u

uc-ime (Deprecated)

To create the Cisco Intercompany Media Engine proxy instance, use the **uc-ime** command in global configuration mode. To remove the proxy instance, use the **no** form of this command.

uc-ime *uc-ime_name*
no uc-ime *uc-ime_name*

Syntax Description

uc-ime_name	Specifies the instance name of the Cisco Intercompany Media Engine proxy configured on the ASA. The *name* is limited to 64 characters. Only one Cisco Intercompany Media Engine proxy can be configured on the ASA.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.
9.4(1)	This command was deprecated.

Usage Guidelines

Configures the Cisco Intercompany Media Engine proxy. Cisco Intercompany Media Engine enables companies to interconnect on-demand, over the Internet with advanced features made available by VoIP technologies. Cisco Intercompany Media Engine allows for business-to-business federation between Cisco Unified Communications Manager clusters in different enterprises by utilizing peer-to-peer, security, and SIP protocols to create dynamic SIP trunks between businesses. A collection of enterprises work together to end up looking like one large business with inter-cluster trunks between them.

You must create the media termination instance before you specify it in the Cisco Intercompany Media Engine proxy.

Only one Cisco Intercompany Media Engine proxy can be configured on the ASA.

Examples

The following example shows how to configure a Cisco Intercompany Media Engine proxy by using the **uc-ime** command.

```
ciscoasa
(config)# uc-ime local_uc-ime_proxy
```

```
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

Related Commands

Command	Description
fallback	Configures the fallback timers that the Cisco Intercompany Media Engine uses to fallback from VoIP to PSTN when connection integrity degrades.
show uc-ime	Displays statistical or detailed information about fallback-notifications, mapping-service-sessions, and signaling-sessions.
ticket	Configures the ticket epoch and password for the Cisco Intercompany Media Engine proxy.
ucm	Configures the Cisco UCMs that the Cisco Intercompany Media Engine Proxy connects to.

ucm (Deprecated)

To configure which Cisco Unified Communication Managers (UCM) that the Cisco Intercompany Media Engine Proxy connects to, use the **ucm** command in global configuration mode. To remove the Cisco UCMs that are connected to the Cisco Intercompanuy Media Engine Proxy, use the **no** form of this command.

ucm address *ip_address* **trunk-security-mode** { **nonsecure | secure** }
no ucm address *ip_address* **trunk-security-mode** { **nonsecure | secure** }

Syntax Description

address	The keyword to configure the IP address of the Cisco Unified Communications Manager (UCM).
ip_address	Specifies the IP address of the Cisco UCM. Enter the IP address in IPv4 format.
nonsecure	Specifies that the Cisco UCM or Cisco UCM cluster is operating in non-secure mode.
secure	Specifies that the Cisco UCM or Cisco UCM cluster is operating in secure mode.
trunk-security-mode	The keyword to configure the security mode of the Cisco UCM or Cisco UCM cluster.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
UC-IME configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.
9.4(1)	This command was deprecated along with all **uc-ime** mode commands.

Usage Guidelines

Specifies the Cisco UCM server in the enterprise.

You can enter multiple **ucm** commands for the Cisco Intercompany Media Engine proxy.

Note You must include an entry for each Cisco UCM in the cluster with Cisco Intercompany Media Engine that has a SIP trunk enabled.

Specifying **secure** for Cisco UCM or Cisco UCM cluster indicates that Cisco UCM or Cisco UCM cluster is initiating TLS; therefore, you must set up configure TLS for components.

You can specify the **secure** option in this task or you can update it later while configuring TLS for the enterprise.

TLS within the enterprise refers to the security status of the Cisco Intercompany Media Engine trunk as seen by the ASA.

If the transport security for the Cisco Intercompany Media Engine trunk changes on Cisco UCM, it must be changed on the adaptive security appliance as well. A mismatch will result in call failure. The adaptive security appliance does not support SRTP with non-secure IME trunks. The adaptive security appliance assumes SRTP is allowed with secure trunks. So SRTP Allowed must be checked for IME trunks if TLS is used. The ASA supports SRTP fallback to RTP for secure IME trunk calls.

The proxy sits on the edge of the enterprise and inspects SIP signaling between SIP trunks created between enterprises. It terminates TLS signaling from the Internet and initiates TCP or TLS to Cisco UCM.

Transport Layer Security (TLS) is a cryptographic protocol that provides security for communications over networks such as the Internet. TLS encrypts the segments of network connections at the Transport Layer end-to-end.

This task is not required if TCP is allowable within the inside network.

Key steps for Configuring TLS within the local enterprise:

- On the local ASA, create another RSA key and trustpoint for the self-signed certificate.
- Exporting and importing the certificates between the local Cisco UCM and local ASA.
- Create a trustpoint for local Cisco UCM on the ASA.

Authentication via TLS: In order for the ASA to act as a port on behalf of N enterprises, the Cisco UCMs must be able to accept the one certificate from the ASA. This can be done by associating all the UC-IME SIP trunks with the same SIP security profile containing the same subject name as that of the one presented by the ASA because the Cisco UCM extracts the subject name from the certificate and compares that with the name configured in the security profile.

Examples

The following example shows how to connect to a UCM proxy:

```
ciscoasa
(config)# uc-ime local_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
```

umbrella

To enable the DNS inspection engine to redirect DNS lookup requests to Cisco Umbrella, use the **umbrella** command in DNS inspection policy map parameters configuration mode. To disable Cisco Umbrella, use the **no** form of this command.

umbrella [**tag** *umbrella_policy*] [**fail-open**]
no umbrella [**tag** *umbrella_policy*] [**fail-open**]

Syntax Description

fail-open	If the Cisco Umbrella DNS server is unavailable, have Umbrella disable itself on this policy map and allow DNS requests to go to the other DNS servers configured on the system, if any. When the Umbrella DNS servers are available again, the policy map resumes using them. If you do not include this option, DNS requests continue to go to the unreachable Umbrella resolver, so they will not get a response.
tag *umbrella_policy*	(Optional.) The name of an Enterprise Security policy, which is defined in Cisco Umbrella, to apply to the device. If you do not specify a policy, or the name you enter does not exist in Cisco Umbrella, the default policy is assigned.

Command Default

If you do not specify a tag, the device registration assigns the default Enterprise Security policy.

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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.
9.12(1)	The **fail-open** keyword was added.

Usage Guidelines

Use this command when configuring a DNS inspection policy map.

The presence of this command in an active DNS inspection policy map starts the registration process with the Cisco Umbrella registration server. You need to have installed the registration server's CA certificate to establish the connection and registration, which happens over HTTPS.

You must also configure the global parameters using the **umbrella-global** command in global configuration mode.

Examples

The following example enables Umbrella using the default policy, and also enables DNScrypt, in the default inspection policy map used in global DNS inspection.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

The following example enables Umbrella to fail open, using the default policy, and also enables DNScrypt, in the default inspection policy map used in global DNS inspection. If you have already registered with a tag, and just want to add the **fail-open** option, you must include the same tag in the command or you will reregister the device with no tag.

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella
 fail-open

ciscoasa(config-pmap-p)# dnscrypt
```

Related Commands

Commands	Description
dnscrypt	Enables DNScrypt encryption for the connection between the device and Cisco Umbrella.
inspect dns	Enables DNS inspection.
policy-map type inspect dns	Creates a DNS inspection policy map.
public-key	Configures the public key used with Cisco Umbrella.
token	Identifies the API token that is needed to register with Cisco Umbrella.
timeout edns	Configures the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.
umbrella-global	Configures the Cisco Umbrella global parameters.

umbrella-global

To enter Umbrella configuration mode so that you can configure the global settings required to connect the device to the Cisco Umbrella portal, use the **umbrella-global** command in global configuration mode. Use the **no** form of this command to remove the global Umbrella configuration.

umbrella-global
no umbrella-global

Syntax Description

This command has no arguments or keywords.

Command Default

There is no default global Umbrella configuration.

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

If you subscribe to the Cisco Umbrella service, you can configure the device so that it registers with Cisco Umbrella.

The Umbrella global settings primarily define the API token that is needed to register the device with Cisco Umbrella. You obtain the token from the Cisco Umbrella dashboard.

The global settings are not sufficient to enable Umbrella. You must also enable Umbrella in your DNS inspection policy map using the umbrella command in parameters configuration mode.

Examples

The following example configures the global Umbrella settings and also shows how to enable Umbrella in the default DNS inspection policy map.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
ciscoasa(config)# policy-map type inspect dns preset_dns_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

Related Commands

Commands	Description
dnscrypt	Enables DNScrypt encryption for the connection between the device and Cisco Umbrella.
local-domain-bypass	Configures the local domains for which DNS requests should bypass Cisco Umbrella.
public-key	Configures the public key used with Cisco Umbrella.
resolver	Configures the addresses of the Cisco Umbrella DNS servers, which resolve DNS requests.
token	Identifies the API token that is needed to register with Cisco Umbrella.
timeout edns	Configures the idle timeout after which a connection from a client to the Umbrella server will be removed if there is no response from the server.
umbrella	Enables the DNS inspection engine to redirect DNS lookup requests to Cisco Umbrella.

undebug

To disable the display of debugging information in the current session, use the **undebug** command in privileged EXEC mode.

undebug { *command* | **all** }

Syntax Description

all	Disables all debug output.
command	Disables debug for the specified command. See the Usage Guidelines for information about the supported commands.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was modified. It includes additional **debug** keywords.

Usage Guidelines

The following commands can be used with the **undebug** command. For more information about debugging a specific command, or for the associated arguments and keywords for a specific **debug** command, see the entry for the **debug** command.

- aaa—AAA information
- acl—ACL information
- all—All debugging
- appfw—Application firewall information
- arp—ARP including NP operations
- asdm—ASDM information
- auto-update—Auto-update information
- boot-mem—Boot memory calculation and set
- cifs—CIFS information

- cmgr—CMGR information
- context—Context information
- cplane—CP information
- crypto—Crypto information
- ctiqbe—CTIQBE information
- ctl-provider—CTL provider debugging information
- dap—DAP information
- dcerpc—DCERPC information
- ddns—Dynamic DNS information
- dhcpc—DHCP client information
- dhcpd—DHCP server information
- dhcprelay—DHCP Relay information
- disk—Disk information
- dns—DNS information
- eap—EAP information
- eigrp—EIGRP protocol information
- email—Email information
- entity—Entity MIB information
- eou—EAPoUDP information
- esmtp—ESMTP information
- fips—FIPS 140-2 information
- fixup—Fixup information
- fover—Failover information
- fsm—FSM information
- ftp—FTP information
- generic—Miscellaneous information
- gtp—GTP information
- h323—H323 information
- http—HTTP information
- icmp—ICMP information
- igmp—Internet Group Management Protocol
- ils—LDAP information

- im—IM inspection information
- imagemgr—Image Manager information
- inspect—inspect debugging information
- integrityfw—Integrity Firewall information
- ip—IP information
- ipsec-over-tcp—IPsec over TCP information
- ipsec-pass-thru—Inspect ipsec-pass-thru information
- ipv6—IPv6 information
- iua-proxy—IUA proxy information
- kerberos—KERBEROS information
- l2tp—L2TP information
- ldap—LDAP information
- mfib—Multicast forwarding information base
- mgcp—MGCP information
- module-boot—Service module boot information
- mrib—Multicast routing information base
- nac-framework—NAC-FRAMEWORK information
- netbios-inspect—NETBIOS inspect information
- npshim—NPSHIM information
- ntdomain—NT domain information
- ntp—NTP information
- ospf—OSPF information
- p2p—P2P inspection information
- parser—Parser information
- pim—Protocol Independent Multicast
- pix—PIX information
- ppp—PPP information
- pppoe—PPPoE information
- pptp—PPTP information
- radius—RADIUS information
- redundant-interface—redundant interface information
- rip—RIP information

- rtp—RTP information
- rtsp—RTSP information
- sdi—SDI information
- sequence—Add sequence number
- session-command—Session command information
- sip—SIP information
- skinny—Skinny information
- sla—IP SLA Monitor Debug
- smtp-client—Email system log messages
- splitdns—Split DNS information
- sqlnet—SQLNET information
- ssh—SSH information
- sunrpc—SUNRPC information
- tacacs—TACACS information
- tcp—TCP for WebVPN
- tcp-map—TCP map information
- timestamps—Add timestamp
- track—static route tracking
- vlan-mapping—VLAN mapping information
- vpn-sessiondb—VPN session database information
- vpnlb—VPN load balancing information
- wccp—WCCP information
- webvpn—WebVPN information
- xdmcp—XDMCP information
- xml—XML parser information

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco TAC. Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Examples

The example disables all debugging output:

```
ciscoasa(config)# undebug all
```

Related Commands

Command	Description
debug	Displays debug information for the selected command.

unit join-acceleration

To enable accelerated cluster joining, use the **unit joint-acceleration** command in cluster configuration mode. To disable this feature, use the **no** form of this command.

unit join-acceleration
no unit join-acceleration

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

When a data node has the same configuration as the control node, it will skip syncing the configuration and will join faster. This feature is enabled by default. This feature is configured on each node, and is not replicated from the control to the data.

Note Some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the node, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** command to view incompatible configuration.

Examples

The following example disables accelerated cluster joining:

```
ciscoasa(config)# cluster cluster1
ciscoasa(cfg-cluster)# no unit join-acceleration
```

Related Commands

Command	Description
cluster	Enters cluster configuration mode

unit parallel-join

To ensure that the security modules in a Firepower 9300 chassis join the cluster simultaneously so that traffic is evenly distributed between the modules, use the **unit parallel-join** command in cluster group configuration mode. To disable parallel joining, use the **no** form of this command.

unit parallel-join *num_of_units* **max-bundle-delay** *max_delay_time*
no unit parallel-join [*num_of_units* **max-bundle-delay** *max_delay_time*]

Syntax Description

num_of_units	Specifies the minimum number of modules in the same chassis required to be ready before a module can join the cluster, between 1 and 3. The default is 1, meaning that a module will not wait for other modules to be ready before it joins the cluster. If you set the value to 3, for example, then each module will wait the *max_delay_time* or until all 3 modules are ready before joining the cluster. All 3 modules will request to join the cluster roughly simultaneously, and will all start receiving traffic around the same time.
max-bundle-delay *max_delay_time*	Specifies the maximum delay time in minutes before a module stops waiting for other modules to be ready before it joins the cluster, between 0 and 30 minutes. The default is 0, meaning the module will not wait for other modules to be ready before it joins the cluster. If you set the *num_of_units* to 1, then this value must be 0. If you set the *num_of_units* to 2 or 3, then this value must be 1 or more. This timer is per module, but when the first module joins the cluster, then all other module timers end, and the remaining modules join the cluster. For example, you set the *num_of_units* to 3, and the *max_delay_time* to 5 minutes. When module 1 comes up, it starts its 5 minute timer. Module 2 comes up 2 minutes later and starts its 5 minute timer. Module 3 comes up 1 minute later, therefore all modules will now join the cluster at the 4 minute mark; they will not wait for the timers to complete. If module 3 never comes up, then Module 1 will join the cluster at the end of its 5 minute timer, and Module 2 will also join, even though its timer still has 2 minutes remaining; it will not wait for its timer to complete.

Command Default

This feature is disabled by default.

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
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.10(1)	Command added.

Usage Guidelines

If a module joins very much in advance of other modules, it can receive more traffic than desired, because the other modules cannot yet share the load.

Examples

The following example sets the number of modules to 2, and the maximum delay time to 6 minutes:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# unit parallel-join 2 max-bundle-delay 6
```

Related Commands

Command	Description
cluster group	Enters cluster group configuration mode.

unix-auth-gid

To set the UNIX group ID, use the **unix-auth-gid** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

unix-auth-gid *identifier*
no storage-objects

Syntax Description

identifier	Specifies an integer in the range 0 through 4294967294.

Command Default

The default is 65534.

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
Group-policy webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The string specifies a network file system (NetFS) location. Only SMB and FTP protocols are supported; for example, smb://(NetFS location) or ftp://(NetFS location). You use the name of this location in the **storage-objects** command.

Examples

The following example sets the UNIX group ID to 4567:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
 unix-auth-gid 4567
```

Related Commands

Command	Description
unix-auth-uid	Sets the UNIX user ID.

unix-auth-uid

To set the UNIX user ID, use the **unix-auth-uid** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

unix-auth-gid *identifier*
no storage-objects

Syntax Description

identifier	Specifies an integer in the range 0 through 4294967294.

Command Default

The default is 65534.

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
Group-policy webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The string specifies a network file system (NetFS) location. Only SMB and FTP protocols are supported; for example, smb://(NetFS location) or ftp://(NetFS location). You use the name of this location in the **storage-objects** command.

Examples

The following example sets the UNIX user ID to 333:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
 unix-auth-gid 333
```

Related Commands

Command	Description
unix-auth-gid	Sets the UNIX group ID.

unsupported

To log Diameter elements that are not directly supported by the software, use the **unsupported** command in policy map parameters configuration mode. Use the **no** form of this command to remove the setting.

unsupported { **application-id | avp | command-code** } **action log**
no unsupported { **application-id | avp | command-code** } **action log**

Syntax Description

application-id	Log Diameter messages whose application ID is not directly supported.
avp	Log Diameter messages that contain an attribute-value pair (AVP) that is not directly supported.
command-code	Log Diameter messages that contain a command code that is not directly supported.

Command Default

The default is to allow the elements without logging them.

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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Use this command when configuring a Diameter inspection policy map.

These options specify application IDs, command codes, and AVP that are not directly supported by the software. The default is to allow the elements without logging them. You can enter the command three times to enable logging for all elements.

Examples

The following example logs all unsupported application IDs, command codes, and AVP:

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# unsupported application-id action log
ciscoasa(config-pmap-p)# unsupported command-code action log
ciscoasa(config-pmap-p)# unsupported avp action log
```

Related Commands

Commands	Description
inspect diameter	Enables Diameter inspection.
policy-map type inspect diameter	Creates a Diameter inspection policy map.

upgrade rommon

To upgrade the ASA 5506-X and ASA 5508-X series security appliances, use the **upgrade rommon** command in privileged EXEC mode.

upgrade rommon { **disk 0 | disk 1 | flash** } **:** / [**path**] **filename**

Syntax Description

disk0:/ [*path* /] *filename*	This option indicates the internal Flash memory. You can also use **flash** instead of **disk0** ; they are aliased.
disk1:/ [*path* /] *filename*	This option indicates the external Flash memory card.
flash:/ [*path* /] *filename*	This option indicates the internal Flash card; **flash** is an alias for **disk0:**

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Once you supply a filename to the command, the command verifies the file and asks you to confirm the upgrade. If you have unsaved configuration information, you are prompted to save the information before beginning the reload. If you confirm, the ASA goes to ROMMON and the upgrade procedure begins.

Examples

The following example shows how to upgrade the ASA 5506-X and ASA 5508-X series security appliances:

```
ciscoasa# upgrade rommon disk0:/kenton_rommon_1-0-19_release.SPA

Verifying file integrity of disk0:/kenton_rommon_1-0-19_release.SPA
Computed Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
                      9ef1fa4c3892f04b2e71a6b19ddb64c4

Embedded Hash   SHA2: cfd031b15f8f9cf8f24bc8f50051d369
                      8fc90ef34d86fab606755bd283d8ccd9
                      05c6da1a4b7f061cc7f1c274bdfac98a
```

```
                        9ef1fa4c3892f04b2e71a6b19ddb64c4

Digital signature successfully validated
File Name                     : disk0:/kenton_rommon_1-0-19_release.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 54232BC5
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

upload-max-size

Note The **upload-max-size** command does not work. Do not use it. However, you might see it in the running configuration, and it is available in the CLI.

To specify the maximum size allowed for an object to upload, use the **upload-max-size** command in group-policy webvpn configuration mode. To remove this object from the configuration, use the **no** version of this command.

upload-max-size*size*
no upload-max-size

Syntax Description

size	Specifies the maximum size allowed for a uploaded object. The range is 0 through 2147483647.

Command Default

The default size is 2147483647.

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
Group-policy webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Related Commands

Command	Description
post-max-size	Specifies the maximum size of an object to post.
download-max-size	Specifies the maximum size of an object to download.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

uri-non-sip

To identify the non-SIP URIs present in the Alert-Info and Call-Info header fields, use the **uri-non-sip** 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.

uri-non-sip action { **mask | log** } [**log**]
no uri-non-sip action { **mask | log** } [**log**]

Syntax Description

log	Specifies standalone or additional log in case of violation.
mask	Masks the non-SIP URIs.

Command Default

This command is disabled by default.

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
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to identify the non-SIP URIs present in the Alert-Info and Call-Info header fields in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# uri-non-sip 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.

url (crl configure) (Deprecated)

To maintain the list of static URLs for retrieving CRLs, use the **url** command in crl configure configuration mode. The crl configure configuration mode is accessible from the **crypto ca trustpoint** configuration mode. To delete an existing URL, use the **no** form of this command.

url*indexurl*
no url *index url*

Syntax Description

index	Specifies a value from 1 to 5 that determines the rank of each URL in the list. The ASA tries the URL at index 1 first.
url	Specifies the URL from which to retrieve the CRL.

Command Default

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
Crl configure configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.13(1)	This command was removed. See the **match certificate** command.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

Examples

The following example enters crl configure mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL https://example.com from which to retrieve CRLs:

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# url 3 https://example.com
ciscoasa(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
policy	Specifies the source for retrieving CRLs.

url (saml idp)

To configure the SAML IdP URL for signing in or signing out, use the **url** command in saml idp configuration mode. You can access the saml idp configuration mode by first entering the **webvpn** command. To remove the URL, use the **no** form of this command.

url { **sign-in | sign-out** } **value** *url*
no url *url*

Syntax Description

url	Specifies the URL from which to retrieve the CRL.

Command Default

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
Saml idp configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

url-block

To manage the URL buffers used for web server responses while waiting for a filtering decision from the filtering server, use the **url-block** command. To remove the configuration, use the **no** form of this command.

url-block block *block_buffer*
no url-block block *block_buffer*
url-block mempool-size *memory_pool_size*
no url-block mempool-size *memory_pool_size*
url-block url-size *long_url_size*
no url-block url-size *long_url_size*

Syntax Description

block *block_buffer*	Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks.
mempool-size *memory_pool_size*	Configures the maximum size of the URL buffer memory pool in Kilobytes (KB). The permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB.
url-size *long_url_size*	Configures the maximum allowed URL size in KB for each long URL being buffered. The permitted values, which specifies a maximum URL size,: for Websense are 2, 3, or 4, representing 2 KB, 3 KB, or 4KB; or for Secure Computing, 2 or 3, representing 2 KB or 3 KB.

Command Default

This command is disabled by default.

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	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

For Websense filtering servers, the url-block url-size command allows filtering of long URLs, up to 4 KB. For Secure Computing, the url-block url-size command allows filtering of long URLs, up to 3 KB. For both Websense and N2H2 filtering servers, the url-block block command causes the ASA to buffer packets received from a web server in response to a web client request while waiting for a response from the URL filtering server. This improves performance for the web client compared to the default ASA behavior, which is to drop the packets and to require the web server to retransmit the packets if the connection is permitted.

If you use the url-block block command and the filtering server permits the connection, the ASA sends the blocks to the web client from the HTTP response buffer and removes the blocks from the buffer. If the filtering server denies the connection, the ASA sends a deny message to the web client and removes the blocks from the HTTP response buffer.

Use the **url-block block command** to specify the number of blocks to use for buffering web server responses while waiting for a filtering decision from the filtering server.

Use the **url-block** url-size command with the url-block mempool-size command to specify the maximum length of a URL to be filtered and the maximum memory to assign to the URL buffer. Use these commands to pass URLs longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense or Secure-Computing server. The **url-block** url-size command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense or Secure-Computing server (through a TCP packet stream) so that the Websense or Secure-Computing server can grant or deny access to that URL.

Examples

The following example assigns 56 1550-byte blocks for buffering responses from the URL filtering server:

```
ciscoasa#(config)# url-block block 56
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

url-cache

To enable URL caching for URL responses received from a Websense server and to set the size of the cache, use the url-cache command in global configuration mode. To remove the configuration, use the **no** form of this command.

url-cache { **dst | src_dst** } *kbytes* [**kb**]
no url-cache { **dst | src_dst** } *kbytes* [**kb**]

Syntax Description

dst	Cache entries based on the URL destination address. Select this mode if all users share the same URL filtering policy on the Websense server.
size *kbytes*	Specifies a value for the cache size within the range 1 to 128 KB.
src_dst	Cache entries based on the both the source address initiating the URL request as well as the URL destination address. Select this mode if users do not share the same URL filtering policy on the Websense server.
statistics	Use the statistics option to display additional URL cache statistics, including the number of cache lookups and hit rate.

Command Default

This command is disabled by default.

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	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **url-cache** command provides a configuration option to cache responses from the URL server.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display cache statistics.

Note The N2H2 server application does not support this command for URL filtering.

Caching stores URL access privileges in memory on the ASA. When a host requests a connection, the ASA first looks in the URL cache for matching access privileges instead of forwarding the request to the Websense server. Disable caching with the **no url-cache** command.

Note If you change settings on the Websense server, disable the cache with the no url-cache command and then re-enable the cache with the url-cache command.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol Version 4 URL filtering while using the **url-cache** command.

Examples

The following example caches all outbound HTTP connections based on the source and destination addresses:

```
ciscoasa(config)# url-cache src_dst 128
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for URL responses received from a Websense filtering server.
url-server	Identifies a Websense server for use with the filter command.

url-entry

To enable or disable the ability to enter any HTTP/HTTPS URL on the portal page, use the **url-entry** command in dap webvpn configuration mode.

url-entry enable | enable

enable | disable	Enables or disables the ability to browse for file servers or shares.

Command Default

No default value or behaviors.

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
Dap webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example shows how to enable URL entry for the DAP record called Finance:

```
ciscoasa
 (config) config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 webvpn
ciscoasa
(config-dynamic-access-policy-record)#
 url-entry enable
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-entry	Enables or disables the ability to enter file server names to access.

url-length-limit

To configure the maximum length of the URL allowed in the RTSP message, use the **url-length-limit** 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.

url-length-limit *length*
no url-length-limit *length*

Syntax Description

length	The URL length limit in bytes. Range is 0 to 6000.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example shows how to configure the URL length limit in an RTSP inspection policy map:

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# url-length-limit 50
```

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.

url-list

To apply a list of WebVPN servers and URLs to a particular user or group policy, use the **url-list** command in group-policy webvpn configuration mode or in username webvpn configuration mode. To remove a list, including a null value created by using the **url-list none command,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a url list, use the **url-list none** command. Using the command a second time overrides the previous setting.

url-list { **value** *name* **| none** } [**index**]
no url-list

Syntax Description

index	Indicates the display priority on the home page.
none	Sets a null value for URL lists. Prevents inheriting a list from a default or specified group policy.
value *name*	Specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.

Command Default

There is no default URL list.

Command Modes

The following table shows the modes in which you enter the commands:

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Using the command a second time overrides the previous setting.

Before you can use the **url-list** command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a user or group policy, you must create the list via an XML object. Use the **import** command in global configuration mode to download a URL list to the security appliance. Then use the url-list command to apply a list to a particular group policy or user.

Examples

The following example applies a URL list called FirstGroupURLs for the group policy named FirstGroup and assigns it first place among the URL lists:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# url-list value FirstGroupURLs 1
```

Related Commands

Command	Description
clear configure url-list	Removes all url-list commands from the configuration. If you include the list name, the ASA removes only the commands for that list.
show running-configuration url-list	Displays the current set of configured **url-list** commands.
webvpn	Lets you enter webvpn mode. This can be webvpn configuration mode, group-policy webvpn configuration mode (to configure webvpn settings for a specific group policy), or username webvpn configuration mode (to configure webvpn settings for a specific user).

url-server

To identify an N2H2 or Websense server for use with the filter command, use the **url-server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

N2H2
url-server [(*if_name*)] **vendor** { **smartfilter | n2h2** } **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** { **TCP** [*connections number*] } | **UDP**]
no url-server [(*if_name*)] **vendor** { **smartfilter | n2h2** } **host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** { **TCP** [**connections** *number*] } | **UDP**]

Websense
url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** { **TCP | UDP | connections** *num_conns*] | *version*]
no url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** { **TCP | UDP** [**connections** *num_conns*] | *version*]

Syntax Description

N2H2

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.
if_name	(Optional) The network interface where the authentication server resides. If not specified, the default is inside.
port *number*	The N2H2 server port. The ASA also listens for UDP replies on this port. The default port number is 4005.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP.
timeout *seconds*	The maximum idle time permitted before the ASA switches to the next server you specified. The default is 30 seconds.
vendor	Indicates URL filtering service, using either ‘smartfilter’ or ‘n2h2’ (for backward compatibility); however, ‘smartfilter’ is saved as the vendor string.

Websense

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.

if_name	The network interface where the authentication server resides. If not specified, the default is inside.
timeout *seconds*	The maximum idle time permitted before the ASA switches to the next server you specified. The default is 30 seconds.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP protocol, Version 1.
vendor websense	Indicates URL filtering service vendor is Websense.
version	Specifies protocol Version **1** or **4**. The default is TCP protocol Version 1. TCP can be configured using Version 1 or Version 4. UDP can be configured using Version 4 only.

Command Default

This command is disabled by default.

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	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The url-server command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers in single context mode and 4 URL servers in multi mode; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the ASA does not update the configuration on the application server; this must be done separately, according to the vendor instructions.

The **url-server** command must be configured before issuing the **filter** command for HTTPS and FTP. If all URL servers are removed from the server list, then all **filter** commands related to URL filtering are also removed.

Once you designate the server, enable the URL filtering service with the **filter url** command.

Use the **show url-server statistics** command to view server statistic information including unreachable servers.

Follow these steps to filter URLs:

1. Designate the URL filtering application server with the appropriate form of the vendor-specific **url-server** command.
2. Enable URL filtering with the **filter** command.

3. (Optional) Use the **url-cache** command to enable URL caching to improve perceived response time.
4. (Optional) Enable long URL and HTTP buffering support using the **url-block** command.
5. Use the **show url-block block statistics**, **show url-cache statistics**, or the **show url-server statistics** commands to view run information.

For more information about filtering by N2H2, visit N2H2's website at:

http://www.n2h2.com

For more information about Websense filtering services, visit the following website:

http://www.websense.com/

Examples

Using N2H2, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
ciscoasa(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
ciscoasa(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP version
 4
ciscoasa(config)# filter url http 0 0 0 0
ciscoasa(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for URL responses received from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.

urgent-flag

To allow or clear the URG pointer through the TCP normalizer, use the **urgent-flag** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

urgent-flag { **allow | clear** }
no urgent-flag { **allow clear** }

Syntax Description

allow	Allows the URG pointer through the TCP normalizer.
clear	Clears the URG pointer through the TCP normalizer.

Command Default

The urgent flag and urgent offset are clear by default.

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
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **urgent-flag** command in tcp-map configuration mode to allow the urgent flag.

The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore, end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks. The default behavior is to clear the URG flag and offset.

Examples

The following example shows how to allow the urgent flag:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# urgent-flag allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 513
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
```

```
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

user

To create a user in a user group object that supports the Identity Firewall feature, use the **user** command in the user-group object configuration mode. Use the **no** form of this command to remove the user. from the object.

user [*domain_nickname* \] *user_name*
[**no**] **user** [*domain_nickname* \] *user_name*

Syntax Description

domain_nickname	(Optional) Specifies the domain in which to add the user.
user_name	Specifies the name for the user. The user name can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If the user name contains a space, you must enclose the name in quotation marks. The *user_name* argument that you specify with the **user** keyword contains an ASCII user name and does not specify an IP address.

Command Default

If you do not specify the *domain_nickname argument, the user is created in the LOCAL domain configured for the Identity Firewall feature*.

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
Object-group user configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for the Identity Firewall feature. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups. A user can belong to local user groups and user groups imported from Active Directory.

The ASA supports up to 256 user groups (including imported user groups and local user groups).

You active user group objects by including them within an access group, capture, or service policy.

Within a user group object, you can define the following object types:

- **User**—adds a single user to the object-group user. The user can be either a LOCAL user or imported user.

The name of an imported user must be the sAMAccountName, which is unique, rather than the common name (cn), which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used for imported users defined by the user object.

- User-group—adds an imported user group, which is defined by an external directory server, such as Microsoft Active Directory server, to the group-object user.

The group name of the user-group must be the sAMAccountName, which is unique, rather than the cn, which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used in the *user_group_name* argument specified with the **user-group** keyword.

Note You can add *domain_nickname**user_group_name* or *domain_nickname**user_ name* directly within a user group object without specifying them in the object first. If the *domain_nickname* is associated with a AAA server, the ASA imports the detailed nested user groups and the users defined in the external directory server, such as the Microsoft Active Directory server, to the ASA when the user object group is activated.

- **Group-object**—adds a group defined locally on the ASA to the object-group user.

Note When including an object-group within a object-group user object, the ASA does not expand the object-group in access groups even when you enable ACL optimization. The output of the **show object-group** command does not display the hit count, which is available only for regular network object-group when ACL optimization is enabled.

- **Description**—adds a description for the object-group user.

Examples

The following example shows how to use the **user** command with the **user-group object** command to add a user in a user group object for use with the Identity Firewall feature:

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

Related Commands

Command	Description
description	Adds a description to the group created with the **object-group user** command.
group-object	Adds a locally defined object group to a user object group created with the **object-group user** command for use with the Identity Firewall feature.
object-group user	Creates an user group object for the Identity Firewall feature.
user-group	Adds a user group imported from Microsoft Active Directory to the group created with the **object-group user** command.
user-identity enable	Creates the Cisco Identity Firewall instance.

user-alert

To enable broadcast of an urgent message to all clientless SSL VPN users with currently active session, use the **user-alert** command in privileged EXEC mode. To disable the message, use the **no** form of this command.

user-alert *string cancel*
no user-alert

Syntax Description

cancel	Cancels pop-up browser window launch.
string	An alpha-numeric.

Command Default

No message.

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
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

When you issue this command, end users see a pop-up browser window with the configured message. This command causes no change in the ASA configuration file.

Examples

The following example shows how to enable DAP trace debugging:

```
ciscoasa
 #
We will reboot the security appliance at 11:00 p.m. EST time. We apologize for any
inconvenience.
ciscoasa
 #
```

user-authentication

To enable user authentication, use the **user-authentication enable** command in group-policy configuration mode. To disable user authentication, use the **user-authentication disable** command. To remove the user authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel.

user-authentication { **enable | disable** }
no user-authentication

Syntax Description

disable	Disables user authentication.
enable	Enables user authentication.

Command Default

User authentication is disabled.

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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Individual users authenticate according to the order of authentication servers that you configure.

If you require user authentication on the primary ASA, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable user authentication for the group policy named "FirstGroup":

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 user-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
secure-unit-authentication	Provides additional security by requiring the VPN client to authenticate with a username and password each time the client initiates a tunnel.
user-authentication-idle-timeout	Sets an idle timeout for individual users. If there is no communication activity on a user connection in the idle timeout period, the ASA terminates the connection.

user-authentication-idle-timeout

To set an idle timeout for individual users behind hardware clients, use the **user-authentication-idle-timeout** command in group-policy configuration mode. To delete the idle timeout value, use the **no** form of this command. This option allows inheritance of an idle timeout value from another group policy. To prevent inheriting an idle timeout value, use the **user-authentication-idle-timeout none** command.

If there is no communication activity by a user behind a hardware client in the idle timeout period, the ASA terminates the connection.

user-authentication-idle-timeout { *minutes* | **none** }
no user-authentication-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the idle timeout period. The range is from 1 through 35791394 minutes
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting an user authentication idle timeout value from a default or specified group policy.

Command Default

30 minutes.

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
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The minimum is 1 minute, the default is 30 minutes, and the maximum is 10,080 minutes.

This timer terminates only the client's access through the VPN tunnel, not the VPN tunnel itself.

The idle timeout indicated in response to the **show uauth** command is always the idle timeout value of the user who authenticated the tunnel on the Cisco Easy VPN remote device.

Examples

The following example shows how to set an idle timeout value of 45 minutes for the group policy named "FirstGroup":

```
ciscoasa
(config)#
```

```
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 user-authentication-idle-timeout 45
```

Related Commands

Command	Description
user-authentication	Requires users behind hardware clients to identify themselves to the ASA before connecting.

user-group

To add a user group imported from Microsoft Active Directory to the group created with the **object-group user** command for use with the Identity Firewall feature, use the **user-group** command in the **user-group object** configuration mode. Use the **no** form of this command to remove the user group from the object.

user-group [*domain_nickname* \] *user_group_name*
[**no**] **user-group** [*domain_nickname* \] *user_group_name*

Syntax Description

domain_nickname	(Optional) Specifies the domain in which to create the user group.
user_group_name	Specifies the name for the user group. The group name can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.]. If the group name contains a space, you must enclose the name in quotation marks.

Command Default

If you do not specify the *domain_nickname argument, the user group is created in the LOCAL domain configured for the Identity Firewall feature*.

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
Object-group user configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The ASA sends an LDAP query to the Active Directory server for user groups globally defined in the Active Directory domain controller. The ASA imports these groups for the Identity Firewall feature. However, the ASA might have localized network resources that are not defined globally that require local user groups with localized security policies. Local user groups can contain nested groups and user groups that are imported from Active Directory. The ASA consolidates local and Active Directory groups. A user can belong to local user groups and user groups imported from Active Directory.

The ASA supports up to 256 user groups (including imported user groups and local user groups).

You activate user group objects by including them within an access group, capture, or service policy.

Within a user group object, you can define the following object types:

- **User**—Adds a single user to the object-group user. The user can be either a LOCAL user or imported user.

The name of an imported user must be the sAMAccountName, which is unique, rather than the common name (cn), which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used for imported users defined by the user object.

- User-group—Adds an imported user group, which is defined by an external directory server, such as Microsoft Active Directory server, to the group-object user.

The group name of the user group must be the sAMAccountName, which is unique, rather than the cn, which might not be unique. However, some Active Directory server administrators might require that the sAMAccountName and the cn be identical. In this case, the cn that the ASA displays in the output of the **show user-identity ad-group-member** command can be used in the *user_group_name* argument specified with the **user-group** keyword.

Note You can add *domain_nickname**user_group_name* or *domain_nickname**user_ name* directly within a user group object without specifying them in the object first. If the *domain_nickname* is associated with a AAA server, the ASA imports the detailed nested user groups and the users defined in the external directory server, such as the Microsoft Active Directory server, to the ASA when the user object group is activated.

- **Group-object**—Adds a group defined locally on the ASA to the object group user.

Note When including an object group within a object group user object, the ASA does not expand the object group in access groups even when you enable ACL optimization. The output of the **show object-group** command does not display the hit count, which is available only for a regular network object group when ACL optimization is enabled.

- **Description**—Adds a description for the object group user.

Examples

The following example shows how to use the **user-group** command with the **user-group object** command to add a user group in a user group object for use with the Identity Firewall feature:

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-all
ciscoasa(config-object-group user)# user CSCO\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group CSCO\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user CSCO\user3
```

Related Commands

Command	Description
description	Adds a description to the group created with the **object-group user** command.

Command	Description
group-object	Adds a locally defined object group to a user object group created with the **object-group user** command for use with the Identity Firewall feature.
object-group user	Creates a user group object for the Identity Firewall feature.
user	Adds a user to the object group created with the **object-group user** command.
user-identity enable	Creates the Cisco Identity Firewall instance.

user-identity action ad-agent-down

To set the action for the Cisco Identity Firewall instance when the Active Directory Agent is unresponsive, use the **user-identity action ad-agent-down** command in global configuration mode. To remove this action for the Identity Firewall instance, use the **no** form of this command.

user-identity action ad-agent-down disable-user-identity-rule
no user-identity action ad-agent-down disable-user-identity-rule

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is disabled.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when the AD Agent is not responding.

When the AD Agent is down and the **user-identity action ad-agent-down** command is configured, the ASA disables the user identity rules associated with the users in that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the **show user-identity user** command.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa
(config)#
user-identity action ad-agent-down disable-user-identity-rule
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity action domain-controller-down

To set the action for the Cisco Identity Firewall instance when the Active Directory domain controller is down, use the **user-identity action domain-controller-down** command in global configuration mode. To remove the action, use the **no** form of this command.

user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**
no user-identity action domain-controller-down *domain_nickname* **disable-user-identity-rule**

Syntax Description

domain_nickname	Specifies the domain name for the Identity Firewall.

Command Default

By default, this command is disabled.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when the domain is down because Active Directory domain controller is not responding.

When the domain is down and the **disable-user-identity-rule** keyword is configured, the ASA disables the user identity-IP address mapping for that domain. Additionally, the status of all user IP addresses in that domain are marked as disabled in the output displayed by the **show user-identity user** command.

Examples

The following example shows how to configure this action for the Identity Firewall:

```
ciscoasa(config)#
user-identity action domain-controller-down SAMPLE disable-user-identity-rule
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity action mac-address-mismatch

To set the action for the Cisco Identity Firewall instance when a user's MAC address is found to be inconsistent with the ASA device IP address, use the **user-identity action mac-address mismatch** command in global configuration mode. To remove the action, use the **no** form of this command.

user-identity action mac-address mismatch remove-user-ip
no user-identity action mac-address mismatch remove-user-ip

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA uses **remove-user-ip** when this command is specified.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when a user's MAC address is found to be inconsistent with the ASA device IP address currently mapped to that MAC address. The action is to disable the effect of user identity rules.

When the **user-identity action mac-address-mismatch** command is configured, the ASA removes the user identity-IP address mapping for that client.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa
(config)#
user-identity action mac-address-mismatch remove-user-ip
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity action netbios-response-fail

To set the action when a client does not respond to a NetBIOS probe for the Cisco Identity Firewall instance, use the **user-identity action netbios-response-fail** command in global configuration mode. To remove the action, use the **no** form of this command.

user-identity action netbios-response-fail remove-user-ip
no user-identity action netbios-response-fail remove-user-ip

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is disabled.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the action when a client does not respond to a NetBIOS probe. For example, the network connection might be blocked to that client or the client is not active.

When the **user-identity action remove-user-ip** command is configured, the ASA removed the user identity-IP address mapping for that client.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa
(config)#
user-identity action netbios-response-fail remove-user-ip
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent aaa-server

To define the server group of the AD Agent for the Cisco Identity Firewall instance, use the **user-identity ad-agent aaa-server** command in AAA server host configuration mode. To remove the action, use the **no** form of this command.

user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*
no user-identity user-identity ad-agent aaa-server *aaa_server_group_tag*

Syntax Description

aaa_server_group_tag	Specifies the AAA server group associated with the Identity Firewall.

Command Default

This command has no defaults.

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
Aaa server host configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

The first server defined in *aaa_server_group_tag* variable is the primary AD Agent and the second server defined is the secondary AD Agent.

The Identity Firewall supports defining only two AD Agent hosts.

When the ASA detects that the primary AD Agent is down and a secondary agent is specified, it switches to secondary AD Agent. The AAA server for the AD agent uses RADIUS as the communication protocol, and should specify the key attribute for the shared secret between the ASA and AD Agent.

Examples

The following example shows how to define the AD Agent AAA server host for the Identity Firewall:

```
ciscoasa(config-aaa-server-hostkey)#
user-identity ad-agent aaa-server adagent
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent active-user-database

To define how the ASA retrieves the user identity-IP address mapping information from the AD Agent for the Cisco Identity Firewall instance, use the **user-identity ad-agent active-user-database** command in global configuration mode. To remove the configuration, use the **no** form of this command.

user-identityuser-identity ad-agent active-user-database { **on-demand | full-download** }
no user-identityuser-identity ad-agent active-user-database { **on-demand | full-download** }

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA 5505 uses the on-demand option. The other ASA platforms use the full-download option.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Defines how the ASA retrieves the user identity-IP address mapping information from the AD Agent:

- **full-download**—Specifies that the ASA send a request to the AD Agent to download the entire IP-user mapping table when the ASA starts and then to receive incremental IP-user mapping when users log in and log out.
- **on-demand**—Specifies that the ASA retrieve the user mapping information of an IP address from the AD Agent when the ASA receives a packet that requires a new connection, and the user of its source IP address is not in the user-identity database.

By default, the ASA 5505 uses the on-demand option. The other ASA platforms use the full-download option.

Full downloads are event driven, meaning that subsequent requests to download the database, send just the updates to the user identity-IP address mapping database.

When the ASA registers a change request with the AD Agent, the AD Agent sends a new event to the ASA.

Examples

The following example shows how to configure this option for the Identity Firewall:

```
ciscoasa(config)#
user-identity ad-agent active-user-database full-download
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent hello-timer

To define the timer between the ASA and the AD Agent for the Cisco Identity Firewall instance, use the **user-identity ad-agent hello-timer** command in global configuration mode. To remove the configuration, use the **no** form of this command.

user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*
no user-identity ad-agent hello-timer seconds *seconds* **retry-times** *number*

Syntax Description

number	Specifies the number of times to retry the timer.
seconds	Specifies the length of time for the timer.

Command Default

By default, the hello timer is set to 30 seconds and 5 retries.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Defines the hello timer between the ASA and the AD Agent.

The hello timer between the ASA and the AD Agent defines how frequently the ASA exchanges hello packets. The ASA uses the hello packet to obtain ASA replication status (in-sync or out-of-sync) and domain status (up or down). If the ASA does not receive a response from the AD Agent, it resends a hello packet after the specified interval.

By default, the hello timer is set to 30 seconds and 5 retries.

Examples

The following example shows how to configure this option for the Identity Firewall:

```
ciscoasa(config)#
user-identity ad-agent hello-timer seconds 20 retry-times 3
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity ad-agent event-timestamp-check

To enable RADIUS event time stamp checking to protect the ASA from a change of authorization replay attack, use the **user-identity ad-agent event-timestamp-check** command in global configuration mode. To remove the configuration, use the **no** form of this command.

user-identity ad-agent event-timestamp-check
no user-identity ad-agent event-timestamp-check

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is disabled.

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(5)	This command was added.

Usage Guidelines

This command enables the ASA to keep track of the last event time stamp that it receives for each identifier and to discard any message if the event time stamp is at least 5 minutes older than the ASA's clock, or if its time stamp is earlier than the last event's time stamp.

For a newly booted ASA that does not have knowledge of the last event time stamp, the ASA compares the event time stamp with its own clock. If the event is at least 5 minutes older, the ASA does not accept the message.

Note We recommend that you configure the ASA, Active Directory, and Active Directory agent to synchronize their clocks among themselves using NTP.

Examples

The following example shows how to configure an event time stamp check for the Identity Firewall:

```
ciscoasa(config)#
user-identity ad-agent event-timestamp-check
```

Related Commands

Command	Description
user-identity ad-agent hello-timer	Defines the timer between the ASA and the AD Agent for the Cisco Identity Firewall instance.

user-identity default-domain

To specify the default domain for the Cisco Identity Firewall instance, use the **user-identity default-domain** command in global configuration mode. To remove the default domain, use the **no** form of this command.

user-identity default-domain *domain_NetBIOS_name*
no user-identity default-domain *domain_NetBIOS_name*

Syntax Description

domain_NetBIOS_name	Specifies the default domain for the Identity Firewall.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

For *domain_NetBIOS_name,* enter a name up to 32 characters consisting of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] except '.' and ' ' at the first character. If the domain name contains a space, enclose the entire name in quotation marks. The domain name is not case sensitive.

The default domain is used for all users and user groups when a domain has not been explicitly configured for those users or groups. When a default domain is not specified, the default domain for users and groups is LOCAL. For multiple context mode, you can set a default domain name for each context, as well as within the system execution space.

Note The default domain name you specify must match the NetBIOS domain name configured on the Active Directory domain controller. If the domain name does not match, the AD Agent will incorrectly associate the user identity-IP address mapping with the domain name that you enter when configuring the ASA. To view the NetBIOS domain name, open the Active Directory user event security log in any text editor.

The Identity Firewall uses the LOCAL domain for all locally defined user groups or locally defined users. Users logging in through a web portal (cut-through proxy) are designated as belonging to the Active Directory domain with which they authenticated. Users logging in through a VPN are designated as belonging to the LOCAL domain unless the VPN is authenticated by LDAP with Active Directory, so that the Identity Firewall can associate the users with their Active Directory domain.

Examples

The following example shows how to configure the default domain for the Identity Firewall:

```
ciscoasa(config)#
user-identity default-domain SAMPLE
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity domain

To associate the domain for the Cisco Identity Firewall instance, use the **user-identity domain** command in global configuration mode. To remove the domain association, use the **no** form of this command.

user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*
no user-identity domain *domain_nickname* **aaa-server** *aaa_server_group_tag*

Syntax Description

aaa_server_group_tag	Specifies the AAA server group associated with the Identity Firewall.
domain_nickname	Specifies the domain name for the Identity Firewall.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Associates the LDAP parameters defined for the AAA server for importing user group queries with the domain name.

For *domain_nickname,* enter a name up to 32 characters consisting of [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.] except '.' and ' ' at the first character. If the domain name contains a space, you must enclose that space character in quotation marks. The domain name is not case sensitive.

Examples

The following example shows how to associate the domain for the Identity Firewall:

```
ciscoasa(config)#
user-identity domain SAMPLE aaa-server ds
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity enable

To create the Cisco Identity Firewall instance, use the **user-identity enable** command in global configuration mode. To disable the Identity Firewall instance, use the **no** form of this command.

user-identity enable
no user-identity enable

Syntax Description

This command has no arguments or keywords.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command enables the Identity Firewall.

Examples

The following example shows how to enable the Identity Firewall:

```
ciscoasa
(config)# user-identity enable
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity inactive-user-timer

To specify the amount of time before a user is considered idle for the Cisco Identity Firewall instance, use the **user-identity inactive-user-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

user-identity inactive-user-timer minutes *minutes*
no user-identity inactive-user-timer minutes *minutes*

Syntax Description

minutes	Specifies the amount of time in minutes before a user is considered idle, meaning the ASA has not received traffic from the user's IP address for the specified amount of time.

Command Default

By default, the idle timeout is set to 60 minutes.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

When the timer expires, the user's IP address is marked as inactive and removed from the local cached user identity-IP address mapping database and the ASA no longer notifies the AD Agent about that IP address removal. Existing traffic is still allowed to pass. When this command is specified, the ASA runs an inactive timer even when the NetBIOS Logout Probe is configured.

Note The Idle Timeout option does not apply to VPN or cut-through-proxy users.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa(config)#
user-identity inactive-user-timer minutes 120
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity logout-probe

To enable NetBIOS probing for the Cisco Identity Firewall instance, use the **user-identity logout-probe** command in global configuration mode. To remove the disable probing, use the **no** form of this command.

user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]
no user-identity logout-probe netbios local-system probe-time minutes *minutes* **retry-interval seconds** *seconds* **retry-count** *times* [**user-not-needed | match-any | exact-match**]

Syntax Description

minutes	Specifies the number of minutes between probes.
seconds	Specifies the length of time for the retry interval.
times	Specifies the number of times to retry the probe.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

To minimize the NetBIOS packets, the ASA only sends a NetBIOS probe to a client when the user has been idle for more than the specified number of minutes.

Set the NetBIOS probe timer from1 to 65535 minutes and the retry interval from 1 to 256 retries. Specify the number of times to retry the probe:

- **match-any**—As long as the NetBIOS response from the client contains the user name of the user assigned to the IP address, the user identity is be considered valid. Specifying this option requires that the client enabled the Messenger service and configured a WINS server.
- **exact-match**—The user name of the user assigned to the IP address must be the only one in the NetBIOS response. Otherwise, the user identity of that IP address is considered invalid. Specifying this option requires that the client enabled the Messenger service and configured a WINS server.
- **user-not-needed**—As long as the ASA received a NetBIOS response from the client the user identity is considered valid.

The Identity Firewall only performs NetBIOS probing for those users identities that are in the active state and exist in at least one security policy. The ASA does not perform NetBIOS probing for clients where the users logged in through cut-through proxy or by using VPN.

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa(config)# user-identity logout-probe netbios local-system probe-time minutes 10
retry-interval seconds 10 retry-count 2 user-not-needed
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity monitor

For Cloud Web Security, to download the specified user or group information from the AD agent, use the user-identity monitor command in global configuration mode. To stop monitoring, use the **no** form of this command.

user-identity monitor { **user-group** [*domain-name* \\ ] *group-name* | **object-group-user** *object-group-name*
no user-identity monitor { **user-group** [*domain-name* \\ ] *group-name* | **object-group-user** *object-group-name*

Syntax Description

object-group-user *object-group-name*	Specifies an **object-group user** name. This group can include multiple groups.
user-group [*domain-name*\\]*group-name*	Specifies a group name inline. Although you specify 2 backslashes (\\) between the domain and the group, the ASA modifies the name to include only one backslash when it sends it to Cloud Web Security, to comply with Cloud Web Security notation conventions.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

When you use the Identity Firewall feature, the ASA only downloads user identity information from the AD server for users and groups included in active ACLs; the ACL must be used in a feature such as an access rule, AAA rule, service policy rule, or other feature to be considered active. Because Cloud Web Security can base its policy on user identity, you may need to download groups that are not part of an active ACL to get full Identity Firewall coverage for all your users. For example, although you can configure your Cloud Web Security service policy rule to use an ACL with users and groups, thus activating any relevant groups, it is not required; you could use an ACL based entirely on IP addresses. The user identity monitor feature lets you download group information directly from the AD Agent.

The ASA can only monitor a maximum of 512 groups, including those configured for the user identity monitor and those monitored through active ACLs.

Examples

The following example monitors the CISCO\\Engineering usergroup:

```
ciscoasa(config)# user-identity monitor user-group CISCO\\Engineering
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current HTTP connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

user-identity poll-import-user-group-timer

To specify the amount of time before the ASA queries the Active Directory server for user group information for the Cisco Identity Firewall instance, use the **user-identity poll-import-user-group-timer** command in global configuration mode. To remove the timer, use the **no** form of this command.

user-identity poll-import-user-group-timer hours *hours*
no user-identity poll-import-user-group-timer hours *hours*

Syntax Description

hours	Sets the hours for the poll timer.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Specifies the amount of time before the ASA queries the Active Directory server for user group information.

If a user is added to or deleted from to an Active Directory group, the ASA received the updated user group after import group timer runs.

By default, the poll timer is 8 hours.

To immediately update user group information, enter the **user-identity update import-user** command:

Examples

The following example shows how to configure the Identity Firewall:

```
ciscoasa(config)#
user-identity poll-import-user-group-timer hours 1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity static user

To create a new user-IP address mapping or set a user's IP address to inactive for the Cisco Identity Firewall feature, use the **user-identity static user** command in global configuration mode. To remove this configuration for the Identity Firewall, use the **no** form of this command.

user-identity static user [*domain* \] *user_name host_ip*
no user-identity static user [*domain* \] *user_name host_ip*

Syntax Description

domain	Creates a new user-IP address mapping or sets the IP address to inactive for the user in the specified domain.
host_ip	Specifies the IP address of the user for which to create a new user-IP address mapping or to set as inactive.
user_name	Specifies the user name for which to create a new user-IP address mapping or the user or sets the users IP address to inactive.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	The command was introduced.

Usage Guidelines

There are no usage guidelines for this command.

Examples

The following example shows how to create a static maping for user1.

```
ciscoasa
(config)#
user-identity static user SAMPLE\user1 192.168.1.101
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity update active-user-database

To download the entire active-user database from the Active Directory Agent, use the **user-identity update active-user-database** command in global configuration mode.

user-identity update active-user-database [**timeout minutes** *minutes*]

Syntax Description

minutes	Specifies the number of minutes for the timeout.

Command Default

The default timeout is 5 minutes.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command downloads the entire active-user database from Active Directory Agent.

This command starts the update operation, generates a starting update log and returns immediately. When the update operation finishes or is aborted at timer expiration, another syslog message is generated. Only one outstanding update operation is allowed. Rerunning the command displays an error message.

When the command finishes running, the ASA displays [Done] at the command prompt then generates a syslog message.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa# user-identity update active-user-database
ERROR: one update active-user-database operation is already in progress
[Done] user-identity update active-user-database
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity update import-user

To download the entire active user database from the Active Directory Agent, use the **user-identity update active-user-database** command in global configuration mode.

user-identity update import-user [[*domain_nickname* \\] *user_group_name* [**timeout seconds** *seconds*]]

Syntax Description

domain_nickname	Specifies the domain of the group to update.
seconds	Specifies the number of seconds for the timeout.
user_group_name	When *user_group_name* is specified, only the specified import-user group is updated. Only activated groups (for example, groups in an access group, access list, capture, or service policy) can be updated. If the given group is not activated, this command rejects the operation. If the specified group has multiple levels of hierarchies, recursive LDAP queries are conducted. If *user_group_name* is not specified, the ASA starts the LDAP update service immediately and tries to periodically update all activated groups.

Command Default

The ASA retries the update up to 5 times and generates warning messages as necessary.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

This command updates the specified import user group database by querying the Active Directory server immediately without waiting for the expiration of the poll import user group timer. There is no command to update the local user group, because the group ID database is updated whenever the local user group has a configuration change.

This command does not block the console to wait for the return of the LDAP query.

This command starts the update operation, generates a starting update log and returns immediately. When the update operation finishes or is aborted at timer expiration, another syslog message is generated. Only one outstanding update operation is allowed. Rerunning the command displays an error message.

If the LDAP query is successful, the ASA stores retrieved user data in the local database and changes the user/group association accordingly. If the update operation is successful, you can run the **show user-identity user-of-group** *domain\\group* command to list all stored users under this group.

The ASA checks after each update for all imported groups. If an activated Active Directory group does not exist in Active Directory, the ASA generates a syslog message.

If *user_group_name* is not specified, the ASA starts the LDAP update service immediately and tries to periodically update all activated groups. The LDAP update service runs in the background and periodically updates import user groups via an LDAP query on the Active Directory server.

At system boot up time, if there are import user groups defined in access groups, the ASA retrieves user/group data via LDAP queries. If errors occur during the update, the ASA retries the update up to 5 times and generates warning messages as necessary.

When the command finishes running, the ASA displays [Done] at the command prompt then generates a syslog message.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa# user-identity update import-user group.sample-group1
ERROR: Update import-user group is already in progress
[Done] user-identity update import-user group.sample-group1
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-identity user-not-found

To enable user-not-found tracking for the Cisco Identity Firewall instance, use the **user-identity user-not-found** command in global configuration mode. To remove this tracking for the Identity Firewall instance, use the **no** form of this command.

user-identity user-not-found enable
no user-identity user-not-found enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is disabled.

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	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Only the last 1024 IP addresses are tracked.

Examples

The following example shows how to enable this action for the Identity Firewall:

```
ciscoasa
(config)#
user-identity user-not-found enable
```

Related Commands

Command	Description
clear configure user-identity	Clears the configuration for the Identity Firewall feature.

user-message

To specify a text message to display when a DAP record is selected, use the user-message command in dynamic-access-policy-record mode. To remove this message, use the **no** version of the command. If you use the command more than once for the same DAP record, the newer message replaces the previous message.

user-message *message*
no user-message

Syntax Description

message	The message for users assigned to this DAP record. Maximum 128 characters. If the message contains spaces, enclose it in double quotation marks.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Dynamic-access-policy-record	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

For a successful SSL VPN connection, the portal page displays a flashing, clickable icon that lets the user see the message(s) associated with the connection. If the connection is terminated from a DAP policy (action = terminate), and if there is a user message configured in that DAP record, then that message displays on the login screen.

If more than one DAP record applies to a connection, the ASA combines the applicable user messages and displays them as a single string.

Examples

The following example shows how to set a user message of "Hello Money Managers" for the DAP record called Finance.

```
ciscoasa
 (config) config-dynamic-access-policy-record
Finance
ciscoasa
(config-dynamic-access-policy-record)#
 user-message "Hello Money Managers"
ciscoasa
(config-dynamic-access-policy-record)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
show running-config dynamic-access-policy-record [*name*]	Displays the running configuration for all DAP records, or for the named DAP record.

user-parameter

To specify the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication, use the **user-parameter** command in aaa-server-host configuration mode.

user-parameter *name*

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 name of the username parameter included in the HTTP POST request. The maximum name size is 128 characters.

Command Default

There is no default value or behavior.

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
Aaa-server-host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

This is an SSO with HTTP Forms command. The WebVPN server of the ASA uses an HTTP POST request to submit a single sign-on authentication request to an SSO server. The required command **user-parameter** specifies that the HTTP POST request must include a username parameter for SSO authentication.

Note At login, the user enters the actual name value which is entered into the HTTP POST request and passed on to the authenticating web server.

Examples

The following example, entered in aaa-server-host configuration mode, specifies that the username parameter userid be included in the HTTP POST request used for SSO authentication:

```
ciscoasa(config)# aaa-server testgrp1 host example.com
```

```
ciscoasa(config-aaa-server-host)# user-parameter userid
ciscoasa(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.
start-url	Specifies the URL at which to retrieve a pre-login cookie.

user-statistics

To activate the collection of user statistics by MPF and match lookup actions for the Identify Firewall, use the **user-statistics** command in policy-map configuration mode. To remove collection of user statistics, use the **no** form of this command.

user-statistics [**accounting | scanning**]
no user-statistics [**accounting | scanning**]

Syntax Description

accounting	(Optional) Specifies that the ASA collect the sent packet count, sent drop count, and received packet count.
scanning	(Optional) Specifies that the ASA collect only the sent drop count.

Command Default

By default, this command is disabled.

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
Policy-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

When you configure a policy map to collect user statistics, the ASA collects detailed statistics for selected users. When you specify the **user-statistics** command without the **accounting** or **scanning** keywords, the ASA collects both accounting and scanning statistics.

Examples

The following example shows how to activate user statistics for the Identity Firewall:

```
ciscoasa
(config)#
class-map c-identity-example-1
ciscoasa
(config-cmap)#
match access-list identity-example-1
ciscoasa
(config-cmap)#
exit
ciscoasa
(config)#
policy-map p-identity-example-1
```

```
ciscoasa
(config-pmap)#
class c-identity-example-1
ciscoasa
(config-pmap)#
user-statistics accounting
ciscoasa
(config-pmap)#
exit
ciscoasa
(config)#
service-policy p-identity-example-1 interface outside
```

Related Commands

Command	Description
policy-map	Assigns actions to traffic that you identified with a Layer 3/4 class map when using the Modular Policy Framework.
service-policy(**global**)	Activates a policy map globally on all interfaces or on a targeted interface.
show service-policy [**user-statistics**]	Displays user statistics for configured service policies when you enable user-statistics scanning or accounting for the Identity Firewall.
show user-identity ip-of-user [**detail**]	Displays received packets, sent packets, and drops statistics for the IP address for a specified user when you enable user statistics scanning or accounting for the Identity Firewall.
show user-identity user active [**detail**]	Displays received packets, sent packets and drops statistics in the specified time period for active users when you enable user statistics scanning or accounting for the Identity Firewall.
show user-identity user-of-ip [**detail**]	Displays received packets, sent packets, and drops statistics for the user for a specified IP address when you enable user statistics scanning or accounting for the Identity Firewall.
user-identity enable	Creates the Identity Firewall instance.

user-storage

To store personalized user information between clientless SSL VPN sessions, use the **user storage** command in group-policy webvpn configuration mode. To disable user storage, use the **no** form of the command.

user-storage *NETFS-location*
no user-storage

Syntax Description

NETFS-location	Specifies a file system desination in the form proto://user:password@host:port/path If the username and password are embedded in the NETFS-location then the password input is treated as clear.

Command Default

User storage is disabled.

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
Group-policy webvpn mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.4(6)	Prevented the password being shown in clear text during show-run.

Usage Guidelines

User-storage enables you to store cached credentials and cookies at a location other than the ASA flash. This command provides single sign on for personal bookmarks of a clientless SSL VPN user. The user credentials are stored in an encrypted format on the FTP/CIFS/SMB server as a <user_id>.cps file that is not decryptable.

Although the username, password, and preshared key are shown in the configuration, this poses no security risk because the ASA stores this information in encrypted form, using an internal algorithm.

If data is encrypted on an external FTP or SMB server, you can define personal bookmarks within the portal page by selecting add bookmark (for example: user-storage cifs://jdoe:test@10.130.60.49/SharedDocs). You can create personalized URLs for all plugin protocols as well.

Note If you have a cluster of ASAs that all refer to the same FTP/CIFS/SMB server and use the same “storage-key,” you can access the bookmarks through any of the ASAs in the cluster.

Examples

The following example shows how to set user storage for a user called newuser with a password of 12345678 at a file share called anyshare, and a path of anyfiler02a/new_share:

```
ciscoasa
(config)#
wgroup-policy DFLTGrpPolicy attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa
(config-group-webvpn)#
 user-storage cifs://newuser:12345678@anyfiler02a/new_share
ciscoasa(config-group_webvpn)#
```

Related Commands

Command	Description
storage-key	Specifies a storage key to protect the data stored between sessions.
storage-objects	Configures storage objects for the data stored between sessions.

username

To add a user to the ASA local database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username that you want to remove.

username *name* [**password** *password* [**pbkdf2 | mschap | encrypted | nt-encrypted**] **| nopassword**] [**privilege** *priv_level*]
no username *name* [**password** *password* [**pbkdf2 | mschap | encrypted | nt-encrypted**] **| nopassword**] [**privilege** *priv_level*]

Syntax Description

encrypted	For 9.6 and earlier, indicates that the password is encrypted (if you did not specify **mschap**) for passwords 32 characters and fewer. When you define a password in the **username** command, the ASA creates an MD5 hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **encrypted** keword. For example, if you enter the password "test," the **show running-config** command output would appear to be something like the following: `username pat password rvEdRh0xPC8bel7s encrypted` The only time you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password. In 9.7 and later, passwords of all lengths use PBKDF2.
mschap	Specifies that the password will be converted to Unicode and hashed using MD4 after you enter it. Use this keyword if users are authenticated using MSCHAPv1 or MSCHAPv2.
name	Specifies the name of the user as a string from 3 to 64 characters in length, using any combination of ASCII printable characters with the exception of spaces and the question mark.
nopassword	Indicates that *any* password can be entered for this user. This is an insecure configuration, so use this keyword with caution. (9.6(2) and later) To create a username without a password, do not enter the **password** or **nopassword** keywords. For example the **ssh authentication** command allows you to install a public key on the ASA and use a private key with your SSH client, so you may not want any password configured.

nt-encrypted	Indicates that the password is encrypted for use with MSCHAPv1 or MSCHAPv2. If you specified the **mschap** keyword when you added the user, then this keyword is displayed instead of the **encrypted** keyword when you view the configuration using the **show running-config** command. When you define a password in the **username** command, the ASA encrypts it when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **nt-encrypted** keyword. For example, if you enter the password "test," the **show running-config** display would appear to be something like the following: `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` The only time you would actually enter the **nt-encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password.

password *password*	Sets the password as a case-sensitive string of 8 to 127 alphanumeric and special characters. You can use any character in the password with the following exceptions:
	
	• No spaces
	• No question marks
	• You cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected:
	  • **abc**user1
	  • user**543**
	  • user**aaaa**
	  • user2**666**

pbkdf2	Indicates that the password is encrypted. For 9.6 and earlier, the PBKDF2 (Password-Based Key Derivation Function 2) hash is used only when the password is more than 32 characters in length. In 9.7 and later, all passwords use PBKDF2. When you define a password in the **username** command, the ASA creates a PBKDF2 hash when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **pbkdf2** keyword. For example, if you enter a long password, the **show running-config** command output would appear to be something like the following: `username pat password rvEdRh0xPC8bel7s pbkdf2` The only time you would actually enter the **pbkdf2** keyword at the CLI is if you are cutting and pasting a configuration to another ASA and you are using the same password. Note that already existing passwords continue to use the MD5-based hash unless you enter a new password.
privilege *priv_level*	Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization.

Command Default

The default privilege level is 2.

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	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0.1	This command was added.
7.2(1)	The **mschap** and **nt-encrypted** keywords were added.
9.6(1)	The password length was increased to 127 characters, and the **pbkdf2** keyword was added.
9.6(2)	You can now create a username without the **password** or **nopassword** keywords.
9.7(1)	Passwords of all lengths are now saved to the configuration using the PBKDF2 hash.
9.17(1)	The minumum password length was changed from 3 to 8 characters. Also you cannot use three or more consecutive sequential or repetitive ASCII characters. For example, the following passwords will be rejected: • **abc**user1 • user**543** • user**aaaa** • user2**666**

Usage Guidelines

The **login** command uses this database for authentication.

If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. (See the **aaa authorization command** command.) Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use AAA authentication so the user will not be able to use the **login** command, or you can set all local users to level 1 so you can control who can use the **enable** password to access privileged EXEC mode.

By default, VPN users that you add with this command have no attributes or group policy association. You must configure all values explicitly using the **username attributes** command.

When password authentication policy is enabled, you can no longer change your own password or delete your own account with the **username** command. You can, however, change your password with the **change-password** command.

To display the username password date, use the **show running-config all username** command.

Examples

The following example shows how to configure a user named “anyuser” with a password of 12345678 and a privilege level of 12:

```
ciscoasa
(config)#
 username anyuser password 12345678 privilege 12
```

Related Commands

Command	Description
aaa authorization command	Configues command authorization.
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure attributes for specific users.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

username attributes

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure attribute-value pairs for a specified user.

username *name***attributes**
no username *name* **attributes**

Syntax Description

name Provides the name of the user.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Username configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **service-type** attribute was added.
9.1(2)	The **ssh authentication** {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]} attribute was added.

Usage Guidelines

The internal user authentication database consists of the users entered with the **username** command. The **login** command uses this database for authentication. You can configure the username attributes using either the **username** command or the **username attributes** command.

The command syntax in username configuration mode has the following characteristics in common:

- The **no** form removes the attribute from the running configuration.
- The **none** keyword also removes the attribute from the running configuration. But it does so by setting the attribute to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

The **username attributes** command enters username attributes mode, in which you can configure any of the following attributes:

Attribute	Function
group-lock	Names an existing tunnel group with which the user is required to connect.
password-storage	Enables or disables storage of the login password on the client system.
service-type [**remote-access** | **admin** | **nas-prompt**]	Restricts console login and enables login for users who are assigned the appropriate level. The **remote-access** option specifies basic AAA services for remote access. The **admin** option specifies AAA services, login console privileges, EXEC mode privileges, the enable privilege, and CLI privileges. The **nas-prompt** option specifies AAA services, login console privileges, EXEC mode privileges, but no enable privileges.
ssh authentication {**pkf** [**nointeractive**] | **publickey** *key* [**hashed**]}	Enables public key authentication on a per-user basis. The value of the *key* argument can refer to the following: • When the *key* argument is supplied and the hashed tag is not specified, the value of the key must be a base64 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 base64 encoded public key, that key is then hashed via SHA-256 and the corresponding 32-byte hash is used for all further comparisons. • 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). The **pkf** option enables you to authenticate using 4096-bit RSA keys as an SSH public key file (PKF). This option is not restricted to 4096-bit RSA keys, but can be used for any size less than or equal to 4096-bit RSA keys. The nointeractive option suppresses all prompts when importing an SSH public key formatted key. This noninteractive data entry mode is only intended for ASDM use. 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. **Note** You can use the PKF option when failover is enabled, but the PKF data is not automatically replicated to the standby system. You must enter the **write standby** command to synchronize the PKF setting to the standby system in the failover pair.
vpn-access-hours	Specifies the name of a configured time-range policy.
vpn-filter	Specifies the name of a user-specific ACL.
vpn-framed-ip-address	Specifies the IP address and the netmask to be assigned to the client.
vpn-group-policy	Specifies the name of a group policy from which to inherit attributes.
vpn-idle-timeout [**alert-interval**]	Specifies the idle timeout period in minutes, or **none** to disable it. Optionally specifies a pre-timeout alert interval.

Attribute	Function
vpn-session-timeout [**alert-interval**]	Specifies the maximum user connection time in minutes, or **none** for unlimited time. Optionally specifies a pre-timeout alert interval.
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed.
vpn-tunnel-protocol	Specifies permitted tunneling protocols.
webvpn	Enters username webvpn configuration mode, in which you configure WebVPN attributes.

You configure webvpn-mode attributes for the username by entering the **username attributes** command and then entering the **webvpn** command in username webvpn configuration mode. See the **webvpn** command (group-policy attributes and username attributes modes) for details.

Examples

The following example shows how to enter username attributes configuration mode for a user named "anyuser":

```
ciscoasa
(config)#
 username anyuser attributes
ciscoasa
(config-username)#
```

Related Commands

Command	Description
clear config username	Clears the username database.
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the ASA database.
webvpn	Enters webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

username-from-certificate

To specify the field in a certificate to use as the username for authorization, use the **username-from-certificate** command in tunnel-group general-attributes mode. The DN of the peer certificate used as username for authorization

To remove the attribute from the configuration and restore default values, use the **no** form of this command.

username-from-certificate { *primary-attr* [*secondary-attr*] | **use-entire-name** }
no username-from-certificate

Syntax Description

primary-attr	Specifies the attribute to use to derive a username for an authorization query from a certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a username for an authentication or authorization query from a digital certificate. If pre-fill-username is enable, the derived name can also be used in an authentication query.
use-entire-name	Specifies that the ASA must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.
use-script	Specifies the use of a script file generated by ASDM to extract the DN fields from a certificate for use as a username.

Command Default

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

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
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

This command selects the field in the certificate to use as the username. It replaces the deprecated **authorization-dn-attributes** command in Release 8.0(4) and following. The **username-from-certificate** command forces the security appliance to use the specified certificate field as the username for username/password authorization.

To use this derived username in the pre-fill username from certificate feature for username/passwordauthentication or authorization, you must also configure the **pre-fill-username** command in tunnel-group webvpn-attributes mode. That is, to use the pre-fill username feature, you must configure both commands.

Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.
use-entire-name	Use entire DN name. Not available as a secondary attribute.
use-script	Use a script file generated by ASDM.

Note When multiple DN attributes are configured in a certificate, ASA extracts the username from the last subject DN attribute.

Examples

The following example, entered in global configuration mode, creates an IPsec remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute and OU as the secondary attribute to use to derive a name for an authorization query from a digital certificate:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN OU
ciscoasa(config-tunnel-general)#
```

The following example shows how to modify the tunnel-group attributes to configure the pre-fill username.

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
 secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

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-choice

To select the certificate from where the username should be used for pre-fill username field for primary authentication or authorization, use the **username-from-certificate-choice** command. Use this command in tunnel-group general-attributes mode. To use the username from the default certificate, use the **no** form of the command.

username-from-certificate-choice { **first-certificate | second-certificate** }
no username-from-certificate-choice { **first-certificate | second-certificate** }

Syntax Description

first-certificate	Specifies if the username from the machine certificate sent in SSL or IKE to be used in pre-fill username field for primary authentication.
second-certificate	Specifies if the username from the user certificate from client to be used in pre-fill username field for peimary authentication.

Command Default

The username for prefill is retrieved from the second certificate by default.

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	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The multiple certificates option allows certificate authentication of both the machine and user via certificates. The pre-fill username field allows a field from the certificates to be parsed and used for subsequent (primary and secondary) AAA authentication in a AAA and certificate authenticated connection. The username for prefill is always retrieved from the second (user) certificate received from the client.

Beginning with 9.14(1), ASA allows you to choose whether the first certificate (machine certificate) or second certificate (user certificate) should be used to derive the username for the pre-fill username field.

This command is available and can be configured for any tunnel groups irrespective of the authentication type (aaa, certificate, or multiple-certificate). However, the configuration takes effect only for Multiple Certificate Authentication (multiple-certificate or aaa multiple-certificate). When the option is not used for Multiple Certificate Authentication, the second certificate is used by default for authentication or authorization purpose.

Examples

The following example shows how to configure the certificate to be used for prefill username for primary and secondary authentication or authorization:

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>

ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice first-certificate
ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

Related Commands

Command	Description
secondary-username-from-certificate-choice	Specify the certificate option for secondary authentication.

username password-date

To enable the system to restore a password creation date at boot time or when copying a file to the running configuration, enter the **username pasword-date** command in non-interactive configuration mode; in other words, this command is only available when booting up a configuration file with this command already present; you cannot enter this command at the CLI prompt.

username *name* **password-date** *date*

Syntax Description

name	Specifies the name of the user as a string from 3 to 64 characters in length, using any combination of ASCII printable characters with the exception of spaces and the question mark.
date	Enables the system to restore password creation dates for usernames, which are read in during bootup. If not present, the password date is set to the current date. The date is in the format, mmm-dd-yyyy.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Non-interactive	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

To display the username password date, use the **show running-config all username** command.

You cannot enter **username password-date** values from a CLI prompt. The password date is saved to the startup configuration only if the password policy lifetime is not zero. This means that password dates are saved only if password expiration is configured. You cannot use the **username password-date** command to prevent users from changing password creation dates.

Related Commands

Command	Description
aaa authorization command	Configues command authorization.
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure attributes for specific users.

Command	Description
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

username-prompt

To customize the username prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **username-prompt** command from webvpn customization mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

username-prompt { **text | style** } *value*
[**no**] **username-prompt** { **text | style** } *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Command Default

The default is text of the username prompt is "USERNAME:".

The default style of the username prompt is color:black;font-weight:bold;text-align:right.

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
Webvpn customization	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the text is changed to "Corporate Username:", and the default style is changed with the font weight increased to bolder:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# username-prompt text Corporate Username:
ciscoasa(config-webvpn-custom)# username-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page.
password-prompt	Customizes the password prompt of the WebVPN page.