CHAPTER 4

Getting Started with Application Networking Manager

Date: 1/9/13

This chapter describes how to set up your Cisco Application Networking Manager (ANM) server. After completing the procedures in this chapter, ANM is ready for you to import network devices to monitor and manage. For details about using ANM, including how to import network devices, see the *User Guide for the Cisco Application Networking Manager 4.2*.

This chapter includes the following sections:

Acquiring and Uploading a Cisco Application Networking Manager License

You must have an ANM license before you can use ANM. Before you can install an ANM license, you must be a registered Cisco.com user and you must have the service license authorization key (PAK) that was shipped with your software CD. For more information, see the "Understanding ANM License Information" section in the "Administering the Cisco Application Networking Manager" chapter of the online help or the *User Guide for the Cisco Application Networking Manager 4.2*.

Note The license installation script reinitializes ANM. If you have performed an HA upgrade, it may also take some time for the system to determine which host is the active host. It may take several minutes before you can log in to ANM after the installation or upgrade.

Procedure

Step 1 From Cisco.com, go to http://www.cisco.com/go/license. You will be asked to log into Cisco.com. If you are not a registered user you will be given a number of options including the option to log in without registering. Once logged in, you will be prompted to enter the product authorization key (PAK).

Step 2 Enter the product authorization key (PAK) exactly as it appears on the label that accompanied the Cisco Information Packet. If you are unable to locate the PAK, contact your Cisco support team or click on the link for a demonstration license.

Note A demo license is valid for 90 days after it is issued. After 90 days, the product will require a standard license.

Step 3 Follow the instructions for registration on the license website. After you finish registering, you will receive a message that confirms your registration, and an e-mail that contains the license/key file will be sent to you at the e-mail address that you provided during product registration.

Step 4 After you receive your software license key by e-mail, save the e-mail and the license file (.lic) that is attached to the e-mail to a temporary directory on your hard drive for safekeeping.

Step 5 (Optional) Copy the file from the temporary directory to your ANM server.

Step 6 From the command line, install the license on the ANM server by entering the following command:

/opt/CSCOanm/bin/anm-license install /*path/ANMxxxxxxxxxxxxxxxx.lic*

Where *path* is the location of the license file and *ANMxxxxxxxxxxxxxxxx.lic* is the name of the license file.

You can install either ANM-DEMO or ANM-SERVER-XX license.

Step 7 Log in to ANM and under the Administration tab, choose **ANM Management > License Management** to make sure you can see ANM-SERVER-XX license.

Note For more information about licenses, see the "Managing Cisco Application Networking Manager Licenses" section on page 4-6.

Uploading Site-Specific Certificate/Key Pair Files for Server Authentication

This section describes how to install a third party certificate/key pair that is used to authenticate your ANM server. The ANM software installation process includes a self-signed certificate/key pair for this purpose; however, you can choose not to use it by installing a third party certificate/key pair.

Caution Installing a third party certificate/key pair overwrites the self-signed certificate/key pair included with the ANM software. There is no documented way to revert to the self-signed certificate/key pair after you install a third party certificate/key pair.

Guidelines and Restrictions

This topic includes the following guidelines and restrictions:

- You can install a third party certificate/key pair at any time, not just during the installation of ANM.
- In HA mode, you must perform this procedure on both ANM servers.

Procedure

Step 1 If necessary, copy the certificate and key pair files from the temporary directory to your ANM server.

Step 2 From the command line, install the certificate and key pair by entering the following command:

/opt/CSCOanm/bin/anm-certificate install *certificate key* **[***key-password***]**

Where *certificate* is the name of the certificate file that you are installing, *key* is the name of the certificate key pair file, and the optional *key-password* is the key password, which is required only if the key is encrypted.

Logging In To Cisco Application Networking Manager

You access ANM features and functions through a web-based interface. The ANM login window allows you to log into the ANM server, change the password for your account, and obtain online help by clicking **Help**.

Procedure

Step 1 Log in to ANM by doing one the following:

- To log in after a new installation, in your browser address field, enter **https://***host* or **http://***host* depending on whether or not you enabled non-SSL HTTP during the installation of ANM.

Note You can omit the port numbers from the URL because ANM uses the default web ports for HTTP and HTTPS, which are 80 and 443 respectively.

Caution If you want to log in using HTTP, you will need to change the properties file. See the "Table 4-1 describes the available ANM licenses." section on page 4-6 for more information. Remember, if you enable HTTP, you are making your connection to ANM less secure.

- To log in after an upgrade, in your browser address field, enter: **https://***host***:10443** or **http://***host***:10080** depending on which port was enabled in the previous release. An upgrade uses the user specified web ports of 10443 and 10080; you must explicitly enter these port numbers.

Note All browsers require that you enable cookies, JavaScript/scripting, Adobe Flash Player 9, and popup windows. If you reinstall a later ANM release, make sure that you delete the cookies and clear the browser cache.

For example, enter **https://192.168.10.10**. The login window appears.

The username is "admin" by default and password is given by the user during installation.

Note The ANM 4.2 client supports use with Firefox 3.6 on Windows XP or Windows Vista. When you use Firefox 3.x to log in and access ANM for the first time, the Firefox web browser displays a warning that the site is untrusted. When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from the ANM server. After you complete this procedure, Firefox accepts the ANM server as a trusted site both now and during all future login attempts. See the "Using the Firefox Web Browser to Access ANM 4.2" section on page 4-5 for details.

Step 2 In the User Name field, enter **admin**.

The admin account was created when ANM was installed. After you log in, you can create additional user accounts. For more information about setting up user accounts, see the *User Guide for the Cisco Application Networking Manager 4.2*.

Step 3 In the Password field, enter the password that you used for installing ANM**.**

Step 4 Click **Login**.

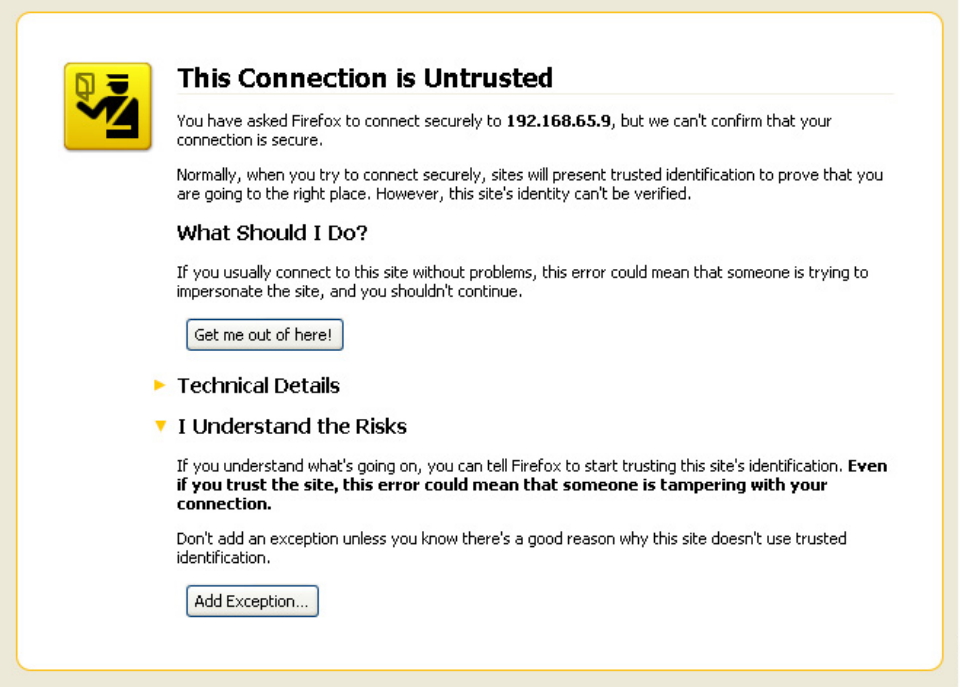
Caution ANM installation takes 90 seconds for initialization to be completed. When the login window appears, make sure that you wait at least 90 seconds before you log in. Failure to wait a minimum of 90 seconds may result in an error.

When you log in, the default page that appears is the ANM Homepage. You can choose the default page that you access after logging in to ANM. By default, the ANM Homepage is the first page that appears after you log in. From the ANM Homepage, you can specify a different page that appears as the default page after you log in. See the *User Guide for the Cisco Application Networking Manager 4.2* for details, including how to use ANM to import and manage your network devices.

Using the Firefox Web Browser to Access ANM 4.2

The ANM 4.2 client supports use with Firefox 3.6 on Windows XP or Windows Vista. When you use Firefox 3.6 or later to log in and access ANM for the first time, the Firefox web browser displays a warning that the site is untrusted (Figure 4-1).

Figure 4-1 Firefox 3.6 Untrusted Connection Warning



When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from the ANM server. After you complete this procedure, Firefox accepts the ANM server as a trusted site both now and during all future login attempts.

Procedure

Step 1 In the This Connection Is Untrusted window, click **I Understand the Risks**.

Step 2 Click **Add Exception** to add a security exception to the Firefox web browser.

The Add Security Exception popup window appears identifying the location of the ANM server.

Step 3 In the Add Security Exception popup window, click **Get Certificate**.

Firefox retrieves the ANM self-signed certificate and the window's Confirm Security Exception button becomes active.

Step 4 Click **Confirm Security Exception**.

Firefox recognizes the ANM server as a trusted site and the ANM Login window appears.

Managing Cisco Application Networking Manager Licenses

ANM licenses are available at no charge. When you install the ANM server license software, you also need to install an ANM license from the command line before you can access ANM.

For information about viewing and managing ANM licenses after installing ANM, see the "Using ANM License Manager to Manage ANM Server or Demo Licenses" section in the *User Guide for the Cisco Application Networking Manager 4.2* or in the online help.

Table 4-1 describes the available ANM licenses.

Table 4-1 ANM Licence Descriptions

License Name	Description
ANM-DEMO or DEMO	Used for demonstration purposes. It lasts for 90 days from the issue day of the license and allows you to use all features.
ANM-SERVER-40-K9	Used to allow access to the ANM server. Beginning with ANM 4.1, ANM does not perform a license version number check; it will accept any version ANM license.

For instructions on uploading your ANM server license, see the "Acquiring and Uploading a Cisco Application Networking Manager License" section on page 4-1.

Changing Configuration Attributes After Installing Cisco Application Networking Manager

You can modify the ANM server software configuration attributes that you specified when installing the software, such as:

- HTTP Port of Web Services
- Enable HTTP for Web Services
- HTTPS Port of Web Services
- Enable HTTPS for Web Services
- Idle session timeout in msec

For details about modifying the software configuration, see the "Changing ANM Configuration Property Values" section in the *User Guide for the Cisco Application Networking Manager 4.2* or the ANM online help. This section also contains configuration examples.

Example ANM Standalone Configuration Session

The following is an example of a configuration session for an ANM standalone system.The values shown in the brackets are the currently configured values.

```
/opt/CSCOanm/bin/anm-tool configure
Configuring ANM

Checking ANM configuration files
  Keep existing ANM configuration? [y/n]: n
  Creating config file (/opt/CSCOanm/etc/cs-config.properties)
```

```
Enable HTTP for Web Server [true]:
Inbound Port for HTTP traffic to ANM Default [80]:
Enable HTTPS for Web Server [true]:
Inbound Port for HTTPS traffic to ANM Default [443]:

These are the values:
Enable HTTP for Web Server: true
Inbound Port for HTTP traffic to ANM Default: 80
Enable HTTPS for Web Server: true
Inbound Port for HTTPS traffic to ANM Default: 443

Commit these values? [y/n/q]: y
Committing values ... done
  Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt

Stopping services
  Stopping monit services (/etc/monit.conf) ...   (0)
  Stopping monit ...  Stopped
  Stopping heartbeat ...  Stopped

Installing system configuration files
  Backing up //opt/CSCOanm/etc/my-local.cnf

Setting service attributes
  Enabling mysql for SELinux
setsebool:  SELinux is disabled.
  Service monit is started by OS at boot time

Starting mysql ... Started
mysql status ... Ready

Configuring mysql
  Checking mysql user/password
  Setting mysql privileges
  Disabling mysql replication

Starting services
  Starting monit ...Starting monit daemon with http interface at [*:2812]
  Started
```

Example ANM HA Configuration Session

The following is an example of a configuration session for an ANM HA system. Standalone systems will not contain any HA properties but will include a limited property value configuration. The values shown in the brackets are the currently configured values.

```
/opt/CSCOanm/bin/anm-tool configure
Configuring ANM

Checking ANM configuration files
Keep existing ANM configuration? [y/n]: n
Creating config file (/opt/CSCOanm/etc/cs-config.properties)

Enable HTTP for Web Server [false]: true
Inbound Port for HTTP traffic to ANM Default [80]: 80
Enable HTTPS for Web Server [true]:
Inbound Port for HTTPS traffic to ANM Default [443]:
Database Password [nI4ewPbmV51S]: passme
HA Node 1 UName []: anm49.cisco.com
```

```
HA Node 2 UName []: anm50.cisco.com
HA Node 1 Primary IP [0.0.0.0]: 10.77.240.126
HA Node 2 Primary IP [0.0.0.0]: 10.77.240.100
HA Node 1 HeartBeat IP [0.0.0.0]: 10.10.10.1
HA Node 2 HeartBeat IP [0.0.0.0]: 10.10.10.2
HA Virtual IP [0.0.0.0]: 10.77.240.101
HA Node ID [1 or 2] []: 1

These are the values:
Enable HTTP for Web Server: true
Inbound Port for HTTP traffic to ANM Default: 80
Enable HTTPS for Web Server: true
Inbound Port for HTTPS traffic to ANM Default: 443
Database Password: passme
HA Node 1 UName: anm49.cisco.com
HA Node 2 UName: anm50.cisco.com
HA Node 1 Primary IP: 10.77.240.126
HA Node 2 Primary IP: 10.77.240.100
HA Node 1 HeartBeat IP: 10.10.10.1
HA Node 2 HeartBeat IP: 10.10.10.2
HA Virtual IP: 10.77.240.101
HA Node ID [1 or 2]: 1


Commit these values? [y/n/q]: y
Committing values ... done
Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt

Stopping services
Stopping monit services (/etc/monit.conf) ...   (0)
Stopping monit ...  Stopped
Stopping heartbeat ...  Stopped

Installing system configuration files

Setting service attributes
Enabling mysql for SELinux
Service monit is started by OS at boot time

Starting mysql ... Started

Configuring mysql
Checking mysql user/password
Setting mysql privileges
Enabling mysql replication
Setting up database
executing /opt/CSCOanm/lib/install/etc/dcmdb.sql ...  done

Starting services
Starting monit ... Started
```

Example ANM Advanced Options Configuration Session

The following is an example of a configuration session for an ANM advanced options.The values shown in the brackets are the currently configured values.

```
/opt/CSCOanm/bin/anm-tool --advanced-options=1 configure
Configuring ANM
Checking ANM configuration files
  Keep existing ANM configuration? [y/n]: n
```

```
  Creating config file (/opt/CSCOanm/etc/cs-config.properties)

Enable HTTP for Web Server [false]:
Inbound Port for HTTP traffic to ANM Default [80]:
Enable HTTPS for Web Server [true]:
Inbound Port for HTTPS traffic to ANM Default [443]:
HTTP Port of Web Services [8080]:
Enable HTTP for Web Services [false]:
HTTPS Port of Web Services [8443]:
Enable HTTPS for Web Services [false]:
Idle session timeout in msec [1800000]:
Change the memory available to ANM process [low|high] [low]:

These are the values:
Enable HTTP for Web Server: false
Inbound Port for HTTP traffic to ANM Default: 80
Enable HTTPS for Web Server: true
Inbound Port for HTTPS traffic to ANM Default: 443
HTTP Port of Web Services: 8080
Enable HTTP for Web Services: false
HTTPS Port of Web Services: 8443
Enable HTTPS for Web Services: false
Idle session timeout in msec: 1800000

Change the memory available to ANM process [low|high]: low
Commit these values? [y/n/q]: y
Committing values ... done
  Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt
Stopping services
  Stopping monit services (/etc/monit.conf) ...   (0)
```

ANM Ports Reference

ANM uses specific ports for its processes. Figure 4-2 illustrates a typical ANM server deployment in a network. This illustration identifies the protocols and ports used by the different network devices in a typical deployment.

- Table 4-2 lists the ports used for ANM client (browser) or ANM server and ANM high availability communication.
- Table 4-3 lists the ports used for communication between ANM and managed devices.

Figure 4-2 ANM Server Deployment

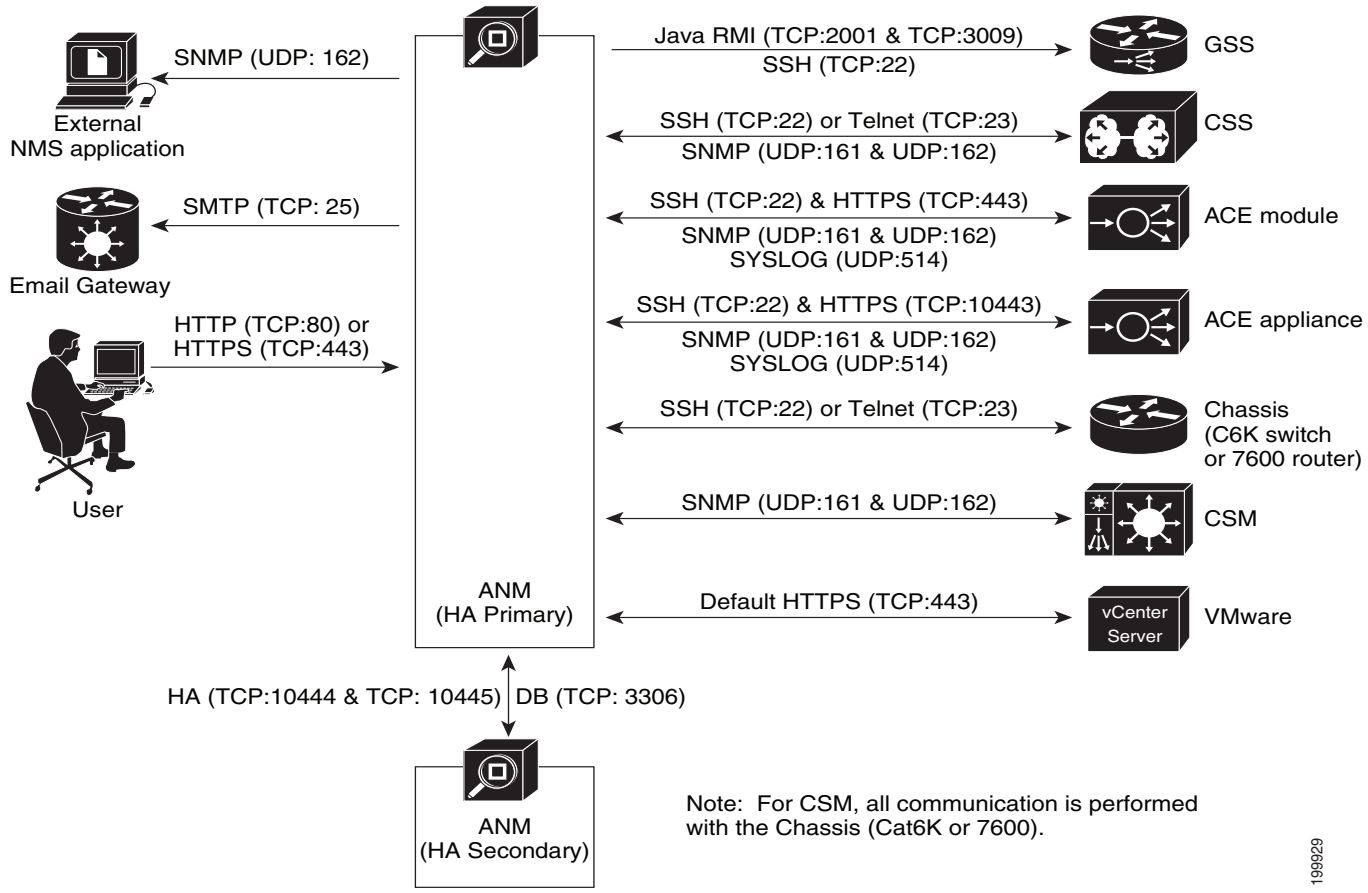


Table 4-2 Ports Used by ANM in a Network Deployment[1]

Port	Description
TCP (80)	Default port if ANM is configured for access using HTTP (using anm-installer).
TCP (443)	Default port if ANM is configured for access using HTTPS (using default install option).
TCP (3306)	MySQL Database system (ANM HA installation opens this port to communicate with the peer ANM).
TCP (10444) and TCP (10445)	ANM License Manager (ANM HA installation opens these two ports to communicate with the peer ANM).
TCP (25)	Port used by ANM server to communicate to Email Gateway through SMTP.
UDP (162)	Port used by ANM server to send out trap notification to external NMS application.
HTTPS (8443) or HTTP (8083)	The web service ports used by ANM Web Service North-Bound API.

1. It is highly recommended that you run ANM on a stand-alone device. However, if you run ANM on a shared device, please note that ANM locally opens the following ports for internal communication:

   TCP Ports: 8980, 10003, 10004, 10023, 10443, 40000, 40001, 40002, 40003
   UDP Ports: 6120, 10003

Table 4-3 Ports Used by ANM for Communication with Managed Devices

Device Type	Port	Description
Chassis (Catalyst 6500 switch or Cisco 7600 router)	SSH (TCP:22) or Telnet (TCP:23)	Discover chassis configuration.
ACE (appliance or module)	HTTPS (TCP:443)	For ACE module: XML/HTTPS interface on the device used to discover, configure, and monitor using specific **show** CLI commands.
	HTTPS (TCP:10443)	For ACE appliance: XML/HTTPS interface on the device used to discover, configure, and monitor using specific **show** CLI commands.
	SSH (TCP: 22)	Discovery and configuration of ACE licenses, certificates/keys (crypto) licensing, scripts, and checkpoints.
	SNMP (UDP: 161 & UDP:162)	Monitor ACE through SNMP requests (UDP: 161) and receive trap notifications (UDP: 162).
CSM	SNMP (UDP: 161 & UDP:162)	Monitor CSM through SNMP requests (UDP: 161) and receive trap notifications (UDP: 162).

Table 4-3 Ports Used by ANM for Communication with Managed Devices (continued)

Device Type	Port	Description
CSS	SSH (TCP:22) or Telnet (TCP:23)	Discover chassis configuration.
	SNMP (UDP: 161 & UDP:162)	Monitor CSS through SNMP requests (UDP: 161) and receive trap notifications (UDP: 162)
GSS	SSH (TCP:22)	Discover chassis configuration and monitoring operational status of DNS rules and VIP answers.
	RMI (TCP:2001 & TCP:3009)	Activate/suspend DNS rules and VIP answers.
VMware vCenter Server	HTTPS (TCP:443)	ANM communicates with the vCenter Server and vSphere Client using HTTPS and default port 443, if you are using the plug-in that is available to integrate ANM with a VMware virtual data center environment. **Note** For more information about using ANM with VMware, see the *User Guide for the Cisco Application Networking Manager 4.2*.