client-access-rule through crl configure Commands

client-access-rule

To configure rules that limit the remote access client types and versions that can connect via IPsec through the ASA, use the **client-access-rule** command in group-policy configuration mode. To delete a rule, use the **no** form of this command.

client-access-rule *priority* {**permit** | **deny**} **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{**permit** | **deny**} **type** *type* **version** *version*]

Syntax Description

deny	Denies connections for devices of a particular type and/or version.
none	Allows no client access rules. Sets **client-access-rule** to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.
permit	Permits connections for devices of a particular type and/or version.
priority	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the ASA ignores it.
type *type*	Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the **show vpn-sessiondb remote** command output, except that you can use the * character as a wildcard.
version *version*	Identifies the device version via free-form strings, for example 7.0. A string must match exactly its appearance in the **show vpn-sessiondb remote** command output, except that you can use the * character as a wildcard.

Defaults

By default, there are no access rules.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To delete all rules, use the **no client-access-rule command** with only the *priority* argument. This deletes all configured rules, including a null rule created by issuing the **client-access-rule none** command.

When there are no client access rules, users inherit any rules that exist in the default group policy. To prevent users from inheriting client access rules, use the **client-access-rule none** command. The result of doing so is that all client types and versions can connect.

Construct rules according to these caveats:

- If you do not define any rules, the ASA permits all connection types.
- When a client matches none of the rules, the ASA denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the ASA denies all connections.
- For both software and hardware clients, type and version must match exactly their appearance in the **show vpn-sessiondb remote** command output.
- The * character is a wildcard, which you can use multiple times in each rule. For example, **client-access-rul**e **3 deny type * version 3.*** creates a priority 3 client access rule that denies all client types running release versions 3.x software.
- You can construct a maximum of 25 rules per group policy.
- There is a limit of 255 characters for an entire set of rules.
- You can use n/a for clients that do not send client type and/or version.

Examples

The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit VPN Clients running software version 4.1, while denying all VPN 3002 hardware clients:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-bypass-proxy

To configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic, use the **client-bypass-proxy** command in group-policy configuration mode. To clear the client bypass protocol setting, use the **no** form of this command.

client-bypass-protocol {**enable** | **disable**}

no client-bypass-protocol {**enable** | **disable**}

Syntax Description

enable	If Client Bypass Protocol is enabled, the the IP traffic for which the ASA did not assign an IP address type is sent from the client in the clear.
disable	If Client Bypass Protocol is disabled, the IPv6 traffic for wich the ASA did not assing an IP address type is is dropped.

Defaults

Client Bypass Protocol is disabled by default in the DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

The Client Protocol Bypass feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.

When the AnyConnect client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or “in the clear.”

For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.

Examples

The following example enables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol enable
hostname(config-group-policy)#
```

The following example disables client bypass protocol:

```
hostname(config-group-policy)# client-bypass-protocol disable
hostname(config-group-policy)#
```

The following example clears the client bypass protocol setting:

```
hostname(config-group-policy)# no client-bypass-protocol enable
hostname(config-group-policy)#
```

client (ctl-provider)

To specify clients allowed to connect to the Certificate Trust List provider, or to specify a username and password for client authentication, use the **client** command in ctl provider configuration mode. To remove the configuration, use the **no** form of this command.

client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

no client [[**interface** *if_name*] *ipv4_addr*] | [**username** *user_name* **password** *password* [**encrypted**]]

Syntax Description

encrypted	Specifies encryption for the password.
interface *if_name*	Specifies the interface allowed to connect.
ipv4_addr	Specifies the IP address of the client.
password *password*	Specifies the password for client authentication.
username *user_name*	Specifies the username for client authentication.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ctl provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **client** command in ctl provider configuration mode to specify the clients allowed to connect to the CTL provider, and to set the username and password for client authentication. More than one command may be issued to define multiple clients. The username and password must match the CCM Administrator's username and password for the CallManager cluster.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
ctl	Parses the CTL file from the CTL client and installs trustpoints.
ctl-provider	Configures a CTL provider instance in ctl provider configuration mode.
export	Specifies the certificate to be exported to the client
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

client (tls-proxy)

To configure trustpoints, keypairs, and cipher suites, use the **client** command in tls proxy configuration mode. To remove the configuration, use the **no** form of this command.

client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]]

no client [**cipher-suite** *cipher_suite*] | [**ldc** [**issuer** *ca_tp_name* | **key-pair** *key_label*]

Syntax Description

cipher-suite *cipher_suite*	Specifies the cipher suite. Options include des-sha1, 3des-sha1, aes128-sha1, aes256-sha1, or null-sha1.
issuer *ca_tp_name*	Specifies the local CA trustpoint to issue client dynamic certificates.
keypair *key_label*	Specifies the RSA keypair to be used by client dynamic certificates.
ldc	Specifies the local dynamic certificate issuer or keypair.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tls proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **client** command in tls proxy configuration mode to control the TLS handshake parameters for the ASA as the TLS client role in TLS proxy. This includes cipher suite configuration, or to set the local dynamic certificate issuer or keypair. The local CA that issues client dynamic certificates is defined by the **crypto ca trustpoint** command, and the trustpoint must have the **proxy-ldc-issuer** command configured, or the default local CA server (LOCAL-CA-SERVER).

The keypair value must have been generated with the **crypto key generate** command.

For client proxy (the proxy acts as a TLS client to the server), the user-defined cipher suite replaces the default cipher suite, or the one defined by the **ssl encryption** command. You can use this command to achieve different ciphers between the two TLS sessions. You should use AES ciphers with the CallManager server.

Examples

The following example shows how to create a TLS proxy instance:

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters ctl provider configuration mode.
server trust-point	Specifies the proxy trustpoint certificate to be presented during the TLS handshake.
show tls-proxy	Shows the TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum number of sessions.

client-firewall

To set personal firewall policies that the ASA pushes to the VPN client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, use the **no** form of this command.

client-firewall none

no client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

Note When the firewall type is **zonelabs-integrity**, do not include arguments. The Zone Labs Integrity Server determines the policies.

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

Syntax Description

acl-in *acl*	Provides the policy the client uses for inbound traffic.
acl-out *acl*	Provides the policy the client uses for outbound traffic.
AYT	Specifies that the client PC firewall application controls the firewall policy. The ASA checks to make sure the firewall is running. It asks, “Are You There?” If there is no response, the ASA tears down the tunnel.
cisco-integrated	Specifies the Cisco Integrated firewall type.
cisco-security-agent	Specifies the Cisco Intrusion Prevention Security Agent firewall type.
CPP	Specifies Policy Pushed as source of the VPN Client firewall policy.
custom	Specifies the Custom firewall type.
description *string*	Describes the firewall.
networkice-blackice	Specifies the Network ICE Black ICE firewall type.

none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing one. Prevents inheriting a firewall policy from a default or specified group policy.
opt	Indicates an optional firewall type.
product-id	Identifies the firewall product.
req	Indicates a required firewall type.
sygate-personal	Specifies the Sygate Personal firewall type.
sygate-personal-pro	Specifies the Sygate Personal Pro firewall type.
sygate-security-agent	Specifies the Sygate Security Agent firewall type.
vendor-id	Identifies the firewall vendor.
zonelabs-integrity	Specifies the Zone Labs Integrity Server firewall type.
zonelabs-zonealarm	Specifies the Zone Labs Zone Alarm firewall type.
zonelabs-zonealarmorpro policy	Specifies the Zone Labs Zone Alarm or Pro firewall type.
zonelabs-zonealarmpro policy	Specifies the Zone Labs Zone Alarm Pro firewall type.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **zonelabs-integrity** firewall type was added.

Usage Guidelines

Only one instance of this command can be configured.

To delete all firewall policies, use the **no client-firewall** command without arguments. This command deletes all configured firewall policies, including a null policy created by issuing the **client-firewall none** command.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, use the **client-firewall none** command.

Examples

The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client trust-point

To specify the proxy trustpoint certificate to be presented during the TLS handshake when configuring the TLS Proxy for Cisco Unified Presence Server (CUPS), use the **client trust-point** command in tls-proxy configuration mode. To remove the proxy trustpoint certificate, use the **no** form of this command.

client trust-point *proxy_trustpoint*

no client trust-point [*proxy_trustpoint*]

Syntax Description

proxy_trustpoint	Specifies the trustpoint defined by the **crypto ca trustpoint** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tls proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **client trust-point** command specifies the trustpoint and associated certificate that the ASA uses in the TLS handshake when the ASA assumes the role of the TLS client. The certificate must be owned by the ASA (identity certificate).

The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential. The **client trust-point** command has precedence over the global **ssl trust-point** command.

Examples

The following example shows the use of the **client trust-point** command to specify the use of trustpoint "ent_y_proxy" in the TLS handshake with the TLS server. The handshake is likely to originate from entity Y to entity X, where the TLS server resides. The ASA functions as the TLS proxy for entity Y.

```
hostname(config-tlsp)# client trust-point ent_y_proxy
```

Usage Guidelines

When there are multiple trustpoints associated with the same CA certificate, only one of the trustpoints can be configured for a specific client type. However, one of the trustpoints can be configured for one client type and the other trustpoint with another client type.

If there is a trustpoint associated with the same CA certificate that is already configured with a client type, the new trustpoint is not allowed to be configured with the same client-type setting. The **no** form of the command clears the setting so that a trustpoint cannot be used for any client validation.

Remote access VPNs can use Secure Sockets Layer (SSL) VPN, IP Security (IPsec), or both, depending on deployment requirements, to permit access to any network application or resource.

Examples

The following example enters crypto ca trustpoint configuration mode for the trustpoint, central, and designates it as an SSL trustpoint:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# client-types ssl
hostname(config-ca-trustpoint)#
```

The following example enters crypto ca trustpoint configuration mode for the trustpoint, checkin1, and designated it as an IPsec trustpoint:

```
hostname(config)# crypto ca trustpoint checkin1
hostname(config-ca-trustpoint)# client-types ipsec
hostname(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
id-usage	Specifies how the enrolled identity of a trustpoint can be used.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

client-update

To issue a client-update for all active remote VPN software and hardware clients and ASAs configured as Auto Update clients, on all tunnel-groups or for a particular tunnel group, use the **client-update** command in privileged EXEC mode.

To configure and change client-update parameters at the global level, including VPN software and hardware clients and ASAs configured as Auto Update clients, use the **client-update** command in global configuration mode.

To configure and change client-update tunnel-group IPsec-attributes parameters for VPN software and hardware clients, use the **client-update** command in tunnel-group ipsec-attributes configuration mode.

To disable a client update, use the **no** form of this command.

Global configuration mode command:

client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

no client-update {**enable** | **component** {**asdm** | **image**} | **device-id** *dev_string* | **family** *family_name* | **type** *type*} **url** *url-string* **rev-nums** *rev-nums*}

Tunnel-group ipsec-attributes configuration mode command:

client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

no client-update type *type* **url** *url-string* **rev-nums** *rev-nums*

Privileged EXEC mode command:

client-update {**all** | *tunnel-group*}

no client-update *tunnel-group*

Syntax Description

all	(Available only in privileged EXEC mode.) Applies the action to all active remote clients in all tunnel groups. You cannot use the keyword **all** with the **no** form of the command.
component {**asdm** | **image**}	The software component for ASAs configured as Auto Update clients.
device-id *dev_string*	If the Auto Update client is configured to identify itself with a unique string, specify the same string that the client uses. The maximum length is 63 characters.
enable	(Available only in global configuration mode). Enables remote client software updates.
family *family_name*	If the Auto Update client is configured to identify itself by device family, specify the same device family that the client uses. It can be asa, pix, or a text string with a maximum length of 7 characters.
rev-nums *rev-nums*	(Not available in privileged EXEC mode.) Specifies the software or firmware images for this client. For Windows, WIN9X, WinNT, and VPN3002 clients, enter up to 4, in any order, separated by commas. For ASAs, only one is allowed. The maximum length of the string is 127 characters.

tunnel-group	(Available only in privileged EXEC mode.) Specifies the name of a valid tunnel-group for remote client update.
type *type*	(Not available in privileged EXEC mode.) Specifies the operating systems of remote PCs or the type of ASAs (configured as Auto Update clients) to notify of a client update. The list is the following: • asa5505: Cisco 5505 Adaptive Security Appliance • asa5510: Cisco 5510 Adaptive Security Appliance • asa5520: Cisco 5520 Adaptive Security Appliance • asa5540: Cisco 5540 Adaptive Security Appliance • linux: A Linux client • mac: MAC OS X client • pix-515: Cisco PIX 515 Firewall • pix-515e: Cisco PIX 515E Firewall • pix-525: Cisco PIX 525 Firewall • pix-535: Cisco PIX 535 Firewall • Windows: all windows-based platforms • WIN9X: Windows 95, Windows 98, and Windows ME platforms • WinNT: Windows NT 4.0, Windows 2000, and Windows XP platforms • vpn3002: VPN 3002 hardware client • A text string of up to 15 characters
url *url-string*	(Not available in privileged EXEC mode.) Specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client. The maximum string length is 255 characters.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	—	•		—
Global configuration	•	—	•		—
Tunnel-group ipsec-attributes configuration	•	—	•		—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added the tunnel-group ipsec-attributes configuration mode.
7.2(1)	Added the **component**, **device-id**, and **family** keywords and their arguments to support the ASA configured as an Auto Update Server.

Usage Guidelines

In tunnel-group ipsec-attributes configuration mode, you can apply this attribute only to the IPsec remote-access tunnel-group type.

The **client-update** command lets you enable the update; specify the types and revision numbers of clients to which the update applies; provide a URL or IP address from which to get the update; and, in the case of Windows clients, optionally notify users that they should update their VPN client version. If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update.

For Windows clients, you can provide a mechanism for users to accomplish that update. For VPN 3002 hardware client users, the update occurs automatically, with no notification. When the client type is another ASA, this ASA acts as an Auto Update server.

Note For all Windows clients and Auto Update clients, you must use the protocol "http://" or "https://" as the prefix for the URL. For the VPN 3002 hardware client, you must specify protocol "tftp://" instead.

Alternatively, for Windows clients and VPN 3002 hardware clients, you can configure client update just for individual tunnel-groups, rather than for all clients of a particular type.

Note You can have the browser automatically start an application by including the application name at the end of the URL; for example: https://support/updates/vpnclient.exe.

After you have enabled client update, you can define a set of client-update parameters for a particular IPsec- remote access tunnel group. To do this, in tunnel-group ipsec-attributes mode, specify the tunnel-group name and its type, and the URL or IP address from which to get the updated image. In addition, you must specify a revision number. If the user client revision number matches one of the specified revision numbers, there is no need to update the client; for example, to issue a client update for all Windows clients.

Optionally, you can send a notice to active users with outdated Windows clients that their VPN client needs updating. For these users, a dialog box appears, offering the opportunity to launch a browser and download the updated software from the site specified in the URL. The only part of this message that you can configure is the URL. Users who are not active get a notification message the next time they log in. You can send this notice to all active clients on all tunnel groups, or you can send it to clients on a particular tunnel group.

If the user client revision number matches one of the specified revision numbers, there is no need to update the client, and users receive no notification message. VPN 3002 clients update without user intervention, and users receive no notification message.

Note If you specify the client-update type as **windows** (specifying all Windows-based platforms) and later want to enter a client-update type of **win9x** or **winnt** for the same entity, you must first remove the windows client type with the **no** form of the command, then use new **client-update** commands to specify the new client types.

Examples

The following example, entered in global configuration mode, enables client update for all active remote clients on all tunnel groups:

```
hostname(config)# client-update enable
hostname#
```

The following example applies only to Windows (Win9x, WinNT). Entered in global configuration mode, it configures client update parameters for all Windows-based clients, including the revision number, 4.7 and the URL for retrieving the update, https://support/updates.

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.7
hostname(config)#
```

The following example applies only to VPN 3002 hardware clients. Entered in tunnel-group ipsec-attributes configuration mode, it configures client update parameters for the IPsec remote-access tunnel-group “salesgrp”. It designates the revision number, 4.7 and uses the TFTP protocol for retrieving the updated software from the site with the IP address 192.168.1.1:

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1 rev-nums
4.7
hostname(config-tunnel-ipsec)#
```

The following example shows how to issue a client update for clients that are Cisco 5520 ASAs configured as Auto Update clients:

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

The following example, entered in privileged EXEC mode, sends a client-update notification to all connected remote clients in the tunnel group named “remotegrp” that need to update their client software. Clients in other groups do not get an update notification.

```
hostname# client-update remotegrp
hostname#
```

The following example, entered in privileged EXEC mode, notifies all active clients on all tunnel groups:

```
hostname# client-update all
hostname#
```

Related Commands

Command	Description
clear configure client-update	Clears the entire client-update configuration.
show running-config client-update	Shows the current client-update configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

clock set

To manually set the clock on the ASA, use the **clock set** command in privileged EXEC mode.

clock set *hh***:***mm***:***ss* {*month day* | *day month*} *year*

Syntax Description

day	Sets the day of the month, from 1 to 31. You can enter the day and month as **april 1** or as **1 april**, for example, depending on your standard date format.
*hh***:***mm***:***ss*	Sets the hour, minutes, and seconds in 24-hour time. For example, set **20:54:00** for 8:54 pm.
month	Sets the month. Depending on your standard date format, you can enter the day and month as **april 1** or as **1 april**.
year	Sets the year using four digits, for example, **2004**. The year range is 1993 to 2035.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you have not entered any **clock** configuration commands, the default time zone for the **clock set** command is UTC. If you change the time zone after you enter the **clock set** command using the **clock timezone** command, the time automatically adjusts to the new time zone. However, if you enter the **clock set** command after you establish the time zone with the **clock timezone** command, then enter the time appropriate for the new time zone and not for UTC. Similarly, if you enter the **clock summer-time** command after the **clock set** command, the time adjusts for daylight saving. If you enter the **clock set** command after the **clock summer-time** command, enter the correct time for daylight saving.

This command sets the time in the hardware chip, and does not save the time in the configuration file. This time endures reboots. Unlike the other **clock** commands, this command is a privileged EXEC command. To reset the clock, you need to set a new time for the **clock set** command.

Examples

The following example sets the time zone to MST, the daylight saving time to the default period in the U.S., and the current time for MDT to 1:15 p.m. on July 27, 2004:

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

The following example sets the clock to 8:15 on July 27, 2004 in the UTC time zone, and then sets the time zone to MST and the daylight saving time to the default period in the U.S. The end time (1:15 in MDT) is the same as the previous example.

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

Related Commands

Command	Description
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
show clock	Shows the current time.

clock summer-time

To set the date range for daylight saving time for the display of the ASA time, use the **clock summer-time** command in global configuration mode. To disable the daylight saving time dates, use the **no** form of this command.

clock summer-time *zone* **recurring** [*week weekday month hh***:***mm week weekday month hh***:***mm*] [*offset*]

no clock summer-time [*zone* **recurring** [*week weekday month hh***:***mm week weekday month hh***:***mm*] [*offset*]]

clock summer-time *zone* **date** {*day month* | *month day*} *year hh***:***mm* {*day month* | *month day*} *year hh***:***mm* [*offset*]

no clock summer-time [*zone* **date** {*day month* | *month day*} *year hh***:***mm* {*day month* | *month day*} *year hh***:***mm* [*offset*]]

Syntax Description

date	Specifies the start and end dates for daylight saving time as a specific date in a specific year. If you use this keyword, you need to reset the dates each year.
day	Sets the day of the month, from 1 to 31. You can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format.
hh:mm	Sets the hour and minutes in 24-hour time.
month	Sets the month as a string. For the **date** command, you can enter the day and month as **April 1** or as **1 April**, for example, depending on your standard date format.
offset	(Optional) Sets the number of minutes to change the time for daylight saving time. By default, the value is 60 minutes.
recurring	Specifies the start and end dates for daylight saving time, in the form of a day and time of the month, and not a specific date in a year. This keyword lets you set a recurring date range that you do not need to alter yearly. If you do not specify any dates, the ASA uses the default date range for the United States: from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.
week	(Optional) Specifies the week of the month as an integer between 1 and 4 or as the words **first** or **last**. For example, if the day might fall in the partial fifth week, then specify **last**.
weekday	(Optional) Specifies the day of the week: **Monday**, **Tuesday**, **Wednesday**, and so on.
year	Sets the year using four digits, for example, **2004**. The year range is 1993 to 2035.
zone	Specifies the time zone as a string, for example, **PDT** for Pacific Daylight Time. When the ASA shows the daylight saving time according to the date range you set with this command, the time zone changes to the value you set here. See the **clock timezone** command to set the base time zone to a zone other than UTC.

Defaults

The default offset is 60 minutes.

The default recurring date range is from 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	The default recurring date range was changed to 2:00 a.m. on the second Sunday in March to 2:00 a.m. on the first Sunday in November.

Usage Guidelines

For the Southern Hemisphere, the ASA accepts the start month to be later in the year than the end month, for example, from October to March.

Examples

The following example sets the daylight saving date range for Australia:

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

Some countries start daylight saving on a specific date. In the following example, daylight saving time is configured to start on April 1, 2008, at 3 a.m. and end on October 1, 2008, at 4 a.m.

```
hostname(config)# clock summer-time UTC date 1 April 2008 3:00 1 October 2008 4:00
```

Related Commands

Command	Description
clock set	Manually sets the clock on the ASA.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show clock	Shows the current time.

clock timezone

To set the time zone for the ASA clock, use the **clock timezone** command in global configuration mode. To set the time zone back to the default of UTC, use the **no** form of this command.

clock timezone *zone* [**-**]*hours* [*minutes*]

no clock timezone [*zone* [**-**]*hours* [*minutes*]]

Syntax Description

[**-**]*hours*	Sets the number of hours of offset from UTC. For example, PST is -8 hours.
minutes	(Optional) Sets the number of minutes of offset from UTC.
zone	Specifies the time zone as a string, for example, PST for Pacific Standard Time.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To set daylight saving time, see the **clock summer-time** command.

The **clock set** command or the time derived from an NTP server sets the time in UTC. You must set the time zone as an offset of UTC using this command.

Examples

The following example sets the time zone to Pacific Standard Time, which is -8 hours from UTC:

```
hostname(config)# clock timezone PST -8
```

Related Commands

Command	Description
clock set	Manually sets the clock on the ASA.
clock summer-time	Sets the date range to show daylight saving time.

Command	Description
ntp server	Identifies an NTP server.
show clock	Shows the current time.

cluster-ctl-file

To use trustpoints that are already created from an existing CTL file stored in flash memory, use the **cluster-ctl-file** command in ctl file configuration mode. To remove the CTL file configuration so that you can create a new CTL file, use the **no** form of this command.

cluster-ctl-file *filename_path*

no cluster-ctl-file *filename_path*

Syntax Description

filename_path	Specifies the path and filename of the CTL file stored on disk or stored in flash memory.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ctl-file configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

When this command is configured, the Phone Proxy parses the CTL file stored in flash memory and installs the trustpoints from that CTL file, then uses that file from flash in the creation of the new CTL file.

Examples

The following example parses the CTL file stored in flash memory to install the trustpoints from that file:

```
hostname(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

cluster encryption

To enable encryption for messages exchanged on the virtual load-balancing cluster, use the **cluster encryption** command in vpn load-balancing configuration mode. To disable encryption, use the **no** form of this command.

cluster encryption

no cluster encryption

Note VPN load balancing requires an active 3DES/AES license. The ASA checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the ASA prevents the enabling of load balancing and prevents internal configuration of 3DES by the load balancing system, unless the license permits this usage.

Syntax Description

This command has no arguments or keywords.

Defaults

Encryption is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command turns encryption on or off for messages exchanged on the virtual load-balancing cluster.

Before configuring the **cluster encryption** command, you must have first used the **vpn load-balancing** command to enter vpn load-balancing configuration mode. You must also use the **cluster key** command to configure the cluster shared secret key before enabling cluster encryption.

Note When using encryption, you must first configure the command **isakmp enable** *inside*, where *inside* designates the load-balancing inside interface. If ISAKMP is not enabled on the load-balancing inside interface, an error message appears when you try to configure cluster encryption.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **cluster encryption** command to enable encryption for the virtual load-balancing cluster:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
cluster key	Specifies the shared-secret key for the cluster.
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster exec

To execute a command on all units in the cluster, or on a specific member, use the **cluster exec** command in privileged EXEC mode.

cluster exec [**unit** *unit_name*] *command*

Syntax Description

unit *unit_name*	(Optional) Performs the command on a specific unit. To view member names, enter **cluster exec unit ?** (to see all names except the current unit), or enter the **show cluster info** command.
command	Specifies the command you want to execute.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

Sending a **show** command to all members collects all output and displays it on the console of the current unit. Other commands, such as **capture** and **copy**, can also take advantage of cluster-wide execution.

Examples

To copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:

```
hostname# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as capture1_asa1.pcap, capture1_asa2.pcap, and so on. In this example, asa1 and asa2 are cluster unit names.

The following sample output for the **cluster exec show port-channel** summary command shows EtherChannel information for each member in the cluster:

```
hostname# cluster exec show port-channel summary
primary(LOCAL):***********************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
```

```
1         Po1              LACP      Yes  Gi0/0(P)
2         Po2              LACP      Yes  Gi0/1(P)
 secondary:*****************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1              LACP      Yes   Gi0/0(P)
2         Po2              LACP      Yes   Gi0/1(P)
```

Related Commands

Command	Description
cluster group	Enters cluster group configuration mode.
show cluster info	Shows cluster information.

cluster group

To configure the cluster bootstrap parameters and other cluster settings, use the **cluster group** command in global configuration mode. To clear the cluster configuration, use the **no** form of this command.

cluster group *name*

no cluster group *name*

Syntax Description

name	Specifies the cluster name as an ASCII string from 1 to 38 characters. You can only configure one cluster group per unit. All members of the cluster must use the same name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

Each unit in the cluster requires a bootstrap configuration to join the cluster. Typically, the first unit you configure to join the cluster will be the master unit. After you enable clustering, after an election period, the cluster elects a master unit. With only one unit in the cluster initially, that unit will become the master unit. Subsequent units that you add to the cluster will be slave units.

Before you configure clustering, you need to set the cluster interface mode using the **cluster interface-mode** command.

You must use the console port or ASDM to enable or disable clustering. You cannot use Telnet or SSH.

Examples

The following example configures a management interface, configures a device-local EtherChannel for the cluster control link, disables the health check (temporarily), and then enables clustering for the ASA called “unit1,” which will become the master unit because it is added to the cluster first:

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    no health-check
    enable noconfirm
```

The following example includes the configuration for a slave unit, unit2:

```
interface tengigabitethernet 0/6
    channel-group 1 mode active
    no shutdown

interface tengigabitethernet 0/7
    channel-group 1 mode active
    no shutdown

cluster group pod1
    local-unit unit2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    no health-check
    enable as-slave
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.

Command	Description
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

cluster ip address

To set the IP address of the virtual load-balancing cluster, use the **cluster ip address** command in vpn load-balancing configuration mode. To remove the IP address specification, use the **no** form of this command.

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

Syntax Description

ip-address	The IP address that you want to assign to the virtual load-balancing cluster.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode and configure the interface to which the virtual cluster IP address refers.

The cluster IP address must be on the same subnet as the interface for which you are configuring the virtual cluster.

In the **no** form of the command, if you specify the optional *ip-address* value, it must match the existing cluster IP address before the **no cluster ip address** command can be completed.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster ip address** command that sets the IP address of the virtual load-balancing cluster to 209.165.202.224:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
interface	Sets the interfaces of the device.
nameif	Assigns a name to an interface.
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster key

To set the shared secret for IPsec site-to-site tunnel exchanges on the virtual load-balancing cluster, use the **cluster key** command in vpn load-balancing configuration mode. To remove this specification, use the **no** form of this command.

cluster key *shared-secret*

no cluster key [*shared-secret*]

Syntax Description

shared-secret	A 3- through 17-character string that defines the shared secret for the VPN load-balancing cluster. Special characters can appear in the string, but not spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode. The shared secret defined in the **cluster key** command is also used for cluster encryption.

You must use the **cluster key** command to configure the shared secret before enabling cluster encryption.

If you specify a value for *shared-secret* in the **no cluster key** form of the command, the shared secret value must match the existing configuration.

Examples

The following example shows a VPN load-balancing command sequence that includes a **cluster key** command to set the shared secret of the virtual load-balancing cluster to 123456789:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enters vpn load-balancing configuration mode.

cluster master unit

To set a new unit as the master unit of an ASA cluster, use the **cluster master unit** command in privileged EXEC mode.

cluster master unit *unit_name*

Caution The best method to change the master unit is to disable clustering on the master unit (see the **no cluster enable** command), waiting for a new master election, and then re-enabling clustering. If you must specify the exact unit you want to become the master, use the **cluster master unit** command. Note, however, that for centralized features, if you force a master unit change using this command, then all connections are dropped, and you have to re-establish the connections on the new master unit.

Syntax Description

unit_name	Specifies the local unit name to be the new master unit. To view member names, enter **cluster master unit ?** (to see all names except the current unit), or enter the **show cluster info** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

You will need to reconnect to the main cluster IP address.

Examples

The following example sets asa2 as the master unit:

```
hostname# cluster master unit asa2
```

Related Commands

Command	Description
cluster exec	Sends a command to all cluster members.

Command	Description
cluster group	Configures a cluster.
cluster remove unit	Removes the unit from the cluster.

cluster remove unit

To remove the unit from the ASA cluster, use the cluster remove unit command in privileged EXEC mode.

cluster remove unit *unit_name*

Syntax Description

unit_name	Specifies the local unit name to removes from the cluster. To view member names, enter **cluster remove unit ?**, or enter the **show cluster info** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

The bootstrap configuration remains intact, as well as the last configuration synced from the master unit, so you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

Examples

The following example checks for unit names, and then removes asa2 from the cluster:

```
hostname(config)# cluster remove unit ?

Current active units in the cluster:
asa2

hostname(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

Related Commands

Command	Description
cluster exec	Sends a command to all cluster members.
cluster group	Configures a cluster.
cluster master unit	Sets a new unit as the master unit of an ASA cluster.

cluster-interface

To specify the cluster control link physical interface and IP address, use the **cluster-interface** command in cluster group configuration mode. To remove the cluster interface, use the **no** form of this command.

cluster-interface *interface_id* **ip** *ip_address mask*

no cluster-interface [*interface_id* **ip** *ip_address mask*]

Syntax Description

interface_id	Specifies a physical interface, an EtherChannel, or a redundant interface. Subinterfaces and Management interfaces are not allowed. This interface cannot have a **nameif** configured. For the ASA 5585-X with an IPS module, you cannot use the IPS module interfaces for the cluster control link.
ip *ip_address mask*	Specify an IPv4 address for the IP address; IPv6 is not supported for this interface. For each unit, specify a different IP address on the same network.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cluster group configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

You need to enable the cluster control link interface before you join the cluster.

We recommend that you combine multiple cluster control link interfaces into an EtherChannel if you have enough interfaces. The EtherChannel is local to the ASA, and is not a spanned EtherChannel. We recommend that you use a Ten Gigabit Ethernet interface for the cluster control link. We recommend using the On mode for EtherChannel member interfaces to reduce unnecessary traffic on the cluster control link. The cluster control link does not need the overhead of LACP traffic because it is an isolated, stable network.

The cluster control link interface configuration is not replicated from the master unit to slave units; however, you must use the same configuration on each unit. Because this configuration is not replicated, you must configure the cluster control link interfaces separately on each unit.

See the configuration guide for more information about the cluster control link.

Examples

The following example creates an EtherChannel, Port-channel 2, for TenGigabitEthernet 0/6 and TenGigabitEthernet 0/7, and then assigns the port channel as the cluster control link. The port-channel interface is created automatically when you assign an interface to the channel group.

```
interface tengigabitethernet 0/6
    channel-group 2 mode on
    no shutdown

interface tengigabitethernet 0/7
    channel-group 2 mode on
    no shutdown

cluster group cluster1
    cluster-interface port-channel2 ip 10.1.1.1 255.255.255.0
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

cluster-mode

To specify the security mode of the cluster, use the **cluster-mode** command in phone-proxy configuration mode. To set the security mode of the cluster to the default mode, use the **no** form of this command.

cluster-mode [**mixed** | **nonsecure**]

no cluster-mode [**mixed** | **nonsecure**]

Syntax Description

mixed	Specifies the cluster mode to be in mixed mode when configuring the Phone Proxy feature.
nonsecure	Specifies the cluster mode to be in nonsecure mode when configuring the Phone Proxy feature.

Defaults

The default cluster mode is nonsecure.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

When you are configuring the Phone Proxy to run in mixed-mode clusters (both secure and nonsecure modes), you must also configure the LDC issuer in case some phones are configured to be in authenticated or encrypted mode:

```
hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024
hostname(config)# crypto key generate rsa label phone_common modulus 1024
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point internal_PP_myctl
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

Examples

The following example sets the security mode of the Phone Proxy to mixed (the IP phones will operate in secure and nonsecure modes):

```
hostname(config-phone-proxy)# cluster-mode mixed
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.
tls-proxy	Configures the TLS Proxy instance.

cluster port

To set the UDP port for the virtual load-balancing cluster, use the **cluster port** command in vpn load-balancing configuration mode. To remove the port specification, use the **no** form of this command.

cluster port *port*

no cluster port [*port*]

Syntax Description

port	The UDP port that you want to assign to the virtual load-balancing cluster.

Defaults

The default cluster port is 9023.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Vpn load-balancing configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must first use the **vpn load-balancing** command to enter vpn load-balancing configuration mode.

You can specify any valid UDP port number. The range is 1-65535.

If you specify a value for *port* in the **no cluster port** form of the command, the port number specified must match the existing configured port number.

Examples

The following example sets the UDP port for the virtual load-balancing cluster to 9023:

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enters vpn load-balancing configuration mode.

command-alias

To create an alias for a command, use the **command-alias** command in global configuration mode. To remove the alias, use the **no** form of this command.

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

Syntax Description

command_alias	Specifies the new name for an existing command.
mode	Specifies the command mode in which you want to create the command alias, for example **exec** (for user and privileged EXEC modes), **configure**, or **interface**.
original_command	Specifies the existing command or command with its keywords for which you want to create the command alias.

Defaults

By default, the following user EXEC mode aliases are configured:

- **h** for **help**
- **lo** for **logout**
- **p** for **ping**
- **s** for **show**

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you enter the command alias, the original command is invoked. You might want to create command aliases to provide shortcuts for long commands, for example.

You can create an alias for the first part of any command and still enter the additional keywords and arguments as normal.

When you use CLI help, command aliases are indicated by an asterisk (*), and displayed in the following format:

```
*command-alias=original-command
```

For example, the **lo** command alias displays along with other privileged EXEC mode commands that start with “lo,” as follows:

```
hostname# lo?
*lo=logout login  logout
```

You can use the same alias in different modes. For example, you can use “happy” in privileged EXEC mode and configuration mode to alias different commands, as follows:

```
hostname(config)# happy?

configure mode commands/options:
*happy="username employee1 password test"

exec mode commands/options:
*happy=enable
```

To list only commands and omit aliases, begin your input line with a space. Also, to circumvent command aliases, use a space before entering the command. In the following example, the alias named “happy” is not shown, because there is a space before the **happy?** command.

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#   happy?
ERROR: % Unrecognized command
```

As with commands, you can use CLI help to display the arguments and keywords that can follow a command alias.

You must enter the complete command alias. Shortened aliases are not accepted. In the following example, the parser does not recognize the **hap** command as indicating the alias named “happy”:

```
hostname# hap
% Ambiguous command: "hap"
```

Examples

The following example shows how to create a command alias named “save” for the **copy running-config startup-config** command:

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

Related Commands

Command	Description
clear configure command-alias	Clears all nondefault command aliases.
show running-config command-alias	Displays all nondefault command aliases configured.

command-queue

To specify the maximum number of MGCP commands that are queued while waiting for a response, use the **command-queue** command in mgcp-map configuration mode. To remove the configuration, use the **no** form of this command.

command-queue *limit*

no command-queue *limit*

Syntax Description

limit	Specifies the maximum number of commands to queue, from 1 to 2147483647.

Defaults

This command is disabled by default.

The default for the MGCP command queue is 200.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Mgcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **command-queue** command to specify the maximum number of MGCP commands that are queued while waiting for a response. The range of allowed values is from 1 to 4294967295. The default is 200. When the limit has been reached and a new command arrives, the command that has been in the queue for the longest time is removed.

Examples

The following example limits the MGCP command queue to 150 commands:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debugging information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.

Commands	Description
show mgcp	Displays MGCP configuration and session information.
timeout	Configures the idle timeout after which an MGCP media or MGCP PAT xlate connection will be closed.

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

compatible rfc1583

no compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Router configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Only the **no** form of this command appears in the configuration.

Examples

The following example shows how to disable an RFC 1583-compatible route summary cost calculation:

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

compression

To enable compression for SVC connections and WebVPN connections, use the **compression** command in global configuration mode. To remove the command from the configuration, use the **no** form of the command.

compression {**all** | **svc** | **http-comp**}

no compression {**all** | **svc** | **http-comp**}

Syntax Description

all	Specifies enabling all available compression techniques.
http-comp	Specifies compression for WebVPN connections.
svc	Specifies compression for SVC connections.

Defaults

The default is *all*. All available compression techniques are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•		—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

For SVC connections, the **compression** command configured in global configuration mode overrides the **svc compression** command configured in group policy webvpn and username webvpn configuration modes.

For example, if you enter the **svc compression** command for a certain group in group policy webvpn configuration mode, and then you enter the **no compression** command in global configuration mode, you override the **svc compression** command settings that you have configured for the group.

Conversely, if you turn compression back on with the **compression** command in global configuration mode, any group settings take effect, and those settings ultimately determine the compression behavior.

If you disable compression with the **no compression** command, only new connections are affected. Active connections remain unaffected.

Examples

In the following example, compression is turned on for SVC connections:

```
hostname(config)# compression svc
```

In the following example, compression is disabled for SVC and WebVPN connections:

```
hostname(config)# no compression svc http-comp
```

Related Commands

Command	Description
show webvpn svc	Displays information about the SVC installation.
svc	Enables or requires the SVC for a specific group or user.
svc compression	Enables compression of HTTP data over an SVC connection for a specific group or user.

config-register

To set the configuration register value that is used the next time you reload the ASA, use the **config-register** command in global configuration mode. To set the value back to the default, use the **no** form of this command.

config-register *hex_value*

no config-register

Syntax Description

hex_value	Sets the configuration register value as a hexadecimal number from 0x0 to 0xFFFFFFFF. This number represents 32 bits and each hexadecimal character represents 4 bits. Each bit controls a different characteristic. However, bits 32 through 20 are either reserved for future use, cannot be set by the user, or are not currently used by the ASA; therefore, you can ignore the three characters that represent those bits, because they are always set to 0. The relevent bits are represented by 5 hexadecimal characters: 0x*nnnnn*. You do not need to include preceding 0s. You do need to include trailing 0s. For example, 0x2001 is equivalent to 0x02001; but 0x10000 requires all the zeros. See Table 10-1 for more information about available values for the relevant bits.

Defaults

The default value is 0x1, which boots from the local image and startup configuration.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is only supported on the ASA 5500 series. The configuration register value determines which image to boot from as well as other boot parameters.

The five characters are numbered from 0 to 4 from right to left, which is standard for hexadecimal and binary numbers. You can select one value for each character, and mix and match values as appropriate. For example, you can select either 0 or 2 for character number 3. Some values take priority if they conflict with other values. For example, if you set 0x2011, which sets the ASA to both boot from the

TFTP server and to boot from the local image, the ASA boots from the TFTP server. Because this value also stipulates that if the TFTP boot fails, the ASA should boot directly into ROMMON, then the action that specifies to boot from the default image is ignored.

A value of 0 means no action unless otherwise specified.

Table 10-1 lists the actions associated with each hexadecimal character; choose one value for each character:

Table 10-1 Configuration Register Values

Prefix	Hexadecimal Character Numbers 4, 3, 2, 1, and 0				
0x	**0**	**0**	**0**[1]	**0**[2]	**0**[2]
	1 Disables the 10 second ROMMON countdown during startup. Normally, you can press Escape during the countdown to enter ROMMON.	**2** If you set the ASA to boot from a TFTP server, and the boot fails, then this value boots directly into ROMMON.		**1** Boots from the TFTP server image as specified in the ROMMON Boot Parameters (which is the same as the **boot system tftp** command, if present). This value takes precedence over a value set for character 1.	**1** Boots the image specified by the first **boot system** *local_flash* command. If that image does not load, the ASA tries to boot each image specified by subsequent **boot system** commands until it boots successfully.
					2, 4, 6, 8 Boots the image specified by a particular **boot system** *local_flash* command. Value 3 boots the image specified in the first **boot system** command, value 5 boots the second image, and so on. If the image does not boot successfully, the ASA does not attempt to fall back to other **boot system** command images (this is the difference between using value 1 and value 3). However, the ASA has a failsafe feature that in the event of a boot failure attempts to boot from any image found in the root directory of internal flash memory. If you do not want the failsafe feature to take effect, store your images in a different directory than root.
				4[3] Ignores the startup configuration and loads the default configuration.	**2, 4, 6, 8** From ROMMON, if you enter the **boot** command without any arguments, then the ASA boots the image specified by a particular **boot system** *local_flash* command. Value 3 boots the image specified in the first **boot system** command, value 5 boots the second image, and so on. This value does not automatically boot an image.
				5 Performs both actions above.	

[1] Reserved for future use.

[2] If character numbers 0 and 1 are not set to automatically boot an image, then the ASA boots directly into ROMMON.

[3] If you disable password recovery using the **service password-recovery** command, then you cannot set the configuration register to ignore the startup configuration.

The configuration register value is not replicated to a standby unit, but the following warning is displayed when you set the configuration register on the active unit:

```
WARNING The configuration register is not synchronized with the standby, their values may
not match.
```

You can also set the configuration register value in ROMMON using the **confreg** command.

Examples

The following example sets the configuration register to boot from the default image:

```
hostname(config)# config-register 0x1
```

Related Commands

Command	Description
boot	Sets the boot image and startup configuration.
service password-recovery	Enables or disables password recovery.

configure factory-default

To restore the configuration to the factory default, use the **configure factory-default** command in global configuration mode.

configure factory-default [*ip_address* [*mask*]]

Syntax Description

ip_address	Sets the IP address of the management or inside interface, instead of using the default address, 192.168.1.1. See the "Usage Guidelines" sections for more information about which interface is configured for your model.
mask	Sets the subnet mask of the interface. If you do not set a mask, the ASA uses the mask appropriate for the IP address class.

Defaults

The default IP address and mask are 192.168.1.1 and 255.255.255.0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	A factory default configuration was added for the ASA 5505.

Usage Guidelines

The factory default configuration is the configuration applied by Cisco to new ASAs. This command is supported on all platforms except for the PIX 525 and PIX 535 ASAs.

For the PIX 515/515E and the ASA 5510 and higher ASAs, the factory default configuration automatically configures a management interface so you can connect to it using ASDM, with which you can then complete your configuration. For the ASA 5505, the factory default configuration automatically configures interfaces and NAT so that the ASA is ready to use in your network.

This command is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces, and setting the interface IP address is one of the actions this command takes. This command is also only available in single context mode; an ASA with a cleared configuration does not have any defined contexts to automatically configure using this command.

This command clears the current running configuration and then configures several commands.

If you set the IP address in the **configure factory-default** command, then the **http** command uses the subnet that you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.

After you restore the factory default configuration, save it to internal flash memory using the **write memory** command. The **write memory** command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared.

Note This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external flash memory card. The next time you reload the ASA after restoring the factory configuration, it boots from the first image in internal flash memory; if you do not have an image in internal flash memory, the ASA does not boot.

To configure additional settings that are useful for a full configuration, see the **setup** command.

ASA 5505 Configuration

The default factory configuration for the ASA 5505 configures the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. If you did not set the IP address in the **configure factory-default** command, then the VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- The default route is also derived from DHCP.
- All inside IP addresses are translated when accessing the outside using interface PAT.
- By default, inside users can access the outside with an access list, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the ASA, so a PC connecting to the VLAN 1 interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
```

```
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 and Higher Configuration

The default factory configuration for the ASA 5510 and higher configures the following:

- The management Management 0/0 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the ASA, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E Security Appliance Configuration

The default factory configuration for the PIX 515/515E security appliance configures the following:

- The inside Ethernet1 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the PIX security appliance, so a PC connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
```

```
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Examples

The following example resets the configuration to the factory default, assigns the IP address 10.1.1.1 to the interface, and then saves the new configuration as the startup configuration:

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

Related Commands

Command	Description
boot system	Sets the software image from which to boot.
clear configure	Clears the running configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
setup	Prompts you to configure basic settings for the ASA.
show running-config	Shows the running configuration.

configure http

To merge a configuration file from an HTTP(S) server with the running configuration, use the **configure http** command in global configuration mode.

configure http[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*]**/**[*path***/**]*filename*

Syntax Description

:password	(Optional) For HTTP(S) authentication, specifies the password.
:*port*	(Optional) Specifies the port. For HTTP, the default is 80. For HTTPS, the default is 443.
@	(Optional) If you enter a name and/or a password, precedes the server IP address with an at sign (@).
filename	Specifies the configuration filename.
http[**s**]	Specifies either HTTP or HTTPS.
path	(Optional) Specifies a path to the filename.
server	Specifies the server IP address or name. For IPv6 server addresses, if you specify the port, then you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the port number. For example, enter the following address and port: `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	(Optional) For HTTP(S) authentication, specifies the username.

Defaults

For HTTP, the default port is 80. For HTTPS, the default port is 443.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command supports IPv4 and IPv6 addresses. A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration, but are not set in the new configuration.

This command is the same as the **copy http running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure http** command is an alternative for use within a context.

Examples

The following example copies a configuration file from an HTTPS server to the running configuration:

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands that you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure memory

To merge the startup configuration with the running configuration, use the **configure memory** command in global configuration mode.

configure memory

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration, but are not set in the new configuration.

If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the ASA, and then enter the **configure memory** command to load the new configuration.

This command is equivalent to the **copy startup-config running-config** command.

For multiple context mode, a context startup configuration is at the location specified by the **config-url** command.

Examples

The following example copies the startup configuration to the running configuration:

```
hostname(config)# configure memory
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands that you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure net

To merge a configuration file from a TFTP server with the running configuration, use the **configure net** command in global configuration mode.

configure net [*server*:[*filename*] | :*filename*]

Syntax Description

:*filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional. If you specify the filename in this command as well as a name in the **tftp-server** command, the ASA treats the **tftp-server** command filename as a directory, and adds the **configure net** command filename as a file under the directory. To override the **tftp-server** command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
server:	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. For IPv6 server addresses, you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the filename. For example, enter the following address: [fe80::2e0:b6ff:fe01:3b7a] The default gateway interface is the highest security interface; however, you can set a different interface name using the **tftp-server** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command supports IPv4 and IPv6 addresses. A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration, but are not set in the new configuration.

This command is the same as the **copy tftp running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure net** command is an alternative for use within a context.

Examples

The following example sets the server and filename in the **tftp-server** command, and then overrides the server using the **configure net** command. The same filename is used.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

The following example overrides the server and the filename. The default path to the filename is /tftpboot/configs/config1. The /tftpboot/ part of the path is included by default when you do not lead the filename with a slash (/). Because you want to override this path, and the file is also in tftpboot, include the tftpboot path in the **configure net** command.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

The following example sets the server only in the **tftp-server** command. The **configure net** command specifies only the filename.

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

Related Commands

Command	Description
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write net	Copies the running configuration to a TFTP server.

configure terminal

To configure the running configuration at the command line, use the **configure terminal** command in privileged EXEC mode.

configure terminal

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command enters global configuration mode, which lets you enter commands that change the configuration.

Examples

The following example enters global configuration mode:

```
hostname# configure terminal
hostname(config)#
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.

config-url

To identify the URL from which the system downloads the context configuration, use the **config-url** command in context configuration mode.

config-url *url*

Syntax Description

url — Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax:

- **disk0:/**[*path***/**]*filename*

  For the ASA 5500 series, this URL indicates the internal flash memory. You can also use the **flash** command instead of the **disk0** command; they are aliased.

- **disk1:/**[*path***/**]*filename*

  For the ASA 5500 series, this URL indicates the external flash memory card.

- **flash:/**[*path***/**]*filename*

  This URL indicates the internal flash memory.

- **ftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path***/**]*filename*[**;type=***xx*]

  The **type** can be one of the following keywords:

  - **ap**—ASCII passive mode
  - **an**—ASCII normal mode
  - **ip**—(Default) Binary passive mode
  - **in**—Binary normal mode

- **http**[**s**]**://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path***/**]*filename*

- **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path***/**]*filename*[**;int=***interface_name*]

  Specify the interface name if you want to override the route to the server address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you add a context URL, the system immediately loads the context so that it is running.

Note Enter the **allocate-interface** command(s) before you enter the **config-url** command. The ASA must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**interface**, **nat**, **global**). If you enter the **config-url** command first, the ASA loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

The filename does not require a file extension, although we recommend using ".cfg."

The admin context file must be stored on the internal flash memory.

If you download a context configuration from an HTTP or HTTPS server, you cannot save changes back to these servers using the **copy running-config startup-config** command. You can, however, use the **copy tftp** command to copy the running configuration to a TFTP server.

If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure with the command-line interface.

To change the URL, reenter the **config-url** command with a new URL.

The ASA merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used. If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

Examples

The following example sets the admin context to "administrator," creates a context called "administrator" on the internal flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Allocates interfaces to a context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

conn-rebalance

To enable connection rebalancing between members of a cluster, use the **conn-rebalance** command in cluster group configuration mode. To disable connection rebalancing, use the **no** form of this command.

conn-rebalance [**frequency** *seconds*]

no conn-rebalance [**frequency** *seconds*]

Syntax Description

frequency *seconds*	(Optional) Sepcifies how often the load information is exchanged, between 1 and 360 seconds. The default is 5 seconds.

Command Default

Connection rebalancing is disabled by default.

If enabled, the default frequency is 5 seconds

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cluster group configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

If the load balancing capabilities of the upstream or downstream routers result in unbalanced flow distribution, you can configure overloaded units to redirect new flows to other units. No existing flows will be moved to other units. If enabled, ASAs exchange load information periodically, and offload new connections from more loaded devices to less loaded devices.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example sets the connection rebalance frequency to 60 seconds:

```
hostname(cfg-cluster)# conn-rebalance frequency 60
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

console timeout

To set the inactivity timeout for an authenticated serial console session (**aaa authentication serial console**) so that a user is logged out of the console after the timeout, or for an authenticated enable session (**aaa authentication enable console**) where the user exits privileged EXEC mode and reverts to user EXEC mode after the timeout, use the **console timeout** command in global configuration mode. To disable the inactivity timeout for an authenticated serial console session, use the **no** form of this command.

console timeout [*number*]

no console timeout [*number*]

Syntax Description

number	Specifies the idle time in minutes (0 through 60) after which the console session ends. 0 means the console never times out.

Defaults

The default timeout is 0, which means the console session will not time out.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **console timeout** command only applies to authenticated serial or enable connections. This command does not alter the Telnet, SSH, or HTTP timeouts; these access methods maintain their own timeout values. The command does not affect unauthenticated console connections.

The **no console timeout** command resets the console timeout value to the default timeout of 0, which means that the console will not time out.

Examples

The following example shows how to set the console timeout to 15 minutes:

```
hostname(config)# console timeout 15
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.
show running-config console timeout	Displays the idle timeout for a console connection to the ASA.

console-replicate

To enable console replication from slave units to the master unit in an ASA cluster, use the **console-replicate** command in cluster group configuration mode. To disable console replication, use the **no** form of this command.

console-replicate

no console-replicate

Syntax Description

This command has no arguments or keywords.

Command Default

Console replication is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Cluster group configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

The ASA prints out some messages directly to the console for certain critical events. If you enable console replication, slave units send the console messages to the master unit so you only need to monitor one console port for the cluster.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units.

Examples

The following example enables console replication:

```
hostname(config)# cluster group cluster1
hostname(cfg-cluster)# console-replicate
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.

Command	Description
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

content-length

To restrict HTTP traffic based on the length of the HTTP message body, use the **content-length** command in http-map configuration mode. To remove this command, use the **no** form of this command.

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a message fails this inspection.
allow	Allows the message.
bytes	Specifies the number of bytes. The permitted range is 1 to 65535 for the **min** option and 1 to 50000000 for the **max** option.
drop	Closes the connection.
log	(Optional) Generates a syslog.
max	(Optional) Specifies the maximum content length allowed.
min	Specifies the minimum content length allowed.
reset	Sends a TCP reset message to the client and server.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Http-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After enabling the **content-length** command, the ASA only allows messages within the configured range and otherwise takes the specified action. Use the **action** keyword to cause the ASA to reset the TCP connection and create a syslog entry.

Examples

The following example restricts HTTP traffic to messages 100 bytes or larger and not exceeding 2000 bytes. If a message is outside this range, the ASA resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

context

To create a security context in the system configuration and enter context configuration mode, use the **context** command in global configuration mode. To remove a context, use the **no** form of this command.

context *name*

no context *name* [**noconfirm**]

Syntax Description

name	Sets the name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. "System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.
noconfirm	(Optional) Removes the context without prompting you for confirmation. This option is useful for automated scripts.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In context configuration mode, you can identify the configuration file URL and interfaces that a context can use. If you do not have an admin context (for example, if you clear the configuration), then the first context you add must be the admin context. To add an admin context, see the **admin-context** command. After you specify the admin context, you can enter the **context** command to configure the admin context.

You can only remove a context by editing the system configuration. You cannot remove the current admin context using the **no** form of this command; you can only remove it if you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to "administrator," creates a context called "administrator" on the internal flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts and the system execution space.
config-url	Specifies the location of the context configuration.
join-failover-group	Assigns a context to a failover group.
show context	Shows context information.

copy

To copy a file from one location to another, use the **copy** command in privileged EXEC mode.

[**cluster exec**] **copy** [**/noconfirm** | **/pcap**] {*url* | **running-config** | **startup-config**} {**running-config** | **startup-config** | *url*}

Syntax Description

cluster exec	(Optional) Enables you to enter the **copy** command on one unit and then simultaneously apply it to all other units in a clustering deployment. (See the "Usage Guidelines" section for more information.)
/noconfirm	Copies the file without a confirmation prompt.
/pcap	Specifies the preconfigured TFTP server defaults. See the **tftp-server** command to configure a default TFTP server.
running-config	Specifies the running configuration stored in memory.
startup-config	Specifies the startup configuration stored in flash memory. The startup configuration for single mode or for the system in multiple context mode is a hidden file in flash memory. From within a context, the location of the startup configuration is specified by the **config-url** command. For example, if you specify an HTTP server for the **config-url** command and then enter the **copy startup-config running-config** command, the ASA copies the startup configuration from the HTTP server using the admin context interface.

url

Specifies the source or destination file to be copied between local and remote locations. (You cannot copy from a remote server to another remote server.) In a context, you can copy the running or startup configuration to a TFTP or FTP server using the context interfaces, but you cannot copy from a server to the running or startup configuration. See the **startup-config** keyword for other options. To download from a TFTP server to the running context configuration, use the **configure net** command. Use the following URL syntax for this command:

- **cache:/**[*path***/**]*filename*]—Indicates the cache memory in the file system.
- **capture:/**[*path***/**]*filename*]—Indicates the output in the capture buffer.
- **disk0:/**[*path***/**]*filename*] or **flash:/**[*path***/**]*filename*]—ASA 5500 series only. Both **flash** and **disk0** indicate the internal flash memory. Can use either option.
- **disk1:/**[*path***/**]*filename*]—ASA 5500 series only. Indicates external memory.
- **smb:/**[*path***/**]*filename*]—Indicates a UNIX server local file system. Use Server Message Block file-system protocol in LAN managers and similar network systems to package data and exchange information with other systems.
- **ftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path***/**]*filename*[**;type=***xx*]—The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default—Binary passive mode), **in** (Binary normal mode).
- **http**[**s**]**://**[*user*[**:***password*]@]*server*[**:***port*]**/**[*path***/**]*filename*]
- **system:/**[*path***/**]*filename*]—Indicates the system memory in the file system.
- **tftp://**[*user*[**:***password*]@]*server*[**:***port*]**/**[*path***/**]*filename*[**;int=***interface_name*]

  The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command. Specify the interface name using the **nameif interface** command if you want to override the route to the server address.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Added support for DNS names.
8.0(2)	Added the **smb:** URL option.
9.0(1)	Added the **cluster exec** option.

Usage Guidelines

- When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.
  If an RSA key cannot be saved in NVRAM, the following error message appears:

  ```
  ERROR: NV RAM does not have enough space to save keypair keypair name
  ```

- After you have performed a cluster-wide capture, you can simultaneously copy the same capture file from all units in the cluster to a TFTP server by entering the following command on the master unit:

  ```
  hostname (config-cluster)# cluster exec copy /pcap capture: cap_name
  tftp://location/path/filename.pcap
  ```

  Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, where A and B are cluster unit names.

  Note A different destination name gets generated if you add the unit name at the end of the filename.

Examples

The following example shows how to copy a file from the disk to a TFTP server in the system execution space:

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

The following example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
hostname(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

The following example shows how to copy an ASDM file from a TFTP server to the internal flash memory:

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

The following example shows how to copy the running configuration in a context to a TFTP server:

```
hostname(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

The **copy** command supports DNS names as well as IP addresses, as shown in this version of the preceding example:

```
hostname(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

Related Commands

Command	Description
configure net	Copies a file from a TFTP server to the running configuration.
copy capture	Copies a capture file to a TFTP server.
tftp-server	Sets the default TFTP server.
write memory	Saves the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

copy capture

To copy a capture file to a server, use the **copy capture** command in privileged EXEC mode.

copy [**/noconfirm**] [**/pcap**] **capture:** [*context_name/*]*buffer_name url*

Syntax Description

/noconfirm	Copies the file without a confirmation prompt.
/pcap	Copies the packet capture as raw data.
buffer_name	Unique name that identifies the capture.
context_name/	Copies a packet capture defined in a security context.
url	Specifies the destination to copy the packet capture file. See the following URL syntax: • **disk0:/**[*path/*]*filename* This option is only available for the ASA, and indicates the internal Flash card. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:/**[*path/*]*filename* This option is only available for the ASA, and indicates the external Flash card. • **flash:/**[*path/*]*filename* This option indicates the internal flash card. For the ASA, **flash** is an alias for **disk0**. • **ftp://**[*user*[:*password*]@]*server*[:*port*]/[*path/*]*filename*[;**type=***xx*] The **type** can be one of the following keywords: – **ap**—ASCII passive mode – **an**—ASCII normal mode – **ip**—(Default) Binary passive mode – **in**—Binary normal mode • **http**[**s**]**://**[*user*[:*password*]@]*server*[:*port*]/[*path/*]*filename* • **tftp://**[*user*[:*password*]@]*server*[:*port*]/[*path/*]*filename*[;**int=***interface_name*] Specify the interface name if you want to override the route to the server address. The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
hostname(config)# copy capture:abc tftp
Address or name of remote host [209.165.200.224]?
Source file name [username/cdisk]?
copying capture to tftp://209.165.200.224/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

You can specify the full path as follows:

```
hostname(config)# copy capture:abc tftp:209.165.200.224/tftpboot/abc.cap
```

If the TFTP server is already configured, the location or filename can be unspecified as follows:

```
hostname(config)# tftp-server outside 209.165.200.224 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
show capture	Displays the capture configuration when no options are specified.

cpu profile activate

To start CPU profiling, use the **cpu profile activate** command in privileged EXEC mode.

cpu profile activate *n-samples* [**sample-process** *process-name*] [**trigger cpu-usage** *cpu %* [*process-name*]]

Syntax Description

n-samples	Allocates memory for storing *n* number of samples. Valid values are from 1 to 100,000.
sample-process *process-name*	Samples only a specific process.
trigger cpu-usage *cpu %*	Prevents the profiler from starting until the global 5-second CPU percentage is greater and stops the profiler if the CPU percentage drops below this value.
trigger cpu-usage *cpu % process-name*	Uses the process 5-second CPU percentage as a trigger.

Defaults

The *n-samples* default value is 1000.

The *cpu %* default value is 0.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
9.1(2)	The **sample-process** *process-name*, **trigger cpu-usage** *cpu %*, and **trigger cpu-usage** *cpu % process-name* options were added. The output format was updated.

Usage Guidelines

The CPU profiler can help you determine which process is using more CPU. Profiling the CPU captures the address of the process that was running on the CPU when the timer interrupt fired. This profiling occurs every 10 milliseconds, regardless of the CPU load. For example, if you take 5000 samples, the profiling takes exactly 50 seconds to complete. If the amount of CPU time that the CPU profiler uses is relatively low, the samples take longer to collect. The CPU profile records are sampled in a separate buffer.

Use the **show cpu profile** command in conjunction with the **cpu profile activate** command to display information that you can collect and that the TAC can use for troubleshooting CPU issues. The **show cpu profile dump** command output is in hexadecimal format.

If the CPU profiler is waiting for a starting condition to occur, the **show cpu profile** command displays the following output:

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

Examples

The following example activates the profiler and instructs it to store 1000 samples.

```
hostname# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

The following examples show the status of the profiing (in-progress and completed):

```
hostname# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.

hostname# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2

Process virtual address map:
---------------------------
…
---------------------------
End of process map
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

Related Commands

Command	Description
show cpu profile	Displays the CPU profiling progress.
show cpu profile dump	Displays incomplete or completed results for profiling.

coredump enable

To enable the coredump feature, enter the **coredump enable** command. To disable the command, use the **no** form of this command.

coredump enable [**filesystem** [**disk0**: | **disk1**: | **flash**:] [**size** [**default** | **size_in_MB**]]

[**no**] **coredump enable** [**filesystem** [**disk0**: | **disk1**: | **flash**:] [**size** [**default** | **size_in_MB**]]

Syntax Description

default	Specifies the default is the suggested value to use, because the ASA calculates what this value should be.
filesystem disk0: | disk1: | flash:	Specifies the disk where the coredump file will be saved.
size	Defines the total size allocated for the coredump file system image on the ASA flash. When configuring coredump, if not enough space is available, an error message appears. It may be helpful to think of the **size** option as a container, which means that coredumps generated will never be allowed to exceed this size in disk space consumption.
size_in_MB	Specifies that the ASA will override the default value and allocate the specified value in MB for the coredump filesystem (if the space is available).

Defaults

By default, coredumps are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	—	—	•

Command History

Release	**Modification**
8.2(1)	This command was introduced.

Usage Guidelines

Enabling this feature provides significant troubleshooting information. Disabling this feature results in a coredump file not being generated on a system crash for all components. In addition, disabling this feature does not delete a previous coredump filesystem image and/or the coredump filesystem image contents. When you enable coredumps, you are prompted to allow the coredump filesystem to be created. The prompt is a confirmation and includes the size (in MB) of the coredump filesystem to be created. It is important that you save your configuration after enabling or disabling coredumps.

When coredumps are enabled, the following file elements get created. You should never manipulate these file elements explicitly.

- coredumpfsys – Directory that includes coredump images
- coredumpfsysimage.bin – Coredump filesystem image used to manage coredumps
- coredumpinfo – Directory that includes the coredump log

Note Disabling coredumps has no effect on crashinfo file generation.

Cisco TAC may request that you enable the coredump feature to troubleshoot application or system crashes on the ASA.

Note Make sure that you archive the coredump files, because it is possible a subsequent coredump may result in previous coredump(s) being removed to fit the current coredump. Coredump files are located on the configured filesystem (for example, “disk0:/coredumpfsys” or “disk1:/coredumpfsys”) and can be removed from the ASA.

To enable coredump, perform the following steps:

1. Make sure that you are in the /root directory. To verify your directory location on the console, enter the **pwd** command.
2. If necessary, change the directory by entering either the **cd disk0:/**, **cd disk1:/**, or **cd flash:/** command.
3. Enter the **coredump enable** command.

When using the **coredump** command to troubleshoot crashes on the ASA, it is possible that no coredump file is saved after a crash. This can occur when the coredump feature has been enabled and a coredump filesystem with preallocated disk space has been created. This condition usually appears while troubleshooting crashes that occur after a few weeks on busy ASAs that have allocated a large amount of RAM.

In the output of the **show coredump** command, something similar to the following appears:

```
Coredump Aborted as the complete coredump could not be written to flash
   Filesystem full on 'disk0', current coredump size <size> bytes too big for allocated
   filesystem
```

To alleviate this issue, you need to have a coredump filesystem card that is large enough to contain the full memory and allocate corresponding space to the coredump filesystem.

Examples

Each bang (!) in these examples represents 1 MB of the coredump filesystem being written.

The following example uses default values and **disk0:** to create the coredump filesystem.

```
hostname(config)# coredump enable
Warning: Enabling coredump on an ASA5505 platform will delay the reload of the system in
the event of software forced reload. The exact time depends on the size of the coredump
generated.
Proceed with coredump filesystem allocation of 60 MB on 'disk0:' (Note this may take a
while) [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following example shows how to specify the filesystem and size by creating a 120-MB coredump filesystem on **disk1:**

```
hostname(config)# coredump enable filesystem disk1: size 120
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceed with coredump filesystem allocation of 120 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The following example shows how to resize the coredump filesystem from 120 MB to 100 MB:

Note The contents of the 120-MB coredump filesystem are not preserved, so make sure that you archive previous coredumps before doing this.

```
hostname(config)# coredump enable filesystem disk1: size 100
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Proceeding with resizing to 100 MB results in
deletion of current 120 MB coredump filesystem and
its contents on 'disk1:', proceed ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
```

The following example enables coredump initially on **disk0:**, then on **disk1:**. Also note the use of the **default** keyword.

Note We do not allow two active coredump filesystems, so you must delete the previous coredump filesystem before proceeding.

```
hostname(config)# coredump enable filesystem disk1: size default
WARNING: Enabling coredump on an ASA5540 platform will delay
the reload of the system in the event of software forced reload.
The exact time depends on the size of the coredump generated.
Coredump is currently configured on 'disk0:', upon successful
configuration on 'disk1:', the coredump filesystem will be
deleted on 'disk0:', proceed ? [confirm]
Proceed with coredump filesystem allocation of 100 MB
on 'disk1:' (Note this may take a while) ? [confirm]
Making coredump file system
image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!
```

The following example shows how to disable the coredump filesystem. However, the current coredump filesystem image and its contents are not affected.

```
hostname(config)# no coredump enable
```

To reenable coredumps, reenter the command you originally used to configure the coredump filesystem.

The following examples disable and reenable coredumps:

- Using default values:

  ```
  hostname(config)# coredump enable
  ```

```
hostname(config)# no coredump enable
hostname(config)# coredump enable
```

- Using explicit values:

```
hostname(config)# coredump enable filesystem disk1: size 200
hostname(config)# no coredump enable
hostname(config)# coredump enable filesystem disk1: size 200
```

Related Commands

Command	Description
clear configure coredump	Removes the coredump filesystem and its contents from your system. Also clears the coredump log.
clear coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log.
show coredump filesystem	Displays files on the coredump filesystem and indicates how full it might be.
show coredump log	Shows the coredump log.

crashinfo console disable

To suppress crash information from being output to the console, use the **crashinfo console disable** command in global configuration mode.

crashinfo console disable

no crashinfo console disable

Syntax Description

disable	Suppresses console output in the event of a crash.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

This command lets you suppress crash information from being output to the console. The crash information may contain sensitive information that is not appropriate for viewing by all users connected to the device. In conjunction with this command, you should also ensure crash information is written to flash, which can be examined after the device reboots. This command affects output for crash information and checkheaps, which is saved to flash and should be sufficient for troubleshooting.

Examples

The following example shows how to suppress crash information from being output to the console:

```
hostname(config)# crashinfo console disable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
fips enable	Enables or disables policy checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.

Command	Description
show crashinfo console	Reads, writes, and configures crash information output to flash.
show running-config fips	Displays the FIPS configuration that is running on the ASA.

crashinfo force

To force the ASA to crash, use the **crashinfo force** command in privileged EXEC mode.

crashinfo force [**page-fault** | **watchdog**]

Syntax Description

page-fault	(Optional) Forces a crash of the ASA as a result of a page fault.
watchdog	(Optional) Forces a crash of the ASA as a result of watchdogging.

Defaults

The ASA saves the crash information file to flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can use the **crashinfo force** command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashinfo force page-fault** or **crashinfo force watchdog** command (because these are real crashes). The ASA reloads after the crash dump is complete.

Caution Do not use the **crashinfo force** command in a production environment. The **crashinfo force** command crashes the ASA and forces it to reload.

Examples

The following example shows the warning that displays when you enter the **crashinfo force page-fault** command:

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

If you enter a carriage return (by pressing the Return or Enter key on your keyboard), “Y,” or “y,” the ASA crashes and reloads; any of these responses are interpreted as confirmation. Any other character is interpreted as a no, and the ASA returns to the command-line prompt.

Related Commands

clear crashinfo	Clears the contents of the crash information file.
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the crash information file.

crashinfo save disable

To disable crash information from writing to flash memory, use the **crashinfo save** command in global configuration mode. To allow the crash information to be written to flash memory and return to the default behavior, use the **no** form of this command.

crashinfo save disable

no crashinfo save disable

Syntax Description

This command has no arguments or keywords.

Defaults

The ASA saves the crash information file to flash memory by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	The **crashinfo save enable** command was deprecated. Use the **no crashinfo save disable** command instead.

Usage Guidelines

Crash information writes to flash memory first, and then to the console.

Note If the ASA crashes during startup, the crash information file is not saved. The ASA must be fully initialized and running first before it can save crash information to flash memory.

Use the **no crashinfo save disable** command to reenable saving the crash information to flash memory.

Examples

The following example shows how to disable crash information from writing to flash memory:

```
hostname(config)# crashinfo save disable
```

Related Commands

clear crashinfo	Clears the contents of the crash file.
crashinfo force	Forces a crash of the ASA.

crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo	Displays the contents of the crash file.

crashinfo test

To test the ability of the ASA to save crash information to a file in flash memory, use the **crashinfo test** command in privileged EXEC mode.

crashinfo test

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If a previous crash information file already exists in flash memory, that file is overwritten.

Note Entering the **crashinfo test** command does not crash the ASA.

Examples

The following example shows the output of a crash information file test.:

```
hostname# crashinfo test
```

Related Commands

clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces the ASA to crash.
crashinfo save disable	Disables crash information from writing to flash memory.
show crashinfo	Displays the contents of the crash file.

crl

To specify CRL configuration options, use the **crl** command in crypto ca trustpoint configuration mode.

crl {**required** | **optional** | **nocheck**}

Syntax Description

nocheck	Directs the ASA not to perform CRL checking.
optional	The ASA can still accept the peer certificate if the required CRL is not available.
required	The required CRL must be available for a peer certificate to be validated.

Defaults

The default value is **nocheck**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	This command was deprecated. The following forms of the **revocation-check** command replace it. • **revocation-check crl none** replaces **crl optional** • **revocation-check crl** replaces **crl required** • **revocation-check none** replaces **crl nocheck**

Examples

The following example enters crypto ca trustpoint configuration mode for a trustpoint central, and requires that a CRL be available for a peer certificate to be validated for this trustpoint:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters crypto ca trustpoint configuration mode.

Command	Description
crl configure	Enters crl configuration mode.
url	Specifies a URL for the CRL retrieval.

crl cache-time

To configure the amount of time (minutes) that a trustpool CRL can remain in the CRL cache before the ASA refreshes it, use the **crl cache-time** command in ca-trustpool configuration mode. To accept the default value of 60 minutes, use the **no** form of this command.

crl cache-time

no crl cache-time

Syntax Description

cache-time	Value in minutes (1-1440).

Defaults

The default value is **60**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Ca-trustpool configuration	•	•	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

This command is consistent with the version of this command supported in the trustpoint configuration mode.

Examples

```
hostname(ca-trustpool)# crl cache-time 30
```

Related Commands

Command	Description
crl enforcenextupdate	Specifies how to handle the NextUpdate CRL field.

crl configure

To enter CRL configuration mode, use the **crl configure** command in crypto ca trustpoint configuration mode.

crl configure

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Crypto ca trustpoint configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters crl configuration mode for a trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)#
```

crl enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **crl enforcenextupdate** command in ca-trustpool configuration mode. If enabled, CRLs are required to have a NextUpdate field that has not yet lapsed. To not enforce this restriction, use the **no** form of this command:

crl enforcenextupdate

no crl enforcenextupdate

Syntax Description

This command has no arguments or keywords.

Defaults

The default is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca-trustpool configuration	•	•	•	—	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

If enabled, CRLs are required to have a NextUpdate field that has not yet elapsed. This command is consistent with the version of this command supported in the trustpoint configuration mode.

Related Commands

Command	Description
crl cache-time	Configures how long a CRL can remain in the CRL cache before ASA refreshes it.