections. You can change this on RHEL and vApp from the maintenance console as follows:

```
[root@aiqum ~]# /opt/netapp/ocum/bin/maintenance_console
Active IQ Unified Manager Maintenance Console
Version : 9.12.N220531.1701-2205311701
System ID : dc006e8a-9273-4d61-870e-b76982afcb37
Status : Running
Main Menu

1 ) Support/Diagnostics

2 ) Reset Server Certificate
3 ) Backup Restore
4 ) External Data Provider
5 ) Performance Polling Interval Configuration
6 ) Disable SAML authentication
7 ) View/Change Application Ports
8 ) Debug Log Configuration
9 ) Control access to MySQL port 3306
x ) Exit
Enter your choice: 9
Maintenance console requires username & password to perform this
operation, enter administrator username & password when prompted.

Enter username: umadmin
Enter password:
The MySQL port 3306 is currently accessible only by localhost.
Do you wish to enable access to everyone? (y/n): y

The MySQL port 3306 is now accessible by everyone.
Active IQ Unified Manager Maintenance Console
Version : 9.12.N220531.1701-2205311701
System ID : dc006e8a-9273-4d61-870e-b76982afcb37
Status : Running
Main Menu

1 ) Support/Diagnostics

2 ) Reset Server Certificate
3 ) Backup Restore
4 ) External Data Provider
5 ) Performance Polling Interval Configuration
6 ) Disable SAML authentication
7 ) View/Change Application Ports
8 ) Debug Log Configuration
9 ) Control access to MySQL port 3306
x ) Exit
Enter your choice: x
[root@aiqum ~]#
```

Roles and users

Active IQ Unified Manager installation creates and uses three types of users:

1. System User
2. Application user i.e. local user
3. MySQL user or db user

System users

System users are the users created by Active IQ Unified Manager installation on an underlying operating system.

- A default system user “umadmin" is created on RHEL/CentOS by Active IQ Unified Manager installation. This user is a maintenance user and is created to execute the maintenance console scripts.
- A similar system user is created on vApp. The credentials for this user are entered by the user deploying vApp. This is a maintenance user and is created to execute the maintenance console script.
- System user “jboss” is created on RHEL and vApp to run Active IQ Unified Manager services. The 'jboss' user has limited permissions on RHEL and vApp to run Active IQ Unified Manager services.
- The maintenance user and “jboss” user on RHEL/CentOS and vApp have permission to execute a few scripts as root. These permissions for maintenance user and “jboss” user are defined in the /etc/sudoers.d/ocum_sudoers file and the /etc/sudoers.d/ocie_sudoers file.
- Files /etc/sudoers.d/ocum_sudoers and /etc/sudoers.d/ocie_sudoers are created during installation of Active IQ Unified Manager. These files are owned by the root and only have read permissions for the root user. Permissions for these files should not be changed.
- On Windows no system user is created by Active IQ Unified Manager installation. Active IQ Unified Manager services on Windows run as the local system account. The “Local System account” has the highest privileges on Windows OS.

Application user

An application user is named as a local user in Active IQ Unified Manager. These are users created in the Active IQ Unified Manager application. Table 3 lists the types of application users.

Table 3) Types of application users

User	Description
Maintenance User	It is created during the initial configuration of Unified Manager. The maintenance user then creates additional users and assigns roles. Unified Manager is installed on a Red Hat Enterprise Linux or CentOS system. The maintenance user is given the username “umadmin" and has a default password. Users should change this password before starting to use Active IQ Unified Manager. This is the only application user which is created by default.
Local User	Performs functions based on the role given by the maintenance user or a user with the Application Administrator role.
Remote Group	A group of users that access the Unified Manager user interface by using the credentials stored on the authentication server. All users within the remote group are given access to the Unified Manager user interface by using their individual user credentials.
Remote User	Accesses the Unified Manager user interface by using the credentials stored on the authentication server.

User	Description
Database User	Has read-only access to data in the Unified Manager database, has no access to the Unified Manager user interface or the maintenance console, and cannot execute API calls. There are two roles associated with database users: 1. Integration schema 2. Report Schema

The local users (application users) have a role associated with them. Table 4 list roles available in Active IQ Unified Manager for local user.

Roles

RBAC (role-based access control) provides the ability to control who has access to various features and resources in Active IQ Unified Manager. The RBAC solution in Active IQ Unified Manager limits users' administrative access to the level granted for their defined role, which allows administrators to manage local users by their assigned role. The local user accounts are static, and the assigned roles cannot be modified. Table 4 lists the predefined roles in Active IQ Unified Manager.

Table 4) Types of pre-defined roles

Role	Description
Operator	Views storage system information and other data collected by Unified Manager, including histories and capacity trends. This role enables the storage operator to view, assign, acknowledge, resolve, and add notes for the events.
Storage Administrator	Configures storage management operations within Unified Manager. This role enables the storage administrator to configure thresholds and to create alerts and other storage management-specific options and policies.
Application Administrator	Configures settings unrelated to storage management. This role enables the management of users, security certificates, database access, and administrative options, including authentication, SMTP, networking, and AutoSupport.
Integration Schema	This role enables read-only access to Unified Manager database views for integrating Unified Manager with OnCommand Workflow Automation (WFA). Users with this role are created in MySQL database and hence they are database users.

User types

A user type specifies the kind of account they have in Active IQ Unified Manager. Each of these types has its own role, which is assigned by a user with the role of Administrator. Active IQ Unified Manager local users can have three roles: Application Administrator, Storage Administrator and Operator. Table 4 explains these roles.

Best practice
It is a security best practice to select the role of the user by using the principle of least privilege.

The users with Integration Schema and Report Schema roles are created in MySQL database. They are known as database users. These users can connect to the MySQL database from remote machines if the MySQL port is open for connections from remote machines. You might not need to create these users; they should only be created when required.

Locking and unlocking an Active IQ Unified Manager application user

An inactive user account poses a security risk to organizations. An inactive account offers an opportunity to a malicious actor to gain access to resources. Active IQ Unified Manager provides a feature to lock or unlock user accounts. Inactive user accounts should be locked. Users with an Application Administrator role can lock or unlock an account.

To lock/unlock a user account, open `Settings -> General` in the menu on the left, then select `Users`. The users page provides an option to lock/unlock user accounts.

Mutual TLS (Certificate Based Authentication)

Starting with ONTAP 9.12, Active IQ Unified Manager uses mutual Transport Layer Security (TLS) for communicating with ONTAP for any new cluster added in ONTAP 9.12. If you upgraded from previous versions of Active IQ Unified Manager, you can enable mutual TLS by editing the cluster properties.

As in the below screenshot, the Cluster setup page shows the status of mTLS (mutual transport layer security) configured for each cluster.

Figure 3) Certificate based authentication status.

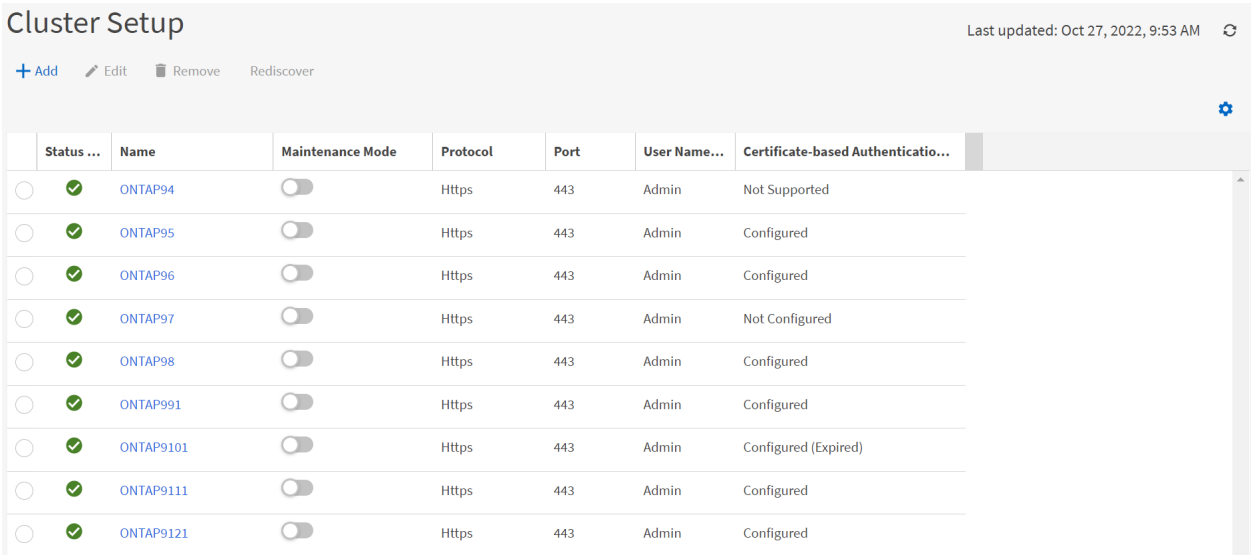


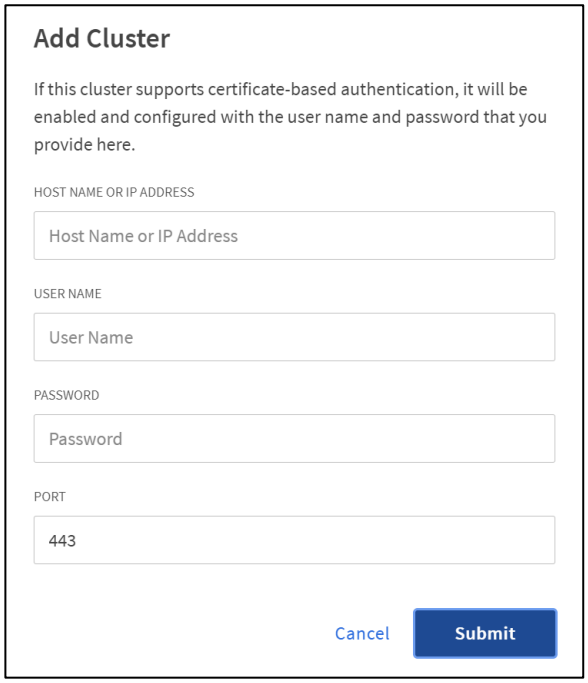
Figure 3 shows four different statuses for certificate-based authentication:

1. **Configured:** mTLS is configured and being used for authentication between Active IQ Unified Manager and ONTAP.
2. **Not Configured:** This is the case when user have upgraded from previous versions of Active IQ Unified Manager and mTLS is yet not configured for this cluster. This can be configured by editing cluster properties.
3. **Not Supported:** ONTAP version is less than 9.5, which does not support mTLS.
4. **Configured (Expired):** Certificate for mTLS is expired.

Cluster add

During a cluster add workflow, if the cluster being added supports mTLS, mTLS is configured by default. No configuration is necessary. Below in Figure 4 is a screen shot of the cluster add.

Figure 4) Add cluster dialogue



Cluster edit

During a cluster edit operation, you might be presented with three different types of screens. This depends on whether mTLS is enabled or the ONTAP cluster supports it.

1. **MTLS Supported and Enabled -** No changes for mTLS when you click on the submit button.
2. **MTLS Supported but not Enabled -** In this case mTLS is enabled when you click on the submit button.
3. **MTLS not supported -** No changes for mTLS when you click the submit button.

Active IQ Unified Manager HTTPS certificate

By default, Active IQ Unified Manager uses a self-signed certificate automatically created during installation for securing HTTPS access to the user interface. Active IQ Unified Manager provides the following features to:

1. Download a HTTPS certificate signing request
2. Install a HTTPS certificate
3. Regenerate a HTTPS certificate

The above options can be accessed in the left pane by navigating to `Settings → General → https Certificate`. Using these features, you can “download https certificate signing request” and once the certificate is signed by a CA it can be installed on the Active IQ Unified Manager server using the “Install https certificate” option. You can use the "regenerate https certificate" option for modifying the self-signed certificate generated at the time of installation. This can be done before creating a certificate signing request as well.

Best practice

It is security best practice to use a CA signed certificate for an Active IQ Unified Manager server. The required steps are described here: [How to generate and convert a signed certificate for Active IQ Unified Manager.]

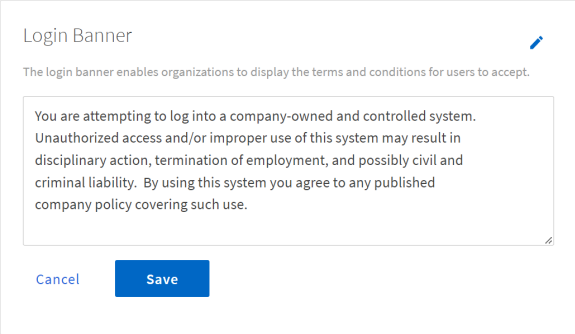
Login banner

The login banner is displayed when you log in to the Active IQ Unified Manager user interface. The login banner enables organizations to display the terms and conditions for its users.

Best practice

By default, the login banner is set to empty. It is security best practice to set the login banner. To configure the login banner, navigate to `Settings -> General -> Feature Settings` and `Login Banner` as seen in Figure 5.

Figure 5) Configuring the login banner.



Inactivity timeout

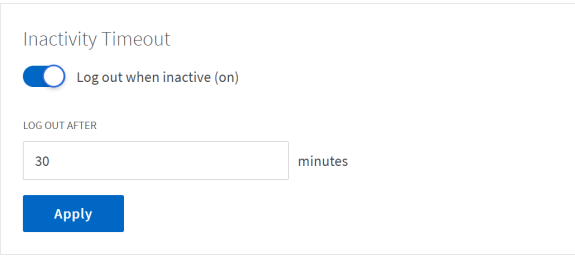
The user interface of Unified Manager has a timeout which logs you out and closes the session after the given inactivity time. This option is enabled by default.

Best practice

The default inactivity timeout for the user interface for Active IQ Unified Manager is three days. It is security best practice to shorten this to 30 minutes or less.

To modify the inactivity timeout, navigate to `Settings -> General -> Feature Settings` and modify the inactivity timeout in minutes and click the Apply button.

Figure 6) Modifying the inactivity timeout.



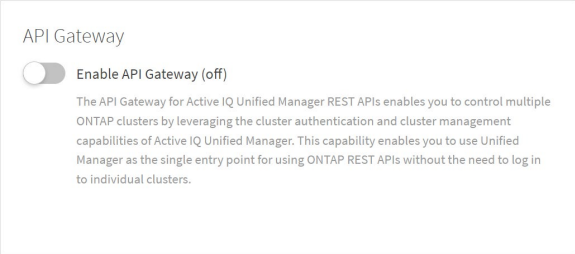
API Gateway

The API Gateway feature in Active IQ Unified Manager allows you to use the ONTAP REST API of a cluster without directly logging in to the ONTAP cluster. Instead the Unified Manager REST API is used to forward API requests to the ONTAP cluster by using the credentials stored in Unified Manager.

Best practice

If the API Gateway feature is not used in Active IQ Unified Manager, it should be disabled. To disable the API Gateway, navigate to `Settings -> General -> Feature Settings` and switch `Enable API Gateway` to `off`.

Figure 7) Disable the API gateway feature.



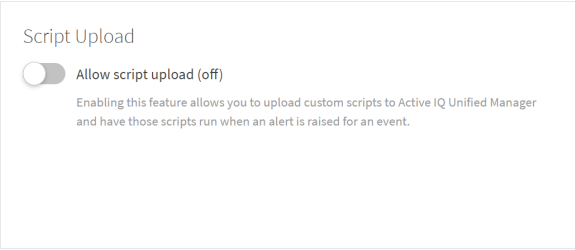
Script upload

Active IQ Unified Manager allows you to run a custom script as an alert action.

Best practice

It is security best practice to disable the script upload capability if it is not being used, navigate to `Settings -> General -> Feature Settings` and switch `Script Upload` to `off` as seen in Figure 8.

Figure 8) Disable script upload.



Maximum concurrent sessions per user

By default, the number of maximum concurrent sessions per user is 100. A user with an Application Administrator role in Active IQ Unified Manager can change this value depending on the requirement for their environment.

Best Practice

It is security best practice to keep the maximum concurrent sessions low as a high value provides a mechanism for DOS or distributed denial of service (DDoS) attacks.

You can change the number of maximum concurrent sessions by using the below commands.

```
# um option list maximum.concurrent.user.session
Name Default Value Value Requires Restart
-------------- -------------- -------------- --------------
maximum.concurrent.user.session 100 100 true
# um option set maximum.concurrent.user.session=500
Changed maximum.concurrent.user.session to 500.

# um option list maximum.concurrent.user.session
Name Default Value Value Requires Restart
-------------- -------------- -------------- --------------
maximum.concurrent.user.session 100 500 true
```

Rate limiting

Rate limiting provides a mechanism against DOS/DDOS attacks. You can rate limit per source IP address for new connections through the OS firewall, which can help lessen the impact of malicious attacks.

RHEL

In RHEL, you can configure a rate limiter through an iptables command. The below command is used to rate limit new connections with an 'n' request per second.

```
iptables -A INPUT -m conntrack --ctstate NEW -m hashlimit --hashlimit-above 10/sec --hashlimit-
burst 5 --hashlimit-mode srcip --hashlimit-name conn-rate-limit -j DROP
```

Using the iptables command

The system allows an average of 10 requests per second with an initial burst of five requests for a unique source IP. Requests above the threshold value are dropped.

vApp

In vApp, by default an IP table with a rate limiter is pre-configured to 10 requests per second. If you need to modify it, Login to vAPP with a diagnostic shell and follow the instructions in the following NetApp Knowledge Base article: How to update Rate Limit in vApp of Active IQ Unified Manager.

Note: The diagnostic shell can execute OS-level commands; you should only use it when directed by technical support.

Windows

Windows does not support the rate limiting feature for their firewalls. You need to install a third-party tool to configure the rate limiter per source IP.

Cryptographic settings

You can disable some of the default ciphers used by Active IQ Unified Manager. To do so, go to `Settings → General → Manage HTTPs cipher Suites` on the Active IQ Unified Manager interface. However, it is recommended to keep all the default ciphers supported for optimum user interface support on all the browsers.

Certificate based SSH and RDP to Active IQ Unified Manager systems

It is good security practice to login to machines where Active IQ Unified Manager is installed, by using certificate based Secure Shell (SSH) or Remote Desktop Protocol (RDP).

Windows: If you have installed Active IQ Unified Manager on a Windows machine, certificate-based RDP should be used for enhanced security. Please follow Microsoft's instructions in the Using certificates in Remote Desktop Services article for configuring certificate based RDP to Windows machines.

vApp: Active IQ Unified Manager maintenance users can login to vApp through SSH. Customers can configure certificate based SSH to Active IQ Unified Manager vApp for added security. For configuring certificate based SSH, you should login to DIAG shell by following the steps in the How to access Active IQ Unified Manager Virtual Machine (OVA) DIAG shell article. All the commands on the DIAG shell must be run using sudo, otherwise users will hit a permission denied issue. Please follow Debian docs for configuring certificate based SSH on vApp.

Note: On vApp only, one user (the maintenance user) can login via SSH. Care must be taken while configuring certificate based SSH. If certificate based SSH is misconfigured it may result in getting locked out of the vApp. .

RHEL/CentOS: Root and other system users can login to the RHEL system for performing Active IQ Unified Manager related operations and/or for normal system maintenance and operations. It is good security practice to use certificate based SSH on Linux machines. Please follow RHEL documentation Using OpenSSH Certificate Authentication for configuring certificate based SSH on RHEL.

Regenerating SSH Fingerprint

While certificates expire after their validity period, if you are using password based SSH, you must regenerate your SSH fingerprint periodically. Users should follow Debian/RHEL/CentOS documentation on how to regenerate SSH fingerprints.

Configuring Network Time Protocol (NTP)

Out of sync NTP network time can sometimes cause security issues.

vApp

You can configure the NTP server from the maintenance_console in vApp.

By default, the service for NTP is ntpd on vApp. This is a legacy service and does not work well for virtual machines in certain cases. You can switch to the "systemd-timesyncd" service for NTP. Systemd-timesyncd is a client only lightweight implementation of the NTP protocol. Users can switch to systemd-timesyncd from the maintenance console by selecting "system config" and then the "change ntp service" option.

RHEL and Windows

Please follow the OS's standard procedure and best practices to configure the NTP service.

On RHEL, customers can use chrony for the ntp service, which offers many improvements over the legacy ntpd service.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- Active IQ Unified Manager Documentation
  https://docs.netapp.com/us-en/active-iq-unified-manager/
- Active IQ Unified Manager Resources
  https://www.netapp.com/support-and-training/documentation/active-iq-unified-manager/

Version history

Version	Date	Document version history
Version 1.0	Nov 2022	Initial document release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright information

Trademark information

TR-4943-1122

NetApp