CHAPTER 40

pre-fill-username through pwd Commands

pre-fill-username

To enable extracting a username from a client certificate for use in authentication and authorization, use the **pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

pre-fill-username {**ssl-client** | **clientless**}

no pre-fill-username

Syntax Description

ssl-client	Enables this feature for AnyConnect VPN client connections.
clientless	Enables this feature for clientless connections.

Defaults

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**
Tunnel-group webvpn-attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	This command was introduced.

Usage Guidelines

The **pre-fill-username** command enables the use of a username extracted from the certificate field specified in the **username-from-certificate** command as the username for username/password authentication and authorization. To use this pre-fill username from certificate feature, you must configure both commands.

To enable this feature, you must also configure the **username-from-certificate** command in tunnel-group general-attributes mode.

Note In Releases 8.0.4 and 8.1.2, the username is not pre-filled; instead, any data sent in the username field is ignored.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies that the name for an authentication or authorization query for an SSL VPN client must be derived from a digital certificate:

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

```
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

preempt

To cause the unit to become active on boot if it has the higher priority, use the **preempt** command in failover group configuration mode. To remove the preemption, use the **no** form of this command.

preempt [*delay*]

no preempt [*delay*]

Syntax Description

seconds	The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds.

Defaults

By default, there is no delay.

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
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). However, if one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Note If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command with a wait time of 100 seconds, so the groups will automatically become active on their preferred unit 100 seconds after the units become available.

```
hostname(config)# failover group 1
```

```
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
primary	Gives the primary unit in a failover pair priority for the failover group being configured.
secondary	Gives the secondary unit in a failover pair priority for the failover group being configured.

prefix-list

To create an entry in a prefix list for ABR type 3 LSA filtering, use the **prefix-list** command in global configuration mode. To remove a prefix list entry, use the **no** form of this command.

prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

no prefix-list *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

Syntax Description

/	A required separator between the *network* and *len* values.
deny	Denies access for a matching condition.
ge *min_value*	(Optional) Specifies the minimum prefix length to be matched. The value of the *min_value* argument must be greater than the value of the *len* argument and less than or equal to the *max_value* argument, if present.
le *max_value*	(Optional) Specifies the maximum prefix length to be matched. The value of the *max_value* argument must be greater than or equal to the value of the *min_value* argument, if present, or greater than the value of the *len* argument if the *min_value* argument is not present.
len	The length of the network mask. Valid values are from 0 to 32.
network	The network address.
permit	Permits access for a matching condition.
prefix-list-name	The name of the prefix list. The prefix-list name cannot contain spaces.
seq *seq_num*	(Optional) Applies the specified sequence number to the prefix list being created.

Defaults

If you do not specify a sequence number, the first entry in a prefix list is assigned a sequence number of 5, and the sequence number for each subsequent entry is increased by 5.

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.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **prefix-list** commands are ABR type 3 LSA filtering commands. ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one area to another area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. The ASA begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a mach is made, the ASA does not go through the rest of the list. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no prefix-list sequence-number** command. Sequence numbers are generated in increments of 5. The first sequence number generated in a prefix list would be 5. The next entry in that list would have a sequence number of 10, and so on. If you specify a value for an entry, and then do not specify values for subsequent entries, the generated sequence numbers are increased from the specified value in increments of 5. For example, if you specify that the first entry in the prefix list has a sequence number of 3, and then add two more entries without specifying a sequence number for the additional entries, the automatically generated sequence numbers for those two entries would be 8 and 13.

You can use the **ge** and **le** keywords to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/len* argument. Exact match is assumed when neither the **ge** or **le** keywords are specified. The range is from *min_value* to 32 if only the **ge** keyword is specified.The range is from *len* to *max_value* if only the **le** keyword is specified.

The value of the *min_value* and *max_value* arguments must satisfy the following condition:

len < *min_value* <= *max_value* <= 32

Use the **no** form of the command to remove specific entries from the prefix list. Use the **clear configure prefix-list** command to remove a prefix list. The clear **configure prefix-list** command also removes the associated **prefix-list description** command, if any, from the configuration.

Examples

The following example denies the default route 0.0.0.0/0:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

The following example permits the prefix10.0.0.0/8:

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to deny all routes with a prefix of 10/8:

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits for routes with a prefix of 192.168.1/24:

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to permit all routes with a prefix of 0/0:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list description	Lets you to enter a description for a prefix list.
prefix-list sequence-number	Enables prefix list sequence numbering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list description

To add a description to a prefix list, use the **prefix-list description** command in global configuration mode. To remove a prefix list description, use the **no** form of this command.

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

Syntax Description

prefix-list-name	The name of a prefix list.
text	The text of the prefix list description. You can enter a maximum of 80 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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can enter **prefix-list** and **prefix-list description** commands in any order for a particular prefix list name; you do not need to create the prefix list before entering a prefix list description. The **prefix-list description** command will always appear on the line before the associated prefix list in the configuration, no matter what order you enter the commands.

If you enter a **prefix-list description** command for a prefix list entry that already has a description, the new description replaces the original description.

You do not need to enter the text description when using the **no** form of this command.

Examples

The following example adds a description for a prefix list named MyPrefixList. The **show running-config prefix-list** command shows that although the prefix list description has been added to the running configuration, the prefix-list itself has not been configured.

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
```

!

Related Commands

Command	Description
clear configure prefix-list	Removes the **prefix-list** commands from the running configuration.
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prefix-list sequence-number

To enable prefix list sequence numbering, use the **prefix-list sequence-number** command in global configuration mode. To disable prefix list sequence numbering, use the **no** form of this command.

prefix-list sequence-number

Syntax Description

This command has no arguments or keywords.

Defaults

Prefix list sequence numbering 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
Global 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. When the **no** form of this command is in the configuration, the sequence numbers, including the manually configured ones, are removed from the **prefix-list** commands in the configuration and new prefix lists entries are not assigned a sequence number.

When prefix list sequence numbering is enabled, all prefix list entries are assigned sequence numbers using the default numbering method (starting with 5 and incrementing each number by 5). If a sequence number was manually assigned to a prefix list entry before numbering was disabled, the manually assigned number is restored. Sequence numbers that are manually assigned while automatic numbering is disabled are also restored, even though they are not displayed while numbering is disabled.

Examples

The following example disables prefix list sequence numbering:

```
hostname(config)# no prefix-list sequence-number
```

Related Commands

Command	Description
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the **prefix-list** commands in the running configuration.

prf

To specify the pseudo-random function (PRF) in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the **prf** command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

prf {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

no prf {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

Syntax Description

md5	Specifies the MD5 algorithm.
sha	(Default) Specifies the Secure Hash Algorithm SHA 1.
sha256	Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest.
sha384	Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest.
sha512	Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest.

Defaults

The default is **sha** (SHA 1).

Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the **crypto ikev2 policy** command, use the **prf** command to select the pseudo-random function used for the construction of keying material for all of the cryptographic algorithms used in the SA.

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(1)	This command was added.
8.4(2)	The **sha256**, **sha384**, and **sha512** keywords were added for SHA 2 support.

Examples

The following example enters IKEv2 policy configuration mode and sets the PRF to MD5:

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# prf md5
```

Related Commands

Command	Description
encryption	Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections.
group	Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections.
integrity	Specifies the ESP integrity algorithm in an IKEv2 SA for AnyConnect IPsec connections.
lifetime	Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections.

primary

To give the primary unit higher priority for a failover group, use the **primary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

primary

no primary

Syntax Description

This command has no arguments or keywords.

Defaults

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

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
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). If one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
```

```
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
secondary	Gives the secondary unit a higher priority than the primary unit.

priority (class)

To enable QoS priority queueing, use the **priority** command in class configuration mode. For critical traffic that cannot tolerate latency, such as voice over IP (VoIP), you can identify traffic for low latency queueing (LLQ) so that it is always transmitted at a minimum rate. To remove the priority requirement, use the **no** form of this command.

Note This command is not supported on the ASA Services Module.

priority

no priority

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or variables.

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
Class configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The ASA supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface (see the **priority-queue** command), while all other traffic goes into the "best effort" queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size. You can also fine-tune the maximum number of packets allowed into the transmit queue. These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.

- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue (the **shape** command). A subset of the shaped traffic can be prioritized. The standard priority queue is not used. See the following guidelines about hierarchical priority queueing:
  - Priority packets are always queued at the head of the shape queue so they are always transmitted ahead of other non-priority queued packets.
  - Priority packets are never dropped from the shape queue unless the sustained rate of priority traffic exceeds the shape rate.
  - For IPsec-encrypted packets, you can only match traffic based on the DSCP or precedence setting.
  - IPsec-over-TCP is not supported for priority traffic classification.

Configuring QoS with Modular Policy Framework

To enable priority queueing, use the Modular Policy Framework. You can use standard priority queueing or hierarchical priority queueing.

For standard priority queueing, perform the following tasks:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map.
3. **service-policy**—Assigns the policy map to an interface or globally.

For hierarchical priority-queueing, perform the following tasks:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map** (for priority queueing)—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.
3. **policy-map** (for traffic shaping)—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.
   c. **service-policy**—Call the priority queueing policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following is an example of the **priority** command in policy-map configuration mode:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)#
```

Related Commands

class	Specifies a class map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

priority (cluster group)

To set the priority of this unit for master unit elections in an ASA cluster, use the **priority** command in cluster group configuration mode. To remove the priority, use the **no** form of this command.

priority *priority_number*

no priority [*priority_number*]

Syntax Description

priority_number	Sets the priority of this unit for master unit elections, between 1 and 100, where 1 is the highest priority.

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

Members of the cluster communicate over the cluster control link to elect a master unit, as follows:

1. When you enable clustering for a unit (or when it first starts up with clustering already enabled), it broadcasts an election request every 3 seconds.
2. Any other units with a higher priority respond to the election request; the priority is set between 1 and 100, where 1 is the highest priority.
3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes master.

Note If multiple units tie for the highest priority, the cluster unit name, and then the serial number is used to determine the master.

4. If a unit later joins the cluster with a higher priority, it does not automatically become the master unit; the existing master unit always remains as the master unless it stops responding, at which point a new master unit is elected.

Note You can manually force a unit to become the master using the **cluster master unit** command. For centralized features, if you force a master unit change, then all connections are dropped, and you have to re-establish the connections on the new master unit. See the configuration guide for a list of centralized features.

Examples

The following example sets the priority to 1 (the highest):

```
hostname(config)# cluster group cluster1
hostname(cfg-cluster)# priority 1
```

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.
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 (vpn load balancing)

To set the priority of the local device participating in the virtual load-balancing cluster, use the **priority** command in VPN load-balancing mode. To revert to the default priority specification, use the **no** form of this command.

priority *priority*

no priority

Syntax Description

priority	The priority, in the range of 1 to 10, that you want to assign to this device.

Defaults

The default priority depends on the model number of the device:

Model Number	Default Priority
5520	5
5540	7

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	—	—	•	—	—

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 mode.

This command sets the priority of the local device participating in the virtual load-balancing cluster.

The priority must be an integer in the range of 1 (lowest) to 10 (highest).

The priority is used in the master-election process as one way to determine which of the devices in a VPN load-balancing cluster becomes the master or primary device for the cluster. See CLI configuration guide for details about the master-election process.

The **no** form of the command reverts the priority specification to the default value.

Examples

The following is an example of a VPN load-balancing command sequence that includes a **priority** command that sets the priority of the current device to 9:

```
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)# priority 9
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
vpn load-balancing	Enter VPN load-balancing mode.

priority-queue

To create a standard priority queue on an interface for use with the **priority** command, use the **priority-queue** command in global configuration mode. To remove the queue, use the **no** form of this command.

Note This command is not supported on ASA 5580 Ten Gigabit Ethernet interfaces. (Ten Gigabit Ethernet interfaces are supported for priority queues on the ASA 5585-X.) This command is also not supported for the ASA 5512-X through ASA 5555-X Management interface.

This command is not supported on the ASA Services Module.

priority-queue *interface-name*

no priority queue *interface-name*

Syntax Description

interface-name	Specifies the name of the physical interface on which you want to enable the priority queue, or for the ASA 5505 or ASASM, the name of the VLAN interface.

Defaults

By default, priority queuing 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
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.2(3)/8.4(1)	Support for Ten Gigabit Ethernet interfaces was added for the ASA 5585-X.

Usage Guidelines

LLQ priority queueing lets you prioritize certain traffic flows (such as latency-sensitive traffic like voice and video) ahead of other traffic.

The ASA supports two types of priority queueing:

- Standard priority queueing—Standard priority queueing uses an LLQ priority queue on an interface that yopu create using the **priority-queue** command, while all other traffic goes into the "best effort" queue. Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is called *tail drop*. To avoid having the queue fill up, you can increase the queue buffer size (the **queue-limit** command).

You can also fine-tune the maximum number of packets allowed into the transmit queue (the **tx-ring-limit** command). These options let you control the latency and robustness of the priority queuing. Packets in the LLQ queue are always transmitted before packets in the best effort queue.

- Hierarchical priority queueing—Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used.

Note On the ASA 5505 only, configuring a priority queue on one interface overwrites the same configuration on all other interfaces; only the last applied configuration is present on all interfaces. Also, if the priority queue configuration is removed from one interface, it is removed from all interfaces. To work around this issue, configure the **priority-queue** command on only one interface. If different interfaces need different settings for the **queue-limit** and/or **tx-ring-limit** commands, use the largest of all queue limits and smallest of all tx-ring-limits on any one interface (CSCsi13132).

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 30,000 packets and a transmit queue limit of 256 packets.

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

Related Commands

Command	Description
queue-limit	Specifies the maximum number of packets that can be enqueued to a priority queue before it drops data.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure priority-queue	Removes the current priority queue configuration.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.

privilege

To configure command privilege levels for use with command authorization (local, RADIUS, and LDAP (mapped) only), use the **privilege** command in global configuration mode. To disallow the configuration, use the **no** form of this command.

privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

no privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

Syntax Description

clear	(Optional) Sets the privilege only for the clear form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
command *command*	Specifies the command you are configuring. You can only configure the privilege level of the *main* command. For example, you can configure the level of all **aaa** commands, but not the level of the **aaa authentication** command and the **aaa authorization** command separately. Also, you cannot configure the privilege level of subcommands separately from the main command. For example, you can configure the **context** command, but not the **allocate-interface** command, which inherits the settings from the **context** command.
configure	(Optional) Sets the privilege only for the configure form of the command. The configure form of the command is typically the form that causes a configuration change, either as the unmodified command (without the **show** or **clear** prefix) or as the **no** form. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.
level *level*	Specifies the privilege level; valid values are from 0 to 15. Lower privilege level numbers are lower privilege levels.
mode enable	(Optional) If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately. The **mode enable** keyword specifies both user EXEC mode and privileged EXEC mode.
mode configure	(Optional) If a command can be entered in user EXEC/privileged EXEC mode as well as configuration mode, and the command performs different actions in each mode, you can set the privilege level for these modes separately. The mode **configure** keyword specifies configuration mode, accessed using the **configure terminal** command.
show	(Optional) Sets the privilege only for the show form of the command. If you do not use the **clear**, **show**, or **configure** keywords, all forms of the command are affected.

Defaults

By default, the following commands are assigned to privilege level 0. All other commands are at level 15.

- **show checksum**
- **show curpriv**

- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

If you move any configure mode commands to a lower level than 15, be sure to move the **configure** command to that level as well, otherwise, the user will not be able to enter configuration mode.

To view all privilege levels, see the **show running-config all privilege all** command.

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)	Support for RADIUS users with Cisco VSA CVPN3000-Privilege-Level was added. LDAP users are supported if you map the LDAP attribute to the CVPN3000-Privilege-Level using the **ldap map-attributes** command.

Usage Guidelines

The **privilege** command lets you set privilege levels for ASA commands when you configure the **aaa authorization command LOCAL** command. Even though the command uses the **LOCAL** keyword, this keyword enables local, RADIUS, and LDAP (mapped) authorization.

Examples

For example, the **filter** command has the following forms:

- **filter** (represented by the **configure** option)
- **show running-config filter**
- **clear configure filter**

You can set the privilege level separately for each form, or set the same privilege level for all forms by omitting this option. For example, set each form separately as follows:

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

Alternatively, you can set all filter commands to the same level:

```
hostname(config)# privilege level 5 command filter
```

The **show privilege** command separates the forms in the display.

The following example shows the use of the **mode** keyword. The **enable** command must be entered from user EXEC mode, while the **enable password** command, which is accessible in configuration mode, requires the highest privilege level.

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

The following example shows an additional command, the **configure** command, which uses the **mode** keyword:

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

Note This last line is for the **configure terminal** command.

Related Commands

Command	Description
clear configure privilege	Removes privilege command statements from the configuration.
show curpriv	Displays current privilege level.
show running-config privilege	Displays privilege levels for commands.

prompt

To customize the CLI prompt, use the **prompt** command in global configuration mode. To revert to the default prompt, use the **no** form of this command.

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]

Syntax Description

cluster-unit	Displays the cluster unit name. Each unit in a cluster can have a unique name.
context	(Multiple mode only) Displays the current context.
domain	Displays the domain name.
hostname	Displays the hostname.
priority	Displays the failover priority as pri (primary) or sec (secondary). Set the priority using the **failover lan unit** command.
state	Displays the traffic-passing state or role of the unit. For failover, the following values are displayed for the **state** keyword: • act—Failover is enabled, and the unit is actively passing traffic. • stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state. • actNoFailover—Failover is not enabled, and the unit is actively passing traffic. • stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit. For clustering, the following values are displayed for the **state** keyword: • master • slave For example, if you set **prompt hostname cluster-unit state**, then in the prompt "ciscoasa/cl2/slave>", the hostname is ciscoasa, the unit name is cl2, and the state name is slave.

Defaults

The default prompt is the hostname. In multiple context mode, the hostname is followed by the current context name (*hostname*/*context*).

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
7.2(1)	This command was introduced.
9.0(1)	The **cluster-unit** option was added. The **state** keyword was updated for clustering.

Usage Guidelines

The order in which you enter the keywords determines the order of the elements in the prompt, which are separated by a slash (/).

In multiple context mode, you can view the extended prompt when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

The ability to add information to a prompt allows you to see at-a-glance which ASA you are logged into when you have multiple modules. During a failover, this feature is useful when both ASAs have the same hostname.

Examples

The following example shows all available elements in the prompt available for failover:

```
hostname(config)# prompt hostname context slot state priority
```

The prompt changes to the following string:

```
hostname/admin/pri/act(config)#
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
show running-config prompt	Displays the configured prompt.

protocol

To specify the protocol and encryption types for an IPsec proposal for IKEv2 connections, use the **protocol** command from IPsec proposal configuration mode. To remove the protocol and encryption types, use the **no** form of the command:

protocol esp {**encryption** {**des | 3des | aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null**} | **integrity** {**md5 | sha-1 | sha-256 | sha-384 | sha-512 | null**}

no protocol esp {**encryption** {**des | 3des | aes | aes-192 | aes-256 | | aes-gcm | aes-gcm-192 | aes-gcm-256 | aes-gmac | aes-gmac-192 | aes-gmac-256 | null**} | **integrity** {**md5 | sha-1 | sha-256 | sha-384 | sha-512 | null**}

Syntax Description

esp	Specifies the Encapsulating Security Payload (ESP) IPsec protocol (currently the only supported protocol for IPsec).
des	Specifies 56-bit DES-CBC encryption for ESP.
3des	(Default) Specifies the triple DES encryption algorithm for ESP.
aes	Specifies AES with a 128-bit key encryption for ESP.
aes-192	Specifies AES with a 192-bit key encryption for ESP.
aes-256	Specifies AES with a 256-bit key encryption for ESP.
aes-gcm	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gcm-192	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gcm-256	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac-192	Specifies which AES-GCM or AES-GMAC algorithm to use.
aes-gmac-256	Specifies which AES-GCM or AES-GMAC algorithm to use.
null	Does not use encryption for ESP.
integrity	Specifies the integrity algorithm for the IPsec protocol.
md5	Specifies the md5 algorithm for the ESP integrity protection.
sha-1	(Default) Specifies the Secure Hash Algorithm (SHA) SHA-1, defined in the U.S. Federal Information Processing Standard (FIPS), for ESP integrity protection.
sha-256	Specifies which algorithm to use as an IPsec integrity algorithm.
sha-384	Specifies which algorithm to use as an IPsec integrity algorithm.
sha-512	Specifies which algorithm to use as an IPsec integrity algorithm.
null	Choose if AES-GCM/GMAC is configured as the encryption algorithm.

Defaults

The default settings for an IPsec proposal are the encryption type 3DES and the integrity type SHA-1.

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
IPsec proposal configuration	•	•	•	—	—

Command History

Release	Modification
8.4(1)	This command was introduced.
9.0(1)	Added AES-GCM or AES-GMAC algorithm support. Added ability to choose an algorithm to use as an IPsec integrity algorithm.

Usage Guidelines

IKEv2 IPsec proposals can have multiple encryption and integrity types. Use this command to specify the types, which allows the peer to pick and choose as desired.

You must choose the null integrity algorithm if AES-GMC/GMAC is configured as the encryption algorithm.

Examples

The following example creates the IPsec proposal *proposal_1*, configures the ESP encryption types DES and 3DES, and specifies the crypto algorithms MD5 and SHA-1 for integrity protection:

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
hostname(config-ipsec-proposal)# protocol ESP encryption des 3des
hostname(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

Related Commands

Command	Description
crypto ikev2 enable	Enables ISAKMP IKEv2 negotiation on the interface on which the IPsec peer communicates.
crypto ipsec ikev2 ipsec-proposal	Creates an IPsec proposal and enters IPsec proposal configuration mode where you specify multiple encryption and integrity types for the proposal.
show running-config ipsec	Displays the configuration of all transform sets.
crypto map set transform-set	Specifies the transform sets to use in a crypto map entry.
crypto dynamic-map set transform-set	Specifies the transform sets to use in a dynamic crypto map entry.
show running-config crypto map	Displays the crypto map configuration.
show running-config crypto dynamic-map	Displays the dynamic crypto map configuration.

protocol-enforcement

To enable the domain name, label length, and format check, including compression and looped pointer check, use the **protocol-enforcement** command in parameters configuration mode. To disable protocol enforcement, use the **no** form of this command.

protocol-enforcement

no protocol-enforcement

Syntax Description

This command has no arguments or keywords.

Defaults

Protocol enforcement is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no protocol-enforcement** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, NAT rewrite is not performed.

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

Under certain conditions, protocol enforcement is performed even if the command is disabled. This occurs when parsing a DNS resource record is required for other purposes, such as DNS resource record classification, NAT or TSIG check.

Examples

The following example shows how to enable protocol enforcement in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-enforcement
```

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.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in ca-crl configuration mode. To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command.

protocol http

no protocol http

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit HTTP.

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-crl configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you use this command, be sure to assign HTTP rules to the public interface filter. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

Examples

The following example enters ca-crl configuration mode, and permits HTTP as a distribution point protocol for retrieving a CRL for trustpoint central:

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

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
protocol ldap	Specifies LDAP as a retrieval method for CRLs.
protocol scep	Specifies SCEP as a retrieval method for CRLs.

protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in ca-crl configuration mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol ldap

no protocol ldap

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit LDAP.

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
crl configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and permits LDAP as a distribution point protocol for retrieving a CRL for trustpoint central:

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

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in crl configure mode. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command.

protocol scep

no protocol scep

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit SCEP.

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
Crl configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and permits SCEP as a distribution point protocol for retrieving a CRL for trustpoint central:

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

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol ldap	Specifies LDAP as a retrieval method for CRLs

protocol-object

To add a protocol object to a protocol object group, use the **protocol-object** command in protocol configuration mode. To remove port objects, use the **no** form of this command.

protocol-object *protocol*

no protocol-object *protocol*

Syntax Description

protocol	Protocol name or 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
Protocol configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **protocol-object** command is used with the **object-group** command to define a protocol object in protocol configuration mode.

You can specify an IP protocol name or number using the *protocol* argument. The udp protocol number is 17, the tcp protocol number is 6, and the egp protocol number is 47.

Examples

The following example shows how to define protocol objects:

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

protocol-violation

To define actions when a protocol violation occurs with HTTP and NetBIOS inspection, use the **protocol-violation** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

protocol-violation action [**drop** [**log**] | **log**]

no protocol-violation action [**drop** [**log**] | **log**]

Syntax Description

drop	Specifies to drop packets that do not conform to the protocol.
log	Specifies to log the protocol violations.

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

This command can be configured in an HTTP or NetBIOS policy map. A syslog is issued when the HTTP or NetBIOS parser cannot detect a valid HTTP or NetBIOS message in the first few bytes of the message. This occurs, for instance, when a chunked encoding is malformed and the message cannot be parsed.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation action drop
```

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.

proxy-auth

To flag the tunnel group as a specific proxy authentication tunnel group, use the **proxy-auth** command in webvpn configuration mode.

proxy-auth [**sdi**]

Syntax Description

sdi	Parses RADIUS/TACACS SDI proxy messages into native SDI directives.

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**
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use the **proxy-auth** command for enabling the parsing of aaa-server proxy authentication text messages into native protocol directives.

proxy-auth_map sdi

To map RADIUS challenge messages returned from a RADIUS proxy server to native SDI messages, use the **proxy-auth_map sdi** command in aaa-server configuration mode.

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

Syntax Description

radius_challenge_message	Specifies the RADIUS challenge messages that are used to map specific SDI messages, which can any of the following: • new-pin-meth—New PIN Method, [default] Do you want to enter your own pin • new-pin-reenter—Reenter new PIN, [default] Reenter PIN: • new-pin-req—New PIN requested, [default] Enter your new Alpha-Numerical PIN • new-pin-sup—New PIN supplied, [default] Please remember your new PIN • new-pin-sys-ok—New PIN accepted, [default] New PIN Accepted • next-ccode-and-reauth—Reauthenticate on token change, [default] new PIN with the next card code • next-code—Provide the tokencode without PIN, [default] Enter Next PASSCODE • ready-for-sys-pin—Accept system generated PIN, [default] ACCEPT A SYSTEM GENERATED PIN
sdi_message	Specifies the native SDI messages.

Defaults

The default mapping on the ASA corresponds to default settings on the Cisco ACS (including the system administration, configuration, and RSA SecureID prompts), which also synchronizes with default settings on the RSA Authentication Manager.

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 configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

To enable parsing and mapping of RADIUS challenge messages from a RADIUS proxy, you must enable the **proxy-auth** command in tunnel-group configuration mode. Then default mapping values are used. You can change the default mapping values using the **proxy-auth_map** command.

A remote user connects to the ASA with the AnyConnect client and tries to authenticate using an RSA SecurID token. The ASA can be configured to use a RADIUS proxy server which in turn, communicates with the SDI server about that authentication.

During authentication, the RADIUS server presents access challenge messages to the ASA. Within these challenge messages are reply messages containing text from the SDI server. The message text is different when the ASA is communicating directly with an SDI server than when the ASA is communicating through the RADIUS proxy.

Therefore, to appear as a native SDI server to the AnyConnect client, the ASA must interpret the messages from the RADIUS server. Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication. The AnyConnect client might fail to respond, and authentication might fail.

Related Commands

Command	Description
proxy-auth	Enables parsing and mapping of RADIUS challenge messages from a RADIUS proxy.

proxy-bypass

To configure the ASA to perform minimal content rewriting, and to specify the types of content to rewrite—external links and/or XML—use the **proxy-bypass** command in webvpn configuration mode. To disable proxy bypass, use the **no** form of the command.

proxy-bypass interface *interface name* **{port** *port number***| path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

no proxy-bypass interface *interface name* **{port** *port number***| path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

Syntax Description

host	Identifies the host to forward traffic to. Use either the host IP address or a hostname.
interface	Identifies the ASA interface for proxy bypass.
interface name	Specifies an ASA interface by name.
link	Specifies rewriting of absolute external links.
none	Specifies no rewriting.
path-mask	Specifies the pattern to match.
path-mask	Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 128 bytes.
port	Identifies the port reserved for proxy bypass.
port number	Specifies a high numbered port reserved for proxy bypass. The port range is 20000-21000. You can use a port for one proxy bypass rule only.
rewrite	(Optional) Specifies the additional rules for rewriting: none or a combination of XML and links.
target	Identifies the remote server to forward the traffic to.
url	Enter the URL in the format **http(s)://***fully_qualified_domain_name*[:*port*]. Maximum 128 bytes. The port for HTTP is 80 and for HTTPS it is 443, unless you specify another port.
xml	Specifies rewriting XML content.

Defaults

No default behavior or values.

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
WebVPN configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use proxy bypass for applications and web resources that work better with minimum content rewriting. The proxy-bypass command determines how to treat specific web applications that travel through the ASA.

You can use this command multiple times. The order in which you configure entries is unimportant. The interface and path mask or interface and port uniquely identify a proxy bypass rule.

If you configure proxy bypass using ports rather than path masks, depending on your network configuration, you might need to change your firewall configuration to allow these ports access to the ASA. Use path masks to avoid this restriction. Be aware, however, that path masks can change, so you might need to use multiple pathmask statements to exhaust the possibilities.

A path is everything in a URL after the .com or .org or other types of domain name. For example, in the URL www.example.com/hrbenefits, *hrbenefits* is the path. Similarly, for the URL www.example.com/hrinsurance, *hrinsurance* is the path. If you want to use proxy bypass for all hr sites, you can avoid using the command multiple times by using the * wildcard as follows: /hr*.

Examples

The following example shows how to configure the ASA to use port 20001 for proxy bypass over the webvpn interface, using HTTP and its default port 80, to forward traffic to example.com and to rewrite XML content.

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://example.com rewrite xml
```

The next example shows how to configure the ASA to use the path mask mypath/* for proxy bypass on the outside interface, using HTTP and its default port 443 to forward traffic to example.com, and to rewrite XML and link content.

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://example.com rewrite xml,link
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
rewrite	Determines whether traffic travels through the ASA.

proxy-ldc-issuer

To issue TLS proxy local dynamic certificates, use the **proxy-ldc-issuer** command in crypto ca trustpoint configuration mode. To remove the configuration, use the **no** form of this command.

proxy-ldc-issuer

no proxy-ldc-issuer

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
8.0(2)	This command was introduced.

Usage Guidelines

Use the **proxy-ldc-issuer** command to issue TLS proxy local dynamic certificates. The **proxy-ldc-issuer** command grants a crypto trustpoint the role as local CA to issue the LDC and can be accessed from crypto ca trustpoint configuration mode.

The **proxy-ldc-issuer** command defines the local CA role for the trustpoint to issue dynamic certificates for TLS proxy. This command can only be configured under a trustpoint with "enrollment self."

Examples

The following example shows how to create an internal local CA to sign the LDC for phones. This local CA is created as a regular self-signed trustpoint with **proxy-ldc-issuer** enabled.

```
hostname(config)# crypto ca trustpoint ldc_server
hostname(config-ca-trustpoint)# enrollment self
hostname(config-ca-trustpoint)# proxy-ldc-issuer
hostname(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
hostname(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
hostname(config-ca-trustpoint)# keypair ldc_signer_key
hostname(config)# crypto ca enroll ldc_server
```

Related Commands

Commands	Description
ctl-provider	Defines a CTL provider instance and enters 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 sessions.

proxy-server

To configure an HTTP proxy for the Phone Proxy feature that is written into the IP phone's configuration file under the <proxyServerURL> tag, use the **proxy-server** command in phone-proxy configuration mode. To remove the HTTP proxy configuration from the Phone Proxy, use the **no** form of this command.

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

Syntax Description

interface *ifc*	Specifies the interface on which the HTTP proxy resides on the ASA.
ip_address	Specifies the IP address of the HTTP proxy.
listen_port	Specifies the listening port of the HTTP proxy. If not specified, the default will be 8080.

Defaults

If the listen port is not specified, the port is configured to be 8080 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**
Phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Setting the proxy server configuration option for the Phone Proxy allows for an HTTP proxy on the DMZ or external network in which all the IP phone URLs are directed to the proxy server for services on the phones. This setting accommodates nonsecure HTTP traffic, which is not allowed back into the corporate network.

The *ip_address* you enter should be the global IP address based on where the IP phone and HTTP proxy server is located.

If the proxy server is located in a DMZ and the IP phones are located outside the network, the ASA does a lookup to see if there is a NAT rule and uses the global IP address to write into the configuration file.

You can enter a hostname in the *ip_address* argument when that hostname can be resolved to an IP address by the ASA (for example, DNS lookup is configured) because the ASA will resolve the hostname to an IP address.

By default, the Phone URL Parameters configured under the Enterprise Parameters use an FQDN in the URLs. The parameters might need to be changed to use an IP address if the DNS lookup for the HTTP proxy does not resolve the FQDNs.

To make sure the proxy server URL was written correctly to the IP phones configuration files, check the URL on an IP phone under Settings > Device Configuration > HTTP configuration >Proxy Server URL.

The Phone Proxy does not inspect this HTTP traffic to the proxy server.

If the ASA is in the path of the IP phone and the HTTP proxy server, use existing debugging techniques (such as syslogs and captures) to troubleshoot the proxy server.

You can configure only one proxy server while the Phone Proxy is in use; however, if the IP phones have already downloaded their configuration files after you have configured the proxy server, you must restart the IP phones so that they get the configuration file with the proxy server's address in the file.

Examples

The following example shows the use of the **proxy-server** command to configure the HTTP proxy server for the Phone Proxy:

```
hostname(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

publish-crl

To allow other ASAs to validate the revocation status of certificates issued by the local CA, use the **publish-crl** command in ca-server configuration mode to allow downloading of the CRL directly from and interface on the ASA. To make the CRL unavailable for downloading, use the **no** form of this command.

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

Syntax Description

interface *interface*	Specifies the *nameif* used for the interface, such as **gigabitethernet0/1**. See the **interface** command for details.
port *portnumber*	(Optional) Specifies the port on which the interface device expects to download the CRL. Port numbers can be in the range of 1-65535.

Defaults

The default **publish-crl** status is **no publish**. TCP port 80 is the default for HTTP.

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-server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The CRL is inaccessible by default. You must enable access to the CRL file on the interface and port required.

TCP port 80 is the HTTP default port number. If you configure a non-default port (other than port 80), be sure the **cdp-url** configuration includes the new port number so other devices know to access this specific port.

The CRL Distribution Point (CDP) is the location of the CRL on the local CA ASA. The URL you configure with the **cdp-url** command is embedded into any issued certificates. If you do not configure a specific location for the CDP, the default CDP URL is: http://hostname.domain/+CSCOCA+/asa_ca.crl.

An HTTP redirect and a CRL download request are handled by the same HTTP listener, if Clientless SSL VPN is enabled on the same interface. The listener checks for the incoming URL and if it matches the one configured with the **cdp-url** command, the CRL file downloads. If the URL does not match the **cdp-url** command, the connection is redirected to HTTPS (if HTTP redirect is enabled).

Examples

The **publish-crl** command example, entered in ca-server configuration mode, enables port 70 of the outside interface for CRL download:

```
hostname(config)# crypto ca server
hostname (config-ca-server)#publish-crl outside 70
hostname(config-ca-server)#
```

Related Commands

Command	Description
cdp-url	Specifies a particular location for the automatically generated CRL.
show interface	Displays the runtime status and statistics of interfaces.

pwd

To display the current working directory, use the **pwd** command in privileged EXEC mode.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

The root directory (/) is the 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	This command was introduced.

Usage Guidelines

This command is similar in functionality to the **dir** command.

Examples

The following example shows how to display the current working directory:

```
hostname# pwd
disk0:/
hostname# pwd
flash:
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
more	Displays the contents of a file.