

Basic Settings

This chapter describes how to configure basic settings on the ASA that are typically required for a functioning configuration and includes the following sections:

- Configuring the Hostname, Domain Name, and Passwords, page 17-1
- Setting the Date and Time, page 17-3
- Configuring the Master Passphrase, page 17-5
- Configuring the DNS Server, page 17-9
- Changing the Heap Memory Size, page 17-10
- Monitoring DNS Cache, page 17-10
- Choosing a Rule Engine Transactional Commit Model, page 17-11

Configuring the Hostname, Domain Name, and Passwords

- Setting the Hostname, Domain Name, and the enable and Telnet Passwords, page 17-2
- Feature History for the Hostname, Domain Name, and Passwords, page 17-3

Setting the Hostname, Domain Name, and the enable and Telnet Passwords

To set the hostname, domain name, and the enable and Telnet passwords, perform the following steps.

Prerequisites

In multiple context mode, you can configure the hostname and domain name in both the system and context execution spaces.

For the enable and Telnet passwords, set them in each context; they are not available in the system. When you session to the ASASM from the switch in multiple context mode, the ASASM uses the login password you set in the admin context.

To change from the system to a context configuration, in the **Configuration > Device List** pane, double-click the context name under the active device IP address.

Detailed Steps

Step 1 In ASDM, choose **Configuration > Device Setup > Device Name/Password**.

Step 2 Enter the hostname. The default hostname is "ciscoasa."

The hostname appears in the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. The hostname is also used in syslog messages.

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line; it can be used for a banner.

Step 3 Enter the domain name. The default domain name is default.domain.invalid.

The ASA appends the domain name as a suffix to unqualified names. For example, if you set the domain name to "example.com" and specify a syslog server by the unqualified name of "jupiter," then the ASA qualifies the name to "jupiter.example.com."

Step 4 Change the privileged mode (enable) password. The default password is blank.

The enable password lets you enter privileged EXEC mode if you do not configure enable authentication (see Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18).

The enable password also lets you log into ASDM with a blank username if you do not configure HTTP authentication (see Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18.

a. Check the **Change the privileged mode password** check box.

b. Enter the old password (the default password is blank), new password, and then confirm the new password.

Step 5 Set the login password for Telnet access. There is no default password.

The login password is used for Telnet access when you do not configure Telnet authentication (see Configuring Authentication for CLI, ASDM, and enable command Access, page 42-18). You also use this password when accessing the ASASM from the switch with the **session** command.

a. Check the **Change the password to access the console of the security appliance** check box.

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

Step 6 Click **Apply** to save your changes.

Feature History for the Hostname, Domain Name, and Passwords

Table 17-1 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 17-1 Feature History for the Master Passphrase

Feature Name	Platform Releases	Feature Information
Removal of the default Telnet password	9.0(2)/9.1(2)	To improve security for management access to the ASA, the default login password for Telnet was removed; you must manually set the password before you can log in using Telnet. **Note**: The login password is only used for Telnet if you do not configure Telnet user authentication. Formerly, when you cleared the password, the ASA restored the default of "cisco." Now when you clear the password, the password is removed. The login password is also used for Telnet sessions from the switch to the ASASM (see the **session** command). For initial ASASM access, you must use the **service-module session** command, until you set a login password. We did not modify any ASDM screens.

Setting the Date and Time

Note Do not set the date and time for the ASASM; it receives these settings from the host switch.

This section includes the following topics:

- Setting the Date and Time Using an NTP Server, page 17-4
- Setting the Date and Time Manually, page 17-5

Setting the Date and Time Using an NTP Server

To obtain the date and time from an NTP server, choose **Configuration > Device Setup > System Time > NTP**:

Detailed Steps

Use the NTP pane to define NTP servers for setting the time dynamically on the ASA. The time appears in the status bar at the bottom of the main ASDM window. Time derived from an NTP server overrides any time set manually in the Clock pane.

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The ASA chooses the server with the lowest stratum—a measure of how reliable the data is.

Adding or Editing the NTP Server Configuration

To add or edit an NTP server, perform the following steps:

Step 1 In ASDM, choose **Configuration > Device Setup > System Time > NTP**.

Step 2 Click **Add** to display the Add NTP Server Configuration dialog box.

Step 3 Enter the NTP server IP address.

Step 4 Check the **Preferred** check box to set this server as a preferred server. NTP uses an algorithm to determine which server is the most accurate and synchronizes to it. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the ASA uses the more accurate one.

Step 5 Choose the interface from the drop-down list. This setting specifies the outgoing interface for NTP packets. If the interface is blank, then the ASA uses the default admin context interface according to the routing table. To change the admin context (and the available interfaces), choose None (the default interface) for stability.

Step 6 Choose the key number from the drop-down list. This setting specifies the key ID for this authentication key, which enables you to use MD5 authentication to communicate with the NTP server. The NTP server packets must also use this key ID. If you have previously configured a key ID for another server, you can select it from the list; otherwise, enter a number between 1 and 4294967295.

Step 7 Check the **Trusted** check box to set this authentication key as a trusted key, which is required for authentication to succeed.

Step 8 Enter the key value to set the authentication key, which is a string that can be up to 32 characters long.

Step 9 Reenter the key value to make sure that you enter it correctly twice.

Step 10 Click **OK**.

Step 11 Check the **Enable NTP authentication** check box to turn on NTP authentication.

Step 12 Click **Apply** to save your changes.

Setting the Date and Time Manually

The time is based on a 24-hour clock and displays in the status bar at the bottom of the main ASDM pane.

In multiple context mode, you can set the time in the system configuration only.

To dynamically set the time using an NTP server, choose **Configuration > Device Setup > System Time > NTP**; time derived from an NTP server overrides any time set manually in the Clock pane.

To manually set the date and time for the ASA, perform the following steps:

Step 1 In ASDM, choose **Configuration > Device Setup > System Time > Clock**.

Step 2 Choose the time zone from the drop-down list. This setting specifies the time zone as GMT plus or minus the appropriate number of hours. If you select the Eastern Time, Central Time, Mountain Time, or Pacific Time zone, then the time adjusts automatically for daylight savings time, from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Note Changing the time zone on the ASA may drop the connection to intelligent SSMs.

Step 3 Click the Date drop-down list to display a calendar. Then find the correct date using the following methods:

- Click the name of the month to display a list of months, then click the desired month. The calendar updates to that month.
- Click the year to change the year. Use the up and down arrows to scroll through the years, or enter a year in the entry field.
- Click the arrows to the right and left of the month and year to scroll the calendar forward and backward one month at a time.
- Click a day on the calendar to set the date.

Step 4 Enter the time manually in hours, minutes, and seconds.

Step 5 Click **Update Display Time** to update the time shown in the bottom right corner of the ASDM pane. The current time updates automatically every ten seconds.

Configuring the Master Passphrase

This section includes the following topics:

- Information About the Master Passphrase, page 17-6
- Licensing Requirements for the Master Passphrase, page 17-6
- Guidelines and Limitations, page 17-6
- Adding or Changing the Master Passphrase, page 17-6
- Disabling the Master Passphrase, page 17-7
- Recovering the Master Passphrase, page 17-8
- Feature History for the Master Passphrase, page 17-8

Information About the Master Passphrase

The master passphrase allows you to securely store plain text passwords in encrypted format and provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. Features that use the master passphrase include the following:

- OSPF
- EIGRP
- VPN load balancing
- VPN (remote access and site-to-site)
- Failover
- AAA servers
- Logging
- Shared licenses

Licensing Requirements for the Master Passphrase

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single and multiple context mode.

Failover Guidelines

If failover is enabled but no failover shared key is set, an error message appears if you change the master passphrase, informing you that you must enter a failover shared key to protect the master passphrase changes from being sent as plain text.

Choose **Configuration > Device Management > High Availability > Failover**, enter any character in the Shared Key field or 32 hexadecimal numbers (0-9A-Fa-f) if a failover hexadecimal key is selected, except a backspace**.** Then click **Apply.**

Adding or Changing the Master Passphrase

To add or change the master passphrase, perform the following steps:

Step 1 In single context mode, choose **Configuration > Device Management > Advanced > Master Passphrase**.

In multiple context mode, choose **Configuration > Device Management > Device Administration > Master Passphrase.**

Step 2 Check the **Advanced Encryption Standard (AES) password encryption** check box.

If no master passphrase is in effect, a warning message appears when you click **Apply**. You can click **OK** or **Cancel** to continue.

If you later disable password encryption, all existing encrypted passwords are left unchanged, and as long as the master passphrase exists, the encrypted passwords will be decrypted as required by the application.

Step 3 Check the **Change the encryption master passphrase** check box to enable you to enter and confirm your new master passphrases. By default, they are disabled.

Your new master passphrase must be between 8 and 128 characters long.

If you are changing an existing passphrase, you must enter the old passphrase before you can enter a new one.

To delete the master passphrase, leave the New and Confirm master passphrase fields blank.

Step 4 Click **Apply**.

When you click **Apply**, warning messages appear under the following conditions:

- The Change the encryption master passphrase field is enabled, and the New master passphrase field is empty. The **no key configuration-key password-encrypt** command is then sent to the device.
- The old master passphrase does not match the hash value in the **show password encryption** command output.
- You use non-portable characters, particularly those with the high-order bit set in an 8-bit representation.
- A master passphrase and failover are in effect, then an error message appears if an attempt to remove the failover shared key occurs.
- Encryption is disabled, but a new or replacement master passphrase is supplied. Click **OK** or **Cancel** to continue.
- If the master passphrase is changed in multiple context mode.
- If Active/Active failover is configured and the master passphrase is changed.
- If any running configurations are configured so that their configurations cannot be saved to their server, such as with context configuration URLs that use HTTP or HTTPS, and the master passphrase is changed.

Disabling the Master Passphrase

Disabling the master passphrase reverts encrypted passwords into plain text passwords. Removing the passphrase might be useful if you downgrade to a previous software version that does not support encrypted passwords.

You must know the current master passphrase to disable it. If you do not know the passphrase, see Recovering the Master Passphrase, page 17-8.

To disable the master passphrase, perform the following steps:

Step 1 In single context mode, choose **Configuration > Device Management > Advanced > Master Passphrase**.

In multiple context mode, choose **Configuration > Device Management > Device Administration > Master Passphrase**.

Step 2 Check the **Advanced Encryption Standard (AES) password encryption** check box.

If no master passphrase is in effect, a warning statement appears when you click **Apply**. Click **OK** or **Cancel** to continue.

Step 3 Check the **Change the encryption master passphrase** check box.

Step 4 Enter the old master passphrase in the Old master passphrase field. You must provide the old master passphrase to disable it.

Step 5 Leave the New master passphrase and the Confirm master passphrase fields empty.

Step 6 Click **Apply**.

Recovering the Master Passphrase

You cannot recover the master passphrase. If the master passphrase is lost or unknown, you can remove it.

To remove the master passphrase, perform the following steps:

Feature History for the Master Passphrase

Table 17-2 lists each feature change and the platform release in which it was implemented. ASDM is backward-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 17-2 Feature History for the Master Passphrase

Feature Name	Platform Releases	Feature Information
Master Passphrase	8.3(1)	We introduced this feature. The master passphrase allows you to securely store plain text passwords in encrypted format and provides a key that is used to universally encrypt or mask all passwords, without changing any functionality. We introduced the following screens: Configuration > Device Management > Advanced > Master Passphrase. Configuration > Device Management > Device Administration > Master Passphrase.

Configuring the DNS Server

Some ASA features require use of a DNS server to access external servers by domain name; for example, the Botnet Traffic Filter feature requires a DNS server to access the dynamic database server and to resolve entries in the static database. Other features, such as the **ping** or **traceroute** command, let you enter a name that you want to ping or traceroute, and the ASA can resolve the name by communicating with a DNS server. Many SSL VPN and certificate commands also support names.

Note The ASA has limited support for using the DNS server, depending on the feature. For these feature, to resolve the server name to an IP address, you must enter the IP address manually by adding the server name in the Configuration > Firewall > Objects > Network Object/Groups pane.

For information about dynamic DNS, see Configuring Dynamic DNS, page 18-3.

Prerequisites

Make sure that you configure the appropriate routing for any interface on which you enable DNS domain lookup so you can reach the DNS server. see Information About Routing, page 25-1 for more information about routing.

To configure the DNS server, perform the following steps:

Step 1 In the ASDM main application window, choose **Configuration > Device Management > DNS > DNS Client**.

Step 2 In the DNS Setup area, choose one of the following options:

- Configure one DNS server group.
- Configure multiple DNS server groups.

Step 3 Click **Add** to display the Add DNS Server Group dialog box.

Step 4 Specify up to six addresses to which DNS requests can be forwarded. The ASA tries each DNS server in order until it receives a response.

Note You must first enable DNS on at least one interface before you can add a DNS server. The DNS Lookup area shows the DNS status of an interface. A False setting indicates that DNS is disabled. A True setting indicates that DNS is enabled.

Step 5 Enter the name of each configured DNS server group.

Step 6 Enter the IP addresses of the configured servers, and click **Add** to include them in the server group. To remove a configured server from the group, click **Delete**.

Step 7 To change the sequence of the configured servers, click **Move Up** or **Move Down**.

Step 8 In the Other Settings area, enter the number of seconds to wait before trying the next DNS server in the list, between 1 and 30 seconds. The default is 2 seconds. Each time the ASA retries the list of servers, the timeout time doubles.

Step 9 Enter the number of seconds to wait before trying the next DNS server in the group.

Step 10 Enter a valid DNS domain name for the group of configured servers.

Step 11 Click **OK** to close the Add DNS Server Group dialog box.

The new DNS server settings appear.

Step 12 To change these settings, click **Edit** to display the Edit DNS Server Group dialog box.

Step 13 Make your desired changes, then click **OK** to close the Edit DNS Server Group dialog box.

The revised DNS server settings appear.

Step 14 To enable a DNS server group to receive DNS requests, click **Set Active**.

Step 15 In the DNS Guard area, to enforce one DNS response per query, check the **Enable DNS Guard on all interfaces** check box. If DNS inspection is enabled, this setting is ignored on the selected interface.

Step 16 Click **Apply** to save your changes, or click **Reset** to discard those changes and enter new ones.

Changing the Heap Memory Size

ASDM supports a maximum configuration size of 512 KB. If you exceed this amount you may experience performance issues. For example, when you load the configuration, the status dialog box shows the percentage of the configuration that is complete, yet with large configurations it stops incrementing and appears to suspend operation, even though ASDM might still be processing the configuration. If this situation occurs, we recommend that you consider increasing the ASDM system heap memory.

To increase the ASDM heap memory size, modify the launcher shortcut by performing the following procedure:

Step 1 Right-click the shortcut for the ASDM-IDM Launcher, and choose **Properties**.

Step 2 Click the **Shortcut** tab.

Step 3 In the Target field, change the argument prefixed with "-Xmx" to specify your desired heap size. For example, change it to -Xmx768m for 768 MB or -Xmx1g for 1 GB. For more information about this parameter, see the Oracle document in the following location:
http://docs.oracle.com/javase/1.5.0/docs/tooldocs/windows/java.html

Along with using troubleshooting information in this guide, see the *ASDM Troubleshooting* document at the following URL:

http://www.cisco.com/en/US/products/ps6121/products_tech_note09186a0080aaeff5.shtml

Monitoring DNS Cache

The ASA provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache

can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache with its corresponding hostname.

To monitor the DNS cache, see the following pane:

Path	Purpose
Tools > Command Line Interface Enter the **show dns-hosts** command, then press **Send.**	Show the DNS cache, which includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the **name** command.

Choosing a Rule Engine Transactional Commit Model

By default, when you change a rule-based policy (such as access rules), the changes become effective immediately. However, this immediacy comes at a slight cost in performance. The performance cost is more noticeable for very large rule lists in a high connections-per-second environment, for example, when you change a policy with 25,000 rules while the ASA is handling 18,000 connections per second.

The performance is affected because the rule engine compiles rules to enable faster rule lookup. By default, the system will also search uncompiled rules when evaluating a connection attempt so that new rules can be applied; since the rules are not compiled, the search takes longer.

You can change this behavior so that the rule engine uses a transactional model when implementing rule changes, continuing to use the old rules until the new rules are compiled and ready for use. Using the transactional model, performance should not drop during the rule compilation. The following table clarifies the behavioral difference.

Model	Before Compilation	During Compilation	After Compilation
Default	Match old rules.	Match new rules. (Connections per second rate will decrease.)	Match new rules.
Transactional	Match old rules.	Match old rules. (Connections per second rate will be unaffected.)	Match new rules.

An additional benefit of the transactional model is that, when replacing an ACL on an interface, there is no gap between deleting the old ACL and applying the new one. This reduces the chances that acceptable connections will be dropped during the operation.

Tip If you enable the transactional model for a rule type, there are syslog messages to mark the beginning and the end of the compilation. These messages are numbered 780001 and following.

Detailed Steps

Step 1 Choose **Configuration > Device Management > Management Access > Rule Engine**.

Step 2 Enable the transactional commit model for the desired features. Options include:

- **Access group**—Access rules applied globally or to interfaces.

Step 3 Click **Apply**.