CHAPTER 62

# software-version through storage-objects Commands

# software-version

To identify the Server and User-Agent header fields, which expose the software version of either a server or an endpoint, use the **software-version** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

**software-version action** {**mask** | **log**} [**log**}

**no software-version action** {**mask** | **log**} [**log**}

## Syntax Description

| | |
|---|---|
| **log** | Specifies standalone or additional log in case of violation. |
| **mask** | Masks the software version in the SIP message. |

## 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 |
| Parameters configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Examples

The following example shows how to identify the software version in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# software-version action log
```

## Related Commands

| Command | Description |
|---|---|
| **class** | Identifies a class map name in the policy map. |
| **class-map type inspect** | Creates an inspection class map to match traffic specific to an application. |
| **policy-map** | Creates a Layer 3/4 policy map. |
| **show running-config policy-map** | Display all current policy map configurations. |

# speed

To set the speed of a copper (RJ-45) Ethernet interface, use the **speed** command in interface configuration mode. To restore the speed setting to the default, use the **no** form of this command.

**speed** {**auto** | **10** | **100** | **1000** | **nonegotiate**}

**no speed** [**auto** | **10** | **100** | **1000** | **nonegotiate**]

## Syntax Description

| | |
|---|---|
| **10** | Sets the speed to 10BASE-T. |
| **100** | Sets the speed to 100BASE-T. |
| **1000** | Sets the speed to 1000BASE-T. For copper Gigabit Ethernet only. |
| **auto** | Auto detects the speed. |
| **nonegotiate** | For fiber interfaces, sets the speed to 1000 Mbps and does not negotiate link parameters. This command and the **no** form of this command are the only settings available for fiber interfaces. When you set the value to **no speed nonegotiate** (the default), the interface enables link negotiation, which exchanges flow-control parameters and remote fault information. |

## Defaults

For copper interfaces, the default is **speed auto**.

For fiber interfaces, the default is **no speed nonegotiate**.

## 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 |
| Interface configuration | • | • | • | — | • |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was moved from a keyword of the **interface** command to an interface configuration mode command. |

## Usage Guidelines

Set the speed on the physical interface only.

If your network does not support auto detection, set the speed to a specific value.

For RJ-45 interfaces on the ASA 5500 series, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the speed to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

**Note** Do not set the **speed** command for an ASA 5500x series or an ASA 5585 with fiber interfaces. Doing so causes a link failure.

## Examples

The following example sets the speed to 1000BASE-T:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure interface** | Clears all configuration for an interface. |
| **duplex** | Sets the duplex mode. |
| **interface** | Configures an interface and enters interface configuration mode. |
| **show interface** | Displays the runtime status and statistics of interfaces. |
| **show running-config interface** | Shows the interface configuration. |

# split-dns

To enter a list of domains to be resolved through the split tunnel, use the **split-dns** command in group-policy configuration mode. To delete a list, use the **no** form of this command.

To delete all split tunneling domain lists, use the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns none** command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, use the **split-dns none** command.

**split-dns** {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

**no split-dns** [*domain-name domain-name2 domain-nameN*]

## Syntax Description

| | |
|---|---|
| **value** *domain-name* | Provides a domain name that the ASA resolves through the split tunnel. |
| **none** | Indicates that there is no split DNS list. Sets a split DNS list with a null value, thereby disallowing a split DNS list. Prevents inheriting a split DNS list from a default or specified group policy. |

## Defaults

Split DNS is disabled.

## 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

Use a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 255 characters. You can use only alphanumeric characters, hyphens (-), and periods (.).

The **no split-dns** command, when used without arguments, deletes all current values, including a null value created by issuing the **split-dns none** command.

Starting with version 3.0.4235, AnyConnect Secure Mobility Client supports true split DNS functionality for Windows platforms.

## Examples

The following example shows how to configure the domains Domain1, Domain2, Domain3 and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

## Related Commands

| Command | Description |
|---|---|
| **default-domain** | Specifies a default domain name that the IPsec client uses the for DNS queries which omit the domain field. |
| split-dns | Provides a list of domains to be resolved through the split tunnel. |
| split-tunnel-network-list | Identifies the access list the ASA uses to distinguish which networks require tunneling. |
| **split-tunnel-policy** | Lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in cleartext form |

# split-horizon

To reenable EIGRP split horizon, use the **split-horizon** command in interface configuration mode. To disable EIGRP split horizon, use the **no** form of this command.

**split-horizon eigrp** *as-number*

**no split-horizon eigrp** *as-number*

## Syntax Description

| | |
|---|---|
| *as-number* | The autonomous system number of the EIGRP routing process. |

## Defaults

The **split-horizon** command 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 |
| Interface configuration | • | — | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |
| 9.0(1) | Multiple context mode is supported. |

## Usage Guidelines

For networks that include links over X.25 packet-switched networks, you can use the **neighbor** command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

In general, it is best that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. If split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

## Examples

The following example disables EIGRP split horizon on interface Ethernet0/0:

```
hostname(config)# interface Ethernet0/0
hostname(config-if)# no split-horizon eigrp 100
```

**Related Commands**

| Command | Description |
|---|---|
| **router eigrp** | Creates an EIGRP routing process and enters configuration mode for that process. |

# split-tunnel-all-dns

To enable the AnyConnect Secure Mobility Client to the resolve all DNS addresses through the VPN tunnel, use the **split-tunnel-all-dns** command from group policy configuration mode.

To remove the command from the running configuration, use the **no** form of this command. This enables inheritance of the value from another group policy.

**split-tunnel-all-dns** {**disable | enable**}

**no split-tunnel-all-dns** [{**disable | enable**}]

## Syntax Description

| | |
|---|---|
| **disable** (default) | The AnyConnect client sends DNS queries over the tunnel according to the split tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list. |
| **enable** | The AnyConnect client resolves all DNS addresses through the VPN tunnel. |

## Defaults

The default is disabled.

## 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 |
|---|---|
| 8.2(5) | This command was introduced. |

## Usage Guidelines

The **split-tunnel-all-dns enable** command applies to VPN connections using the SSL or IPsec/IKEv2 protocol, and instructs the AnyConnect client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the AnyConnect client does not try to resolve the address through public DNS servers.

By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list.

## Examples

The following example configures the ASA to enable the AnyConnect client to resolve all DNS queries through the VPN tunnel:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-all-dns enable
```

**Related Commands**

| Command | Description |
|---|---|
| **default-domain** | Specifies a default domain name that the legacy IPsec (IKEv1) VPN client or the AnyConnect VPN Client (SSL) uses for DNS queries that omit the domain field. |
| **split-dns** | Provides a list of domains to be resolved through the split tunnel. |
| **split-tunnel-network-list** | Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not. |
| **split-tunnel-policy** | Lets a legacy VPN client (IPsec/IKEv1) or the AnyConnect VPN client (SSL) conditionally direct packets over a tunnel in encrypted form, or to a network interface in clear text form |

# split-tunnel-network-list

To create a network list for split tunneling, use the **split-tunnel-network-list** command in group-policy configuration mode. To delete a network list, use the **no** form of this command.

To delete all split tunneling network lists, use the **no split-tunnel-network-list** command without arguments. This deletes all configured network lists, including a null list created by issuing the **split-tunnel-network-list none** command.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, use the **split-tunnel-network-list none** command.

Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling.

**split-tunnel-network-list {value** *access-list name* **| none}**

**no split-tunnel-network-list value** [*access-list name*]

## Syntax Description

| | |
|---|---|
| **none** | Indicates that there is no network list for split tunneling; the ASA tunnels all traffic.<br><br>Sets a split tunneling network list with a null value, thereby disallowing split tunneling. Prevents inheriting a default split tunneling network list from a default or specified group policy. |
| **value** *access-list name* | Identifies an access list that enumerates the networks to tunnel or not tunnel. |

## Defaults

By default, there are no split tunneling network lists.

## 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

The ASA makes split tunneling decisions on the basis of a network list, which is a standard ACL that consists of a list of addresses on the private network.

The **no split-tunnel-network-list** command, when used without arguments, deletes all current network lists, including a null value created by issuing the **split-tunnel-network-list none** command.

**Note** The ASA provides supports for 200 split networks.

## Examples

The following example shows how to set a network list called FirstList for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Creates an access list, or uses a downloadable access list. |
| **default-domain** | Specifies a default domain name that he IPsec client uses the for DNS queries that omit the domain field. |
| **split-dns** | Provides a list of domains to be resolved through the split tunnel. |
| **split-tunnel-policy** | Lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in cleartext form. |

# split-tunnel-policy

To set a split tunneling policy, use the **split-tunnel-policy** command in group-policy configuration mode. To remove the split-tunnel-policy attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for split tunneling from another group policy.

Split tunneling lets a remote-access VPN client conditionally direct packets over an IPsec or SSL tunnel in encrypted form, or to a network interface in cleartext form. With split-tunneling enabled, packets not bound for destinations on the other side of the IPsec or SSL VPN tunnel endpoint do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies this split tunneling policy to a specific network.

**split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}**

**no split-tunnel-policy**

## Syntax Description

| | |
|---|---|
| **excludespecified** | Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. |
| **split-tunnel-policy** | Indicates that you are setting rules for tunneling traffic. |
| **tunnelall** | Specifies that no traffic goes in the clear or to any other destination than the ASA. Remote users reach internet networks through the corporate network and do not have access to local networks. |
| **tunnelspecified** | Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's internet service provider. |

## Defaults

Split tunneling is disabled by default, which is tunnelall.

## 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

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable split tunneling.

## Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

## Related Commands

| Command | Description |
|---|---|
| **default-domain** | Specifies a default domain name that he IPsec client uses the for DNS queries that omit the domain field. |
| **split-dns** | Provides a list of domains to be resolved through the split tunnel. |
| **split-tunnel-network-list none** | Indicates that no access list exists for split tunneling. All traffic travels across the tunnel. |
| **split-tunnel-network-list value** | Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not. |

# spoof-server

To substitute a string for the server header field for HTTP protocol inspection, use the **spoof-server** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

**spoof-server** *string*

**no spoof-server** *string*

## Syntax Description

| | |
|---|---|
| *string* | String to substitute for the server header field. 82 characters maximum. |

## 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 |
| Parameters configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Usage Guidelines

WebVPN streams are not subject to the **spoof-server** comand.

## Examples

The following example shows how to substitute a string for the server header field in an HTTP inspection policy map:

```
hostname(config-pmap-p)# spoof-server string
```

## Related Commands

| Command | Description |
|---|---|
| **class** | Identifies a class map name in the policy map. |
| **class-map type inspect** | Creates an inspection class map to match traffic specific to an application. |
| **policy-map** | Creates a Layer 3/4 policy map. |
| **show running-config policy-map** | Display all current policy map configurations. |

# sq-period

To specify the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture, use the **sq-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC policy, use the **no** form of this command.

**sq-period** *seconds*

**no sq-period** [*seconds*]

## Syntax Description

| | |
|---|---|
| *seconds* | Number of seconds between each successful posture validation. The range is 30 to 1800. |

## Defaults

The default value is 300.

## 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 |
| Nac-policy-nac-framework configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.3(0) | "nac-" removed from command name. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode. |
| 7.2(1) | This command was introduced. |

## Usage Guidelines

The ASA starts the status query timer after each successful posture validation and status query response. The expiration of this timer triggers a query for changes in the host posture, referred to as a *status query.*

## Examples

The following example changes the value of the status query timer to 1800 seconds:

```
hostname(config-nac-policy-nac-framework)# sq-period 1800
hostname(config-nac-policy-nac-framework)
```

The following example removes the status query timer from the NAC Framework policy:

```
hostname(config-nac-policy-nac-framework)# no sq-period
hostname(config-nac-policy-nac-framework)
```

## Related Commands

| Command | Description |
|---|---|
| **nac-policy** | Creates and accesses a Cisco NAC policy, and specifies its type. |
| **nac-settings** | Assigns a NAC policy to a group policy. |
| **eou timeout** | Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration. |
| **reval-period** | Specifies the interval between each successful posture validation in a NAC Framework session. |
| **debug eap** | Enables logging of Extensible Authentication Protocol events to debug NAC Framework messaging. |

# ssh

To add SSH access to the ASA, use the **ssh** command in global configuration mode. To disable SSH access to the ASA, use the **no** form of this command.

**ssh** {*ip_address mask* | *ipv6_address/prefix*} *interface*

**no ssh** {*ip_address mask* | *ipv6_address/prefix*} *interface*

## Syntax Description

| | |
|---|---|
| *interface* | The ASA interface on which SSH is enabled. If not specified, SSH is enabled on all interfaces except the outside interface. |
| *ip_address* | IPv4 address of the host or network authorized to initiate an SSH connection to the ASA. For hosts, you can also enter a host name. |
| *ipv6_address/prefix* | The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the ASA. |
| *mask* | Network mask for *ip_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 |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

This command supports IPv4 and IPv6 addresses. The **ssh** *ip_address* command specifies hosts or networks that are authorized to initiate an SSH connection to the ASA. You can have multiple ssh commands in the configuration. The **no** form of the command removes a specific SSH command from the configuration. Use the **clear configure ssh** command to remove all SSH commands.

Before you can begin using SSH to the ASA, you must generate a default RSA key using the **crypto key generate rsa** command.

The following security algorithms and ciphers are supported on the ASA:

- 3DES and AES ciphers for data encryption
- HMAC-SHA and HMAC-MD5 algorithms for packet integrity
- RSA public key algorithm for host authentication

The following SSH Version 2 features are not supported on the ASA:

- X11 forwarding
- Port forwarding
- SFTP support
- Kerberos and AFS ticket passing
- Data compression

## Examples

The following example shows how to configure the inside interface to accept SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh scopy enable
hostname(config)# ssh timeout 60
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure ssh** | Clears all SSH commands from the running configuration. |
| **crypto key generate rsa** | Generates RSA key pairs for identity certificates. |
| **debug ssh** | Displays debugging information and error messages for SSH commands. |
| **show running-config ssh** | Displays the current SSH commands in the running configuration. |
| **ssh scopy enable** | Enables a secure copy server on the ASA. |
| **ssh version** | Restricts the ASA to using either SSH Version 1 or SSH Version 2. |

# ssh authentication

To enable public key authentication on a per-user basis, use the **ssh authentication** command in username attributes mode. To disable public key authentication on a per-user basis, use the **no** form of this command.

**ssh authentication** {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

**no ssh authentication** {**pkf** | **publickey** [**nointeractive**] *key* [**hashed**]}

## Syntax Description

| | |
|---|---|
| **hashed** | Hashed with SHA-256 and 32 bytes long, with each byte separated by a colon (for parsing purposes). |
| *key* | The value of the *key* argument can be one of the following:<br>• When the *key* argument is supplied and the hashed tag is not specified, the value of the key must be a Base 64 encoded public key that is generated by SSH key generation software that can generate SSH-RSA raw keys (that is, with no certificates). After you submit the Base 64 encoded public key, that key is then hashed via SHA-256 and the corresponding 32-byte hash is used for all further comparisons.<br>• When the *key* argument is supplied and the hashed tag is specified, the value of the key must have been previously hashed with SHA-256 and be 32 bytes long, with each byte separated by a colon (for parsing purposes). |
| **nointeractive** | The **nointeractive** option suppresses all prompts when importing an SSH public key file formatted key. This noninteractive data entry mode is only intended for ASDM use. |
| **pkf** | For a **pkf** key, you are prompted to paste in a PKF formatted key, up to 4096 bits. Use this format for keys that are too large to paste inline in Base64 format. For example, you can generate a 4096-bit key using ssh keygen, then convert it to PKF, and use the **pkf** keyword to be prompted for the key.<br>**Note** You can use the **pkf** option with failover, but the PKF key is not automatically replicated to the standby system. You must enter the **write standby** command to synchronize the PKF key. |
| **publickey** | For a **publickey**, the *key* is a Base64-encoded public key. You can generate the key using any SSH key generation software (such as ssh keygen) that can generate SSH-RSA raw keys (with no certificates). |

## Defaults

No default behaviors or values.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple Context | System |
| Username attributes | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 9.1(2) | This command was introduced. |

## Usage Guidelines

You can specify a public key file (PKF) formatted key (the **pkf** keyword) or a Base64 key (the **publickey** keyword).

The *key* field and the **hashed** keyword are only available with the **publickey** option, and the **nointeractive** keyword is only available with the **pkf** option.

When you save the configuration, the hashed key value is saved to the configuration and used when the ASA is rebooted.

When you view the key on the ASA using the **show running-config username** command, the key is encrypted using a SHA-256 hash. Even if you entered the key as **pkf**, the ASA hashes the key, and shows it as a hashed **publickey**. If you need to copy the key from **show** output, specify the **publickey** type with the **hashed** keyword.

## Examples

The following example shows how to authenticate using a PKF formatted key:

```
hostname(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
hostname(config-username)
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure ssh** | Clears all SSH commands from the running configuration. |
| **debug ssh** | Displays debugging information and error messages for SSH commands. |

| Command | Description |
|---|---|
| **show running-config ssh** | Displays the current SSH commands in the running configuration. |
| **ssh version** | Restricts the ASA to using either SSH Version 1 or SSH Version 2. |

# ssh disconnect

To disconnect an active SSH session, use the **ssh disconnect** command in privileged EXEC mode.

**ssh disconnect** *session_id*

## Syntax Description

| | |
|---|---|
| *session_id* | Disconnects the SSH session specified by the ID number. |

## 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

You must specify a session ID. Use the **show ssh sessions** command to obtain the ID of the SSH session you want to disconnect.

## Examples

The following example shows an SSH session being disconnected:

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

**Related Commands**

| Command | Description |
|---|---|
| **show ssh sessions** | Displays information about active SSH sessions to the ASA. |
| **ssh timeout** | Sets the timeout value for idle SSH sessions. |

# ssh key-exchange

To exchange keys using either the Diffie-Hellman (DH) Group 1 or DH Group 14 key-exchange method, use the **ssh key-exchange** command in global configuration mode. To disable key exchange using either the DH Group 1 or DH Group 14 key-exchange method, use the **no** form of this command.

**ssh key-exchange group** {**dh-group1** | **dh-group14**} **sha1**

**no ssh key-exchange group** {**dh-group1** | **dh-group14**} **sha1**

## Syntax Description

| | |
|---|---|
| **dh-group1** | Indicates that the DH group 1 key-exchange method will follow and should be used when exchanging keys. DH group 2 is called DH group 1 for legacy reasons. |
| **dh-group14** | Indicates that the DH group 14 key-exchange method will follow and should be used when exchanging keys. |
| **group** | Indicates that either the DH group 1 key-exchange method or the DH group 14 key-exchange method will follow and should be used when exchanging keys. |
| **key-exchange** | Specifies that either the DH group 1 or DH group 14 key-exchange method will follow and should be used when exchanging keys. |
| **sha-1** | Specifies that the SHA-1 encryption algorithm should be used. |

## 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 |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 8.4(4) | This command was introduced. |
| 9.1(2) | This command was changed to **ssh key-exchange group dh-group1-sha1**. |

## Usage Guidelines

Before you can begin using SSH to the ASA, you must generate a default RSA key using the **crypto key generate rsa** command.

Both the DH Group 1 and Group 14 key-exchange methods for key exchange are supported on the ASA. If no DH group key-exchange method is specified, the DH group 1 key-exchange method is used. For more information about using DH key-exchange methods, see RFC 4253.

**Note** This command is not available in the 9.1(1) or 9.1.1(2) release.

## Examples

The following example shows how to exchange keys using the DH Group 14 key-exchange method:

```
hostname(config)# ssh key-exchange dh-group-1-sha1
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure ssh** | Clears all SSH commands from the running configuration. |
| **crypto key generate rsa** | Generates RSA key pairs for identity certificates. |
| **debug ssh** | Displays debugging information and error messages for SSH commands. |
| **show running-config ssh** | Displays the current SSH commands in the running configuration. |
| **ssh scopy enable** | Enables a secure copy server on the ASA. |
| **ssh version** | Restricts the ASA to using either SSH Version 1 or SSH Version 2. |

# ssh scopy enable

To enable Secure Copy (SCP) on the ASA, use the **ssh scopy enable** command in global configuration mode. To disable SCP, use the **no** form of this command.

**ssh scopy enable**

**no ssh scopy enable**

## 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

SCP is a server-only implementation; it will be able to accept and terminate connections for SCP but can not initiate them. The ASA has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the ASA internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The ASA license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Before initiating the file transfer, the ASA check available Flash memory. If there is not enough available space, the ASA terminates the SCP connection. If you are overwriting a file in Flash memory, you still need to have enough free space for the file being copied to the ASA. The SCP process copies the file to a temporary file first, then copies the temporary file over the file being replaced. If you do not have enough space in Flash to hold the file being copied and the file being overwritten, the ASA terminates the SCP connection.

## Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh scopy enable
hostname(config)# ssh timeout 60
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure ssh** | Clears all SSH commands from the running configuration. |
| **debug ssh** | Displays debug information and error messages for SSH commands. |
| **show running-config ssh** | Displays the current SSH commands in the running configuration. |
| **ssh** | Allows SSH connectivity to the ASA from the specified client or network. |
| **ssh version** | Restricts the ASA to using either SSH Version 1 or SSH Version 2. |

# ssh timeout

To change the default SSH session idle timeout value, use the **ssh timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

**ssh timeout** *number*

**no ssh timeout**

## Syntax Description

| | |
|---|---|
| *number* | Specifies the duration in minutes that an SSH session can remain inactive before being disconnected. Valid values are from 1 to 60 minutes. |

## Defaults

The default session timeout value is 5 minutes.

## 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 |
|---|---|
| Preexisting | This command was preexisting. |

## Usage Guidelines

The **ssh timeout** command specifies the duration in minutes that a session can be idle before being disconnected. The default duration is 5 minutes.

## Examples

The following example shows how to configure the inside interface to accept only SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure ssh** | Clears all SSH commands from the running configuration. |
| **show running-config ssh** | Displays the current SSH commands in the running configuration. |

| Command | Description |
|---|---|
| **show ssh sessions** | Displays information about active SSH sessions to the ASA. |
| **ssh disconnect** | Disconnects an active SSH session. |

# ssh version

To restrict the version of SSH accepted by the ASA, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command. The default values permits SSH Version 1 and SSH Version 2 connections to the ASA.

**ssh version** {**1** | **2**}

**no ssh version** [**1** | **2**]

## Syntax Description

| | |
|---|---|
| **1** | Specifies that only SSH Version 1 connections are supported. |
| **2** | Specifies that only SSH Version 2 connections are supported. |

## Defaults

By default, both SSH Version 1 and SSH Version 2 are supported.

## 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

1 and 2 specify which version of SSH the ASA is restricted to using. The **no** form of the command returns the ASA to the default stance, which is compatible mode (both version can be used).

## Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure ssh** | Clears all SSH commands from the running configuration. |
| **debug ssh** | Displays debug information and error messages for SSH commands. |

| Command | Description |
|---|---|
| **show running-config ssh** | Displays the current SSH commands in the running configuration. |
| **ssh** | Allows SSH connectivity to the ASA from the specified client or network. |

# ssl certificate-authentication

To enable client certificate authentication for backwards compatibility for versions previous to 8.2(1), use the **ssl certificate-authentication** command in global configuration mode. To disable ssl certificate authentication, use the **no** version of this command.

**ssl certificate-authentication interface** *interface-name* **port** *port-number*

**no ssl certificate-authentication interface** *interface-name* **port** *port-numbe***r**

## Syntax Description

| | |
|---|---|
| *interface-name* | The name of the selected interface, such as inside, management, and outside. |
| *port-number* | The TCP port number, an integer in the range 1-65535. |

## Defaults

This feature 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 |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 8.0(3) | This command was introduced. |
| 8.2(1) | This command is no longer needed, but the ASA retains it for downgrading to previous versions. |

## Usage Guidelines

This command replaces the deprecated http authentication-certificate command.

## Examples

The following example shows how to configure the ASA to use the SSL certificate authentication feature:

```
hostname(config)# ssl certificate-authentication interface inside port 330
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config ssl** | Displays the current set of configured SSL commands. |

# ssl client-version

To specify the SSL/TLS protocol version the ASA uses when acting as a client, use the **ssl client-version** command in global configuration mode. To revert to the default, **any**, use the **no** version of this command. This command lets you restrict the versions of SSL/TLS that the ASA sends.

**ssl client-version** [*any* | *sslv3-only* | *tlsv1-only*]

**no ssl client-version**

## Syntax Description

| | |
|---|---|
| any | The ASA sends SSL version3 hellos, and negotiates either SSL version 3 or TLS version 1. |
| sslv3-only | The security appliance sends SSL version 3 hellos, and accepts only SSL version 3. |
| tlsv1-only | The security appliance sends TLSv1 client hellos, and accepts only TLS version 1. |

## Defaults

The default value is **any**.

## 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

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

| | |
|---|---|
| Negotiate SSLv3 | Java downloads |
| Negotiate SSLv3/TLSv1 | Java downloads |
| Negotiate TLSv1 | Java does NOT download |
| TLSv1Only | Java does NOT download |
| SSLv3Only | Java does NOT download |

The issue is that JAVA only negotiates SSLv3 in the client Hello packet when you launch the Port Forwarding application.

## Examples

The following example shows how to configure the ASA to communicate using only TLSv1 when acting as an SSL client:

```
hostname(config)# ssl client-version tlsv1-only
```

## Related Commands

| Command | Description |
|---|---|
| **clear config ssl** | Removes all SSL commands from the configuration, reverting to the default values. |
| **ssl encryption** | Specifies the encryption algorithms that the SSL/TLS protocol uses. |
| **show running-config ssl** | Displays the current set of configured SSL commands. |
| **ssl server-version** | Specifies the SSL/TLS protocol version the ASA uses when acting as a server. |
| **ssl trust-point** | Specifies the certificate trust point that represents the SSL certificate for an interface. |

# ssl encryption

To specify the encryption algorithms for the SSL DTLS and TLS protocols, use the **ssl encryption** command in global configuration mode**.** Issuing the command again overwrites the previous setting. To restore the default, which is the complete set of encryption algorithms, use the **no** version of the command.

**ssl encryption** [**3des-sha1**] [**aes128-sha1**] [**aes256-sha1**] [**des-sha1**] [**null-sha1**] [**rc4-md5**] [**rc4-sha1**] **[dhe-aes256-sha1] [dhe-aes128-sha1]**

**no ssl encryption**

## Syntax Description

| | |
|---|---|
| **3des-sha1** | Specifies triple DES 168-bit encryption with Secure Hash Algorithm 1 (FIPS-compliant). |
| **aes128-sha1** | Specifies triple AES 128-bit encryption with Secure Hash Algorithm 1 (FIPS-compliant). |
| **aes256-sha1** | Specifies triple AES 256-bit encryption with Secure Hash Algorithm 1 (FIPS-compliant). |
| **dhe-aes128-sha1** | Specifies AES 128-bit encryption ciphersuites for Transport Layer Security (TLS). |
| **dhe-aes256-sha1** | Specifies AES 256-bit encryption ciphersuites for Transport Layer Security (TLS). |
| **des-sha1** | Specifies DES 56-bit encryption with Secure Hash Algorithm 1. |
| **null-sha1** | Specifies null encryption with Secure Hash Algorithm 1. This setting enforces message integrity without confidentiality.<br>⚠ **Caution** If you specify **null-sha1**, data is not encrypted. |
| **rc4-md5** | Specifies RC4 128-bit encryption with an MD5 hash function. |
| **rc4-sha1** | Specifies RC4 128-bit encryption with Secure Hash Algorithm 1. |

## Defaults

By default, the SSL encryption list on the ASA contains these algorithms in the following order:

1. RC4-SHA1
2. AES128-SHA1 (FIPS-compliant)
3. AES256-SHA1 (FIPS-compliant)
4. 3DES-SHA1 (FIPS-compliant)
5. DHE-AES256-SHA1
6. DHE-AES128-SHA1

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |
| 9.1(2) | Support for ssl encryption dhe-aes128-sha1 and dhe-aes256-sha1 was added. |

## Usage Guidelines

The ASDM License tab reflects the maximum encryption the license supports, not the value you configure.

The ordering of the algorithms determines preference for their use. You can add or remove algorithms to meet the needs of your environment.

For FIPS-compliant AnyConnect client SSL connections, you must ensure a FIPS-compliant cipher is the first one specified in the list of SSL encryptions.

Several applications do not support DHE, so include at least one other SSL encryption method to ensure a cipher suite common to both.

Cryptographic operations use symmetric-key algorithms as referenced in http://en.wikipedia.org/wiki/Symmetric-key_algorithm.

## Examples

The following example shows how to configure the ASA to use the 3des-sha1 and des-sha1 encryption algorithms:

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

## Related Commands

| Command | Description |
|---|---|
| **clear config ssl** | Removes all SSL commands from the configuration, reverting to the default values. |
| **show running-config ssl** | Displays the current set of configured SSL commands. |
| **ssl client-version** | Specifies the SSL/TLS protocol version the ASA uses when acting as a client. |
| **ssl server-version** | Specifies the SSL/TLS protocol version the ASA uses when acting as a server. |
| **ssl trust-point** | Specifies the certificate trust point that represents the SSL certificate for an interface. |

# ssl server-version

To specify the SSL/TLS protocol version the ASA uses when acting as a server, use the **ssl server-version** command in global configuration mode. To revert to the default, any, use the **no** version of this command. This command lets you restrict the versions of SSL/TSL that the ASA accepts.

**ssl server-version** [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

**no ssl server-version**

## Syntax Description

| | |
|---|---|
| *any* | The ASA accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1. |
| *sslv3* | The ASA accepts SSL version 2 client hellos, and negotiates to SSL version 3. |
| *sslv3-only* | The security appliance accepts only SSL version 3 client hellos, and uses only SSL version 3. |
| *tlsv1* | The ASA accepts SSL version 2 client hellos, and negotiates to TLS version 1. |
| *tlsv1-only* | The security appliance accepts only TLSv1 client hellos, and uses only TLS version 1. |

## Defaults

The default value is **any**.

## 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

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

| | |
|---|---|
| Negotiate SSLv3 | Java downloads |
| Negotiate SSLv3/TLSv1 | Java downloads |
| Negotiate TLSv1 | Java does NOT download |
| TLSv1Only | Java does NOT download |
| SSLv3Only | Java does NOT download |

If you configure e-mail proxy, do not set thhe SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.

Remote endpoints with FIPS enabled cannot communicate when ssl-version is configured for sslv3 or sslv3-only. For that environment, set ssl server-version to tlsv1 or to any.

## Examples

The following example shows how to configure the ASA to communicate using only TLSv1 when acting as an SSL server:

```
hostname(config)# ssl server-version tlsv1-only
```

## Related Commands

| Command | Description |
|---|---|
| **clear config ssl** | Removes all ssl commands from the configuration, reverting to the default values. |
| **show running-config ssl** | Displays the current set of configured ssl commands. |
| **ssl client-version** | Specifies the SSL/TLS protocol version the ASA uses when acting as a client. |
| **ssl encryption** | Specifies the encryption algorithms that the SSL/TLS protocol uses. |
| **ssl trust-point** | Specifies the certificate trust point that represents the SSL certificate for an interface. |

# ssl trust-point

To specify the certificate trustpoint that represents the SSL certificate for an interface, use the **ssl trust-point** command with the *interface* argument in global configuration mode. If you do not specify an interface, this command creates the fallback trustpoint for all interfaces that do not have a trustpoint configured. To remove an SSL trustpoint from the configuration that does not specify an interface, use the **no** version of this command. To remove an entry that does specify an interface, use the **no ssl trust-point {***trustpoint [interface]***}** version of the command.

**ssl trust-point {***trustpoint [interface]***}**

**no ssl trust-point**

## Syntax Description

| | |
|---|---|
| *interface* | The name for the interface to which the trustpoint applies. The **nameif** command specifies the name of the interface. |
| *trustpoint* | The *name* of the CA trustpoint as configured in the **crypto ca trustpoint** {*name*} command. |

## Defaults

The default is no trustpoint association. The ASA uses the default self-generated RSA key-pair certificate.

## 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

Observe these guidelines when using this command:

- The value for *trustpoint* must be the name of the CA trustpoint as configured in the **crypto ca trustpoint {*name*}** command.
- The value for *interface* must be the *nameif* name of a previously configured interface.
- Removing a trustpoint also removes any **ssl trust-point** entries that reference that trustpoint.
- You can have one **ssl trustpoint** entry for each interface and one that specifies no interfaces.
- You can reuse the same trustpoint for multiple entries.

The following example explains how to use the **no** versions of this command:

The configuration includes these SSL trustpoints:

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

Issue the command:

no ssl trust-point

Then show run ssl will have:

ssl trust-point tp2 outside

## Examples

The following example shows how to configure an ssl trustpoint called FirstTrust for the inside interface, and a trustpoint called DefaultTrust with no associated interface.

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

The next example shows how to use the **no** version of the command to delete a trustpoint that has no associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

The next example shows how to delete a trustpoint that does have an associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

## Related Commands

| Command | Description |
|---|---|
| **clear config ssl** | Removes all SSL commands from the configuration, reverting to the default values. |
| **show running-config ssl** | Displays the current set of configured SSL commands. |
| **ssl client-version** | Specifies the SSL/TLS protocol version the ASA uses when acting as a client. |
| **ssl encryption** | Specifies the encryption algorithms that the SSL/TLS protocol uses. |
| **ssl server-version** | Specifies the SSL/TLS protocol version the ASA uses when acting as a server. |

# sso-server

To create a Single Sign-On (SSO) server for ASA user authentication, use the **sso-server** command in webvpn configuration mode. With this command, you must specify the SSO server type.

To remove an SSO server, use the **no** form of this command.

**sso-server** *name* **type** [*siteminder* | *saml-v1.1-post* ]

**no sso-server** *name*

**Note** This command is required for SSO authentication.

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the SSO server. Minimum of 4 characters and maximum of 31 characters. |
| *saml-v1.1-post* | Specifies that the ASA SSO server being configured is a SAML, Version 1.1, SSO server of the POST type. |
| *siteminder* | Specifies that the ASA SSO server being configured is a Computer Associates SiteMinder SSO server. |
| **type** | Specifies the type of SSO server. SiteMinder and SAML-V1.1-POST are the only types available. |

## Defaults

There is no default value or behavior.

## 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** |
| Webvpn configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.1(1) | This command was introduced. |

## Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **sso-server** command lets you create an SSO server.

In the authentication, the ASA acts as a proxy for the WebVPN user to the SSO server. The ASA currently supports the SiteMinder SSO server (formerly Netegrity SiteMinder) and the SAML POST-type SSO server. Currently, the available arguments for the type option are restricted to *siteminder* or *saml-V1.1-post*.

## Examples

The following example, entered in webvpn configuration mode, creates a SiteMinder-type SSO server named “example1”:

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example1 type siteminder
hostname(config-webvpn-sso-siteminder)#
```

The following example, entered in webvpn configuration mode, creates a SAML, Version 1.1, POST-type SSO server named “example2”:

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example2 type saml-v1.1-post
hostname(config-webvpn-sso-saml)#
```

## Related Commands

| Command | Description |
|---|---|
| **assertion-consumer-url** | Identifies the URL for the SAML-type SSO assertion consumer service. |
| **issuer** | Specifies the SAML-type SSO server’s security device name. |
| **max-retry-attempts** | Configures the number of times the ASA retries a failed SSO authentication attempt. |
| **policy-server-secret** | Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server. |
| **request-timeout** | Specifies the number of seconds before a failed SSO authentication attempt times out. |
| **show webvpn sso-server** | Displays the operating statistics for an SSO server. |
| **test sso-server** | Tests an SSO server with a trial authentication request. |
| **trustpoint** | Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion |
| **web-agent-url** | Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests. |

# sso-server value (group-policy webvpn)

To assign an SSO server to a group policy, use the **sso-server value** command in webvpn configuration mode available in group-policy configuration mode.

To remove the assignment and use the default policy, use the **no** form of this command.

To prevent inheriting the default policy, use the **sso-server none** command.

**sso-server** {**value** *name* | **none**}

[**no**] **sso-server value** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the SSO server being assigned to the group policy. |

## Defaults

The default policy assigned to the group is 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 webvpn configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.1(1) | This command was introduced. |

## Usage Guidelines

The **sso-server value** command, when entered in group-policy webvpn mode, lets you assign an SSO server to a group policy.

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

**Note** Enter the same command, **sso-server value**, in username-webvpn configuration mode to assign SSO servers to user policies.

## Examples

The following example commands create the group policy my-sso-grp-pol and assigns it to the SSO server named example:

```
hostname(config)# group-policy my-sso-grp-pol internal
```

```
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

## Related Commands

| Command | Description |
|---|---|
| **policy-server-secret** | Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server. |
| **show webvpn sso-server** | Displays the operating statistics for all SSO servers configured on the security device. |
| **sso-server** | Creates a single sign-on server. |
| **sso-server value** (**username webvpn**) | Assigns an SSO server to a user policy. |
| **web-agent-url** | Specifies the SSO server URL to which the ASA makes SiteMinder-type SSO authentication requests. |

# sso-server value (username webvpn)

To assign an SSO server to a user policy, use the **sso-server value** command in webvpn configuration mode available in username configuration mode.

To remove an SSO server assignment for a user, use the **no** form of this command.

When a user policy inherits an unwanted SSO server assignment from a group policy, use the **sso-server none** command to remove the assignment.

**sso-server** {**value** *name* | **none**}

[**no**] **sso-server value** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the SSO server being assigned to the user policy. |

## Defaults

The default is for the user policy to use the SSO server assignment in the group policy.

## 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 |
| Username webvpn configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.1(1) | This command was introduced. |

## Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

The **sso-server value** command lets you assign an SSO server to a user policy.

**Note** Enter the same command, **sso-server value**, in group-webvpn configuration mode to assign SSO servers to group policies.

## Examples

The following example commands assign the SSO server named my-sso-server to the user policy for a WebVPN user named Anyuser:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value my-sso-server
```

```
hostname(config-username-webvpn)#
```

## Related Commands

| Command | Description |
|---|---|
| **policy-server-secret** | Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server. |
| **show webvpn sso-server** | Displays the operating statistics for all SSO servers configured on the security device. |
| **sso-server** | Creates a single sign-on server. |
| **sso-server value (config-group-webvpn)** | Assigns an SSO server to a group policy. |
| **web-agent-url** | Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests. |

# start-url

To enter the URL at which to retrieve an optional pre-login cookie, use the **start-url** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command.

**start-url** *string*

**Note** To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

## Syntax Description

| | |
|---|---|
| *string* | The URL for an SSO server. The maximum URL length is 1024 characters. |

## Defaults

There is no default value or behavior.

## 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 |
| Aaa-server-host configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.1(1) | This command was introduced. |

## Usage Guidelines

The WebVPN server of the ASA can use an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The authenticating web server may execute a pre-login sequence by sending a Set-Cookie header along with the login page content. You can discover this by connecting directly to the authenticating web server's login page with your browser. If the web server sets a cookie when the login page loads and if this cookie is relevant for the following login session, you must use the **start-url** command to enter the URL at which the cookie is retrieved. The actual login sequence starts after the pre-login cookie sequence with the form submission to the authenticating web server.

**Note** The **start-url** command is only required in the presence of the pre-login cookie exchange.

## Examples

The following example, entered in aaa-server host configuration mode, specifies a URL for retrieving the pre-login cookie of https://example.com/east/Area.do?Page-Grp1:

```
hostname(config)# aaa-server testgrp1 (inside) host example.com
hostname(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
hostname(config-aaa-server-host)#
```

## Related Commands

| Command | Description |
|---|---|
| **action-uri** | Specifies a web server URI to receive a username and password for single sign-on authentication. |
| **auth-cookie-name** | Specifies a name for the authentication cookie. |
| **hidden-parameter** | Creates hidden parameters for exchange with the authenticating web server. |
| **password-parameter** | Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication. |
| **user-parameter** | Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication. |

# state-checking

To enforce state checking for H.323, use the **state-checking** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

**state-checking [h225 | ras]**

**no state-checking [h225 | ras]**

## Syntax Description

| | |
|---|---|
| **h225** | Enforces state checking for H.225. |
| **ras** | Enforces state checking for RAS. |

## 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** |
| Parameters configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Examples

The following example shows how to enforce state checking for RAS on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# state-checking ras
```

## Related Commands

| Command | Description |
|---|---|
| **class** | Identifies a class map name in the policy map. |
| **class-map type inspect** | Creates an inspection class map to match traffic specific to an application. |
| **policy-map** | Creates a Layer 3/4 policy map. |
| **show running-config policy-map** | Display all current policy map configurations. |

# strict-header-validation

To enable strict validation of the header fields in the SIP messages according to RFC 3261, use the **strict-header-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

**strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]

**no strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]

## Syntax Description

| | |
|---|---|
| **drop** | Drops the packet if validation occurs. |
| **drop-connection** | Drops the connection of a violation occurs. |
| **reset** | Resets the connection of a violation occurs. |
| **log** | Specifies standalone or additional log in case of violation. It can be associated to any of the actions. |

## 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 |
| Parameters configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was introduced. |

## Examples

The following example shows how to enable strict validation of SIP header fields in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# strict-header-validation action log
```

## Related Commands

| Command | Description |
|---|---|
| **class** | Identifies a class map name in the policy map. |
| **class-map type inspect** | Creates an inspection class map to match traffic specific to an application. |

| Command | Description |
|---|---|
| **policy-map** | Creates a Layer 3/4 policy map. |
| **show running-config policy-map** | Display all current policy map configurations. |

# strict-http

To allow forwarding of non-compliant HTTP traffic, use the **strict-http** command in HTTP map configuration mode, which is accessible using the **http-map** command. To reset this feature to its default behavior, use the **no** form of the command.

**strict-http action** {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

## Syntax Description

| | |
|---|---|
| **action** | The action taken when a message fails this command inspection. |
| **allow** | Allows the message. |
| **drop** | Closes the connection. |
| **log** | (Optional) Generate a syslog. |
| **reset** | Closes the connection with a TCP reset message to client and server. |

## Defaults

This command is enabled 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

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the ASA to allow forwarding of non-compliant HTTP traffic. This command overrides the default behavior, which is to deny forwarding of non-compliant HTTP traffic.

## Examples

The following example allows forwarding of non-compliant HTTP traffic:

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)#
```

## Related Commands

| Commands | Description |
|---|---|
| **class-map** | Defines the traffic class to which to apply security actions. |
| **debug appfw** | Displays detailed information about traffic associated with enhanced HTTP inspection. |
| **http-map** | Defines an HTTP map for configuring 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. |

# strip-group

This command applies only to usernames received in the form user@realm. A realm is an administrative domain appended to a username with the "@" delimiter (juser@abc).

To enable or disable strip-group processing, use the **strip-group** command in tunnel-group general-attributes mode. The ASA selects the tunnel group for IPsec connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the ASA sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the ASA sends the entire username including the realm.

To disable strip-group processing, use the **no** form of this command.

**strip-group**

**no strip-group**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default setting for this command is disabled.

## 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 |
| Tunnel-group general attributes configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was introduced. |

## Usage Guidelines

You can apply this attribute only to the IPsec remote access tunnel-type.

**Note** Because of a limitation of MSCHAPv2, you cannot perform tunnel group switching when MSCHAPv2 is used for PPP authentication. The hash computation during MSCHAPv2 is bound to the username string (such as user + delimit + group).

## Examples

The following example configures a remote access tunnel group named "remotegrp" for type IPsec remote access, then enters general configuration mode, sets the tunnel group named "remotegrp" as the default group policy, and then enables strip group for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPsec_ra
```

```
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-group
```

## Related Commands

| Command | Description |
|---|---|
| **clear-configure tunnel-group** | Clears all configured tunnel groups. |
| **group-delimiter** | Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated. |
| **show running-config tunnel group** | Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group. |
| **tunnel-group general-attributes** | Specifies the general attributes for the named tunnel-group. |

# strip-realm

To enable or disable strip-realm processing, use the **strip-realm** command in tunnel-group general-attributes configuration mode. Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. A realm is an administrative domain appended to a username with the @ delimiter (username@realm). If the command is enabled, the ASA sends only the user part of the username authorization/authentication. Otherwise, the ASA sends the entire username.

To disable strip-realm processing, use the **no** form of this command.

**strip-realm**

**no strip-realm**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default setting for this command is disabled.

## 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 |
| Tunnel-group general attributes configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0.1 | This command was introduced. |

## Usage Guidelines

You can apply this attribute only to the IPsec remote access tunnel-type.

## Examples

The following example configures a remote access tunnel group named “remotegrp” for type IPsec remote access, then enters general configuration mode, sets the tunnel group named “remotegrp” as the default group policy, and then enables strip realm for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-real
```

# storage-key

To specify a storage key to protect the date stored between sessions, use the **storage-key** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

**storage- key** { **none** | **value** *string*}

**no storage-key**

## Syntax Description

| | |
|---|---|
| *string* | Specifies a string to use as the value of the storage key. This string can be up to 64 characters long. |

## Defaults

The default is **none**.

## 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 webvpn configuration mode | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |

## Usage Guidelines

While you can use any character except spaces in the storage key value, we recommend using only the standard alphanumeric character set: 0 through 9 and a through z.

## Examples

The following example sets the storage key to the value abc123:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-key value abc123
```

## Related Commands

| Command | Description |
|---|---|
| **storage-objects** | Configures storage objects for the data stored between sessions. |

# storage-objects

To specify which storage objects to use for the data stored between sessions, use the **storage-objects** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

**storage- objects** { **none** | **value** *string*}

**no storage-objects**

## Syntax Description

| | |
|---|---|
| *string* | Specifies the name of the storage objects. This string can be up to 64 characters long. |

## Defaults

The default is **none**.

## 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 webvpn configuration mode | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was introduced. |

## Usage Guidelines

While you can use any character except spaces and commas in the storage object name, we recommend using only the standard alphanumeric character set: 0 through 9 and a through z. Use a comma, with no space, to separate the names of storage objects in the string.

## Examples

The following example sets the storage object names to cookies and xyz456:

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# storage-object value cookies,xyz456
```

## Related Commands

| Command | Description |
|---|---|
| **storage-key** | Configures storage key to use for the data stored between sessions. |
| **user-storage** | Configures a location for storing user data between sessions |