Configure the ASAv

The ASAv deployment pre-configures ASDM access. From the client IP address you specified during deployment, you can connect to the ASAv management IP address with a web browser. This chapter also describes how to allow other clients to access ASDM and also how to allow CLI access (SSH or Telnet). Other essential configuration tasks covered in this chapter include the license installation and common configuration tasks provided by wizards in ASDM.

Start ASDM

Procedure

1. On the PC that you specified as the ASDM client, enter the following URL:

   https://*asa_ip_address***/admin**

   The ASDM launch page appears with the following buttons:

   - **Install ASDM Launcher and Run ASDM**
   - **Run ASDM**
   - **Run Startup Wizard**

2. To download the Launcher:

   a. Click **Install ASDM Launcher and Run ASDM**.

   b. Leave the username and password fields empty (for a new installation), and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. Note: If you enabled HTTPS authentication, enter your username and associated password.

   c. Save the installer to your PC, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

   d. Enter the management IP address, leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

3. To use Java Web Start:

   a. Click **Run ASDM** or **Run Startup Wizard**.

   b. Save the shortcut to your PC when prompted. You can optionally open it instead of saving it.

   c. Start Java Web Start from the shortcut.

d. Accept any certificates according to the dialog boxes that appear. The Cisco ASDM-IDM Launcher appears.

e. Leave the username and password blank (for a new installation), and then click **OK**. Note: If you enabled HTTPS authentication, enter your username and associated password.

Configure Additional Management Access

If you want to finish your configuration at the CLI or from a different ASDM management station, you can use ASDM to configure SSH, Telnet, and ASDM access.

Procedure

1. In ASDM, choose **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**, and click **Add**.

   The **Add Device Access Configuration** dialog box appears.

2. Choose the type of session from the three options listed: **ASDM/HTTPS**, **Telnet**, or **SSH**.
3. From the **Interface Name** drop-down list, choose the interface to use for administrative access.
4. In the **IP Address** field, enter the IP address of the network or host that is allowed access.
5. From the **Mask** drop-down list, choose the mask associated with the network or host that is allowed access.
6. Click **OK**.
7. Configure **HTTP Settings**.

   a. **Enable HTTP Server**—Enable the HTTP server for ASDM access. This is enabled by default.

   b. (Optional) **Port Number**—The default port is 443.

   c. (Optional) **Idle Timeout**—The default idle timeout is 20 minutes.

   d. (Optional) **Session Timeout**—By default, the session timeout is disabled. ASDM connections have no session time limit.

   e. (Optional) **Require client certificate to access ASDM on the following interfaces**—Specify the interface from the drop-down list.

8. (Optional) Configure **Telnet Settings**.

   – **Telnet Timeout**—The default timeout value is 5 minutes.

9. (Optional) Configure **SSH Settings**.

   a. **Allowed SSH Version(s)**—The default value is 1 & 2.

   b. **SSH Timeout**—The default timeout value is 5 minutes.

   c. **DH Key Exchange**—Click the applicable radio button to choose Diffie-Hellman (DH) Key Exchange Group 1 or Group 14. Both the DH Group 1 and Group 14 key-exchange methods for key exchange are supported on the ASA. If no DH group key-exchange method is specified, the DH group 1 key-exchange method is used. For more information about using DH key-exchange methods, see RFC 4253.

10. Click **Apply**.

    The changes are saved to the running configuration.

11. (Required for Telnet) Set a login password before you can connect with Telnet; there is no default password.

a. Choose **Configuration > Device Setup > Device Name/Password**.

b. In the **Telnet Password** area, check the **Change the password to access the console of the security appliance** checkbox.

c. Enter the old password (for a new ASA, leave this field blank), new password, and then confirm the new password.

d. Click **Apply**.

12. (Required for SSH) Configure SSH user authentication.

a. Choose **Configuration > Device Management > Users/AAA > AAA Access > Authentication**.

b. Check the **SSH** check box.

c. From the **Server Group** drop-down list, choose the **LOCAL** database. You can alternatively configure authentication using a AAA server.

d. Click **Apply**.

e. Add a local user. Choose **Configuration > Device Management > Users/AAA > User Accounts**, and then click **Add**.

The **Add User Account-Identity** dialog box appears.

a. Enter a username and password, and then confirm the password.

b. Click **OK,** then click **Apply**.

Apply the ASAv License

After you deploy the ASAv, you must install a model license.

Until you install a license, throughput is limited to 100 Kbps so that you can perform preliminary connectivity tests. A license is required for regular operation. You also see the following messages repeated on the console until you install a license:

```
Warning: ASAv platform license state is Unlicensed.
Install ASAv platform license for full functionality.
```

CLI License Procedure

Procedure

1. In the ASAv console, view and note the serial number by entering the following command:

```
ciscoasa# show version | grep Serial
```

For example:

```
ciscoasa# show version | grep Serial
Serial Number: VBXQEFMXX44
ciscoasa#
```

2. Obtain a Product Authorization Key, which you can purchase from your Cisco account representative. You need to purchase a separate Product Authorization Key for each feature license. For the ASAv, the only required feature license is for CPUs (1 to 4), but you can purchase other feature keys as well.

3. Request an activation key from Cisco.com for the serial number according to the ASA licensing guide. Be sure to request a CPU license that matches the number of CPUs you specified when you deployed the ASAv.
4. After you receive the activation key from Cisco, at the ASAv console, apply the key:

   ```
   ciscoasa# activation-key key
   ```

   For example:

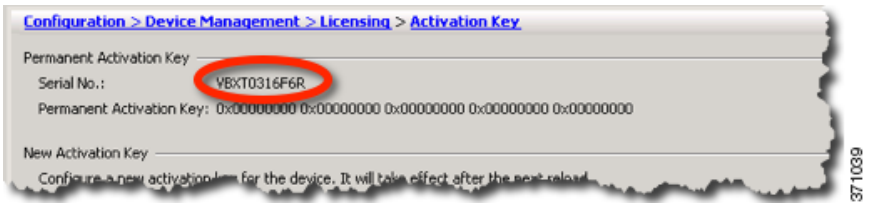
   ```
   ciscoasa# activation-key 592811f1 19ed804b 613befa3 d85bb703 c61b7da2
   Validating activation key. This may take a few minutes...
   The requested key is a timebases key and is activated, it has 364 days remaining.

   ASAv platform license state is Compliant
   ```

ASDM License Procedure

Procedure

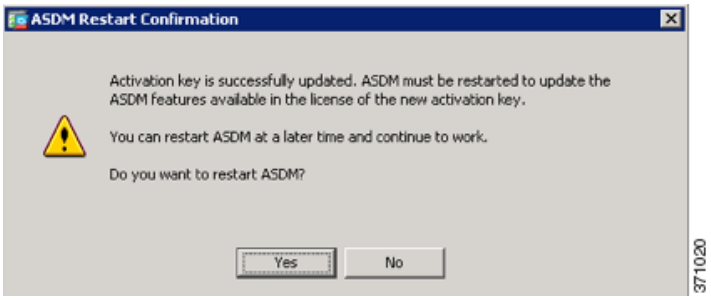
1. View the serial number by clicking the **License** tab on the main ASDM page and then clicking **More Licenses**.
2. From the **Configuration > Device Management > Licensing > Activation Key** pane, write down the serial number.



3. Obtain a Product Authorization Key, which you can purchase from your Cisco account representative. You need to purchase a separate Product Authorization Key for each feature license. For the ASAv, the only required feature license is for vCPUs (1 to 4), but you can purchase other feature keys as well.
4. Request an activation key from Cisco.com for the serial number according to the ASA licensing guide. Be sure to request a CPU license that matches the number of CPUs you specified when you deployed the ASAv.
5. After you receive the activation key from Cisco, on the **Configuration > Device Management > Licensing > Activation Key** pane, paste the key into the **New Activation Key** field.
6. Click **Update Activation Key**.

   ASDM shows a status dialog box while it verifies the key.

   When the key update is complete, you see the following dialog box:



7. Click **Yes** to restart ASDM.

Perform Initial Configuration Using ASDM

You can perform initial configuration using the following ASDM wizards and procedures. For CLI configuration, see the CLI configuration guides.

Run the Startup Wizard

Run the **Startup Wizard** (choose **Wizards > Startup Wizard)** so that you can customize the security policy to suit your deployment. Using the startup wizard, you can set the following:

- Hostname
- Domain name
- Administrative passwords
- Interfaces
- IP addresses
- Static routes
- DHCP server
- Network address translation rules
- and more...

(Optional) Allow Access to Public Servers Behind the ASAv

The **Configuration** > **Firewall** > **Public Servers** pane automatically configures the security policy to make an inside server accessible from the Internet. As a business owner, you might have internal network services, such as a web and FTP server, that need to be available to an outside user. You can place these services on a separate network behind the ASAv, called a demilitarized zone (DMZ). By placing the public servers on the DMZ, any attacks launched against the public servers do not affect your inside networks.

(Optional) Run VPN Wizards

You can configure VPN using the following wizards (**Wizards** > **VPN Wizards)**:

- Site-to-Site VPN Wizard—Creates an IPsec site-to-site tunnel between two ASAvs.
- AnyConnect VPN Wizard—Configures SSL VPN remote access for the Cisco AnyConnect VPN client. AnyConnect provides secure SSL connections to the ASA for remote users with full VPN tunneling to corporate resources. The ASA policy can be configured to download the AnyConnect client to remote users when they initially connect via a browser. With AnyConnect 3.0 and later, the client can run either the SSL or IPsec IKEv2 VPN protocol.
- Clientless SSL VPN Wizard—Configures clientless SSL VPN remote access for a browser. Clientless, browser-based SSL VPN lets users establish a secure, remote-access VPN tunnel to the ASA using a web browser. After authentication, users access a portal page and can access specific, supported internal resources. The network administrator provides access to resources by users on a group basis. ACLs can be applied to restrict or allow access to specific corporate resources.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard—Configures IPsec VPN remote access for the Cisco IPsec client.

(Optional) Run Other Wizards in ASDM

- High Availability and Scalability Wizard—Configure failover or VPN load balancing.

- Packet Capture Wizard—Configure and run packet capture. The wizard will run one packet capture on each of the ingress and egress interfaces. After capturing packets, you can save the packet captures to your PC for examination and replay in the packet analyzer.

Advanced Configuration

To continue configuring your ASAv, see the documents available for your software version at:
http://www.cisco.com/go/asadocs