



upgrade-mp through write terminal Commands

upgrade-mp

To upgrade the maintenance partition software, use the **upgrade-mp** command.

```
upgrade-mp {http[s]:// user password@server port}/pathname | tftp // }
```

Syntax Description

	Specifies a TFTP server. If you do not specify the server and path, you are prompted for the information. See the tftp-server command to configure a default TFTP server.
http[s]	Specifies an HTTP(S) server.
	Specifies the HTTP(S) or TFTP server IP address.
	Specifies the pathname and filename of the software image.
	(Optional) Specifies the HTTP(S) username.
	(Optional) Specifies the user password.
	(Optional) Specifies the HTTP(S) port.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example shows how to download an image from a TFTP server:

```
hostname# upgrade-mp tftp://10.192.1.1/c6svc-mp.2-1-1.bin.gz
```

copy	Copies a file to Flash memory.
-------------	--------------------------------

url

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**

url index url

index url

Specifies a value from 1 to 5 that determines the rank of each URL in the list. The FWSM tries the URL at index 1 first.

Specifies the URL from which to retrieve the CRL.

No default behaviors or values.

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

CRL configure configuration					—

3.1(1)	This command was introduced.
--------	------------------------------

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` configuration 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:

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

crl configure	Enters ca-crl configuration mode.
	Enters trustpoint configuration mode.
	Specifies the source for retrieving CRLs.

url-block

url-block

no

url-block block *block_buffer_limit*

block_buffer_limit

Websense only:

memory_pool_size

memory_pool_siz

block_buffer_limit

mode, the permitted values are from 0 to 128, which specifies the number of 1550-byte blocks. In multiple context mode, the permitted values are from 0 to 16.

For Websense URL filtering only. The size of the URL buffer memory pool in Kilobytes (KB). In single context mode, the permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB. In multiple context mode, the permitted values are from 0 to 512.

url-size *long_url_size*

Global configuration

1.1(1)

This command was introduced.

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 FWSM 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-cache` command and the filtering server permits the connection, the FWSM 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 FWSM sends a deny message to the web client and removes the blocks from the HTTP response buffer.

Use the `url-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-cache` command with the `url-block` command to specify the maximum length of a URL to be filtered by a Websense filtering server 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 server. The `url-cache` command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense server (through a TCP packet stream) so that the Websense server can grant or deny access to that URL.

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

```
url-block block 56
```

```
Directs traffic to a URL filtering server.
```

```
show url-block
```

```
url-cache
```

```
url-server
```

```
filter
```

url-cache

```
{ | src_dst [kb]
no url-cache dst src_dst [kb]
```

dst

kb

kb

src_dst

statistics

statistics

url-cache

url-cache

no url-cache



Note

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 that 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 and for N2H2 URL filtering while using the `url-cache` command.

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

```
url-cache src_dst 128
```

url-server

N2H2

() vendor n2h2 host port timeout protocol TCP
UDP connections

no url-server () vendor n2h2 host port timeout protocol
TCP UDP connections

url-server () vendor websense host timeout protocol TCP UDP
connections

no url-server () vendor websense host timeout protocol TCP UDP
connections

N2H2

connections

host

port

protocol TCP UDP

timeout

vendor n2h2

Websense

connections

host

timeout

protocol TCP UDP



<http://www.websense.com/>

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

```
url-server (perimeter) host 10.0.1.1 protocol TCP version 4
filter url http 0 0 0 0
filter url except 10.0.2.54 255.255.255.255 0 0
```

user-authentication

enable | disable

no user-authentication

Syntax Description

Defaults

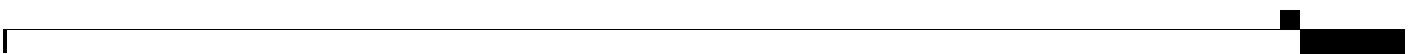
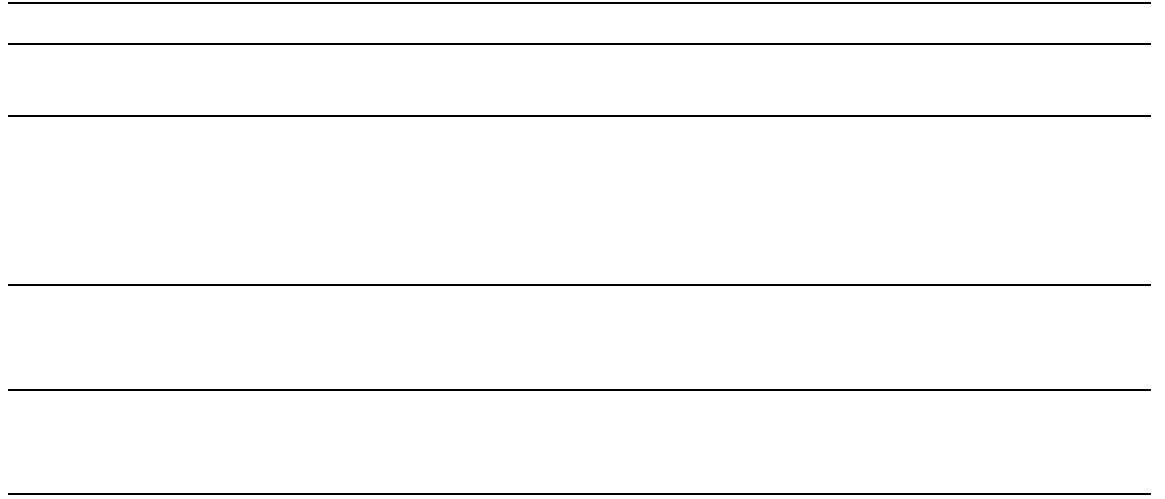
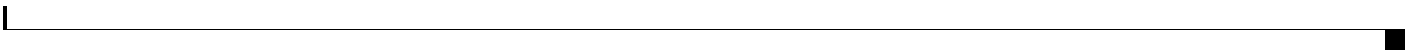
Command Modes

Command History

Usage Guidelines

Examples

```
“FirstGroup”:  
    # group-policy FirstGroup attributes  
    (config-group-policy)#
```



from 1 through 35791394 minutes

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.

Group-policy		—		—	—

3.1(1) This command was introduced.

```
hostname(config)#  
hostname(config-group-policy)#
```

Requires users behind hardware clients to identify themselves to the FWSM before connecting.

To add a user to the FWSM database, enter the `username` command in global configuration mode. To remove a user, use the `no username` version of this command with the username you want to remove. To remove all usernames, use the `no usernames` version of this command without appending a username.

```
username {username} {password} [encrypted] [privilege]
no username {username}
no usernames
```

Indicates that the password is encrypted. When you define a password in the `username` command, the FWSM encrypts it when it saves it to the configuration for security purposes. When you enter the `show username` command, the `show username` command does not show the actual password; it shows the encrypted password followed by the keyword. For example, if you enter the password “test,” the display would appear to be something like the following:

```
username pat password rvEdRh0xPC8bel7s encrypted
```

The default privilege level is 2.

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

Mode	Command	Privilege	Configuration
Global	<code>username</code>	15	Yes
Configuration	<code>username</code>	15	Yes
Privileged EXEC	<code>show username</code>	12	No
Configuration	<code>show username</code>	15	Yes

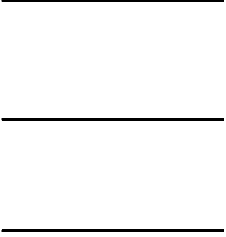
The `username` command uses this database for authentication.

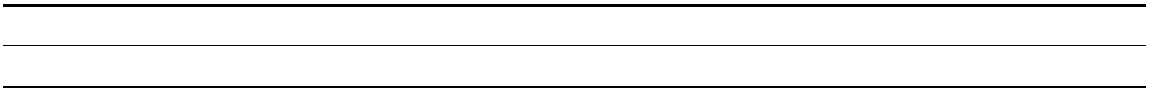
command.) Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use AAA authentication so the user will not be able to use the `enable` command, or 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` command.

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

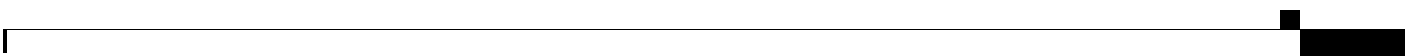
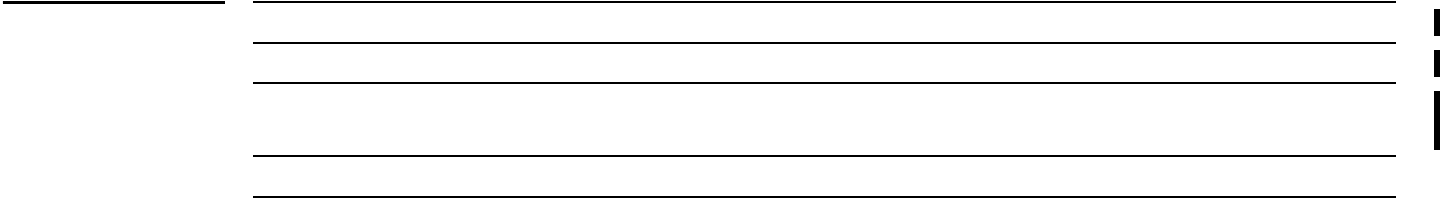
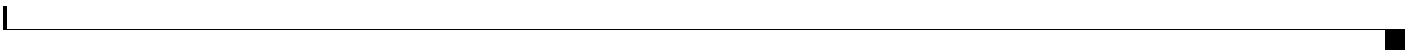
```
hostname(config)# username anyuser password 12345678 privilege 12
```





username anyuser attributes





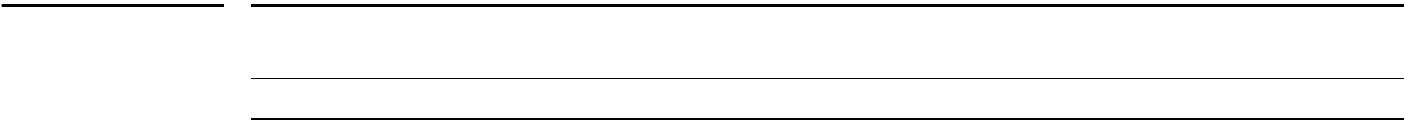
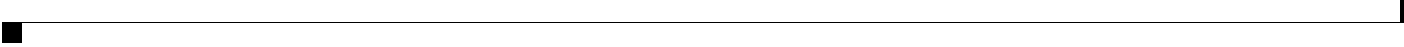


Caution

Examples

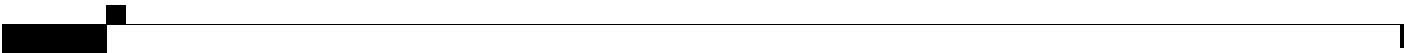
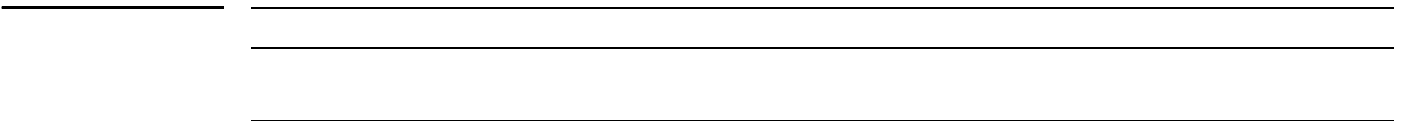
```
access-list HTTP-ACL extended permit tcp 10.1.1.0 any eq 80
aaa authentication match HTTP-ACL inside tacacs+
virtual http 10.1.2.1
```

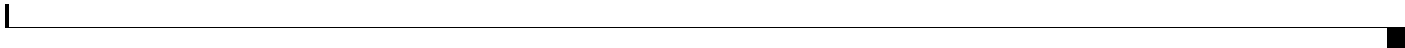
```
access-list AUTH extended permit tcp 10.1.1.0 host 10.1.2.1 eq telnet
access-list AUTH extended permit tcp 10.1.1.0 host 209.165.200.225 eq
smtp
aaa authentication match AUTH inside tacacs+
virtual telnet 10.1.2.1
```



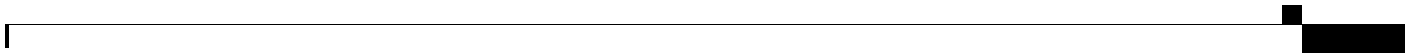


group-policy FirstGroup attributes
vpn-access-hours 824





vpn-addr-assign dhcp







vpn-filter

Syntax Description

Indicates that there is no access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
Provides the name of the previously configured access list.

Defaults

Command Modes

Group-policy					—
Username					—

Command History

3.1(1) This command was introduced.

Usage Guidelines

Examples

The following example shows how to set a filter that invokes an access list named `acl_vpn` for the group policy named `FirstGroup`:

Creates an access list.

To specify the IP address to assign to a particular user, use the `username ip` command in username mode. To remove the IP address, use the `username no ip` form of this command.

```
username ip { ip-address }
```

Provides the IP address for this user.

No default behavior or values.

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

Username					

3.1(1) Support for this command was introduced.

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

Provides the subnet mask for this user.

To specify the subnet mask to assign to a particular user, use the `username subnetmask` command in username mode. To remove the subnet mask, use the `username no subnetmask` form of this command.

```
username username subnetmask ip-address mask
```

Provides the subnet mask for this user.

No default behavior or values.

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

	Global Configuration Mode		User Configuration Mode	
	Configurable	Supported	Configurable	Supported
Username attributes configuration				—

3.1(1) Support for this command was introduced.

The following example shows how to set a subnet mask of 255.255.255. 254 for a user named anyuser:

Provides the IP address for this user.

vpn-group-policy

Syntax Description

Defaults

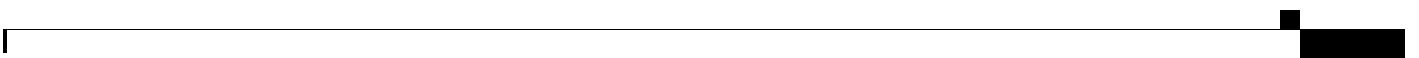
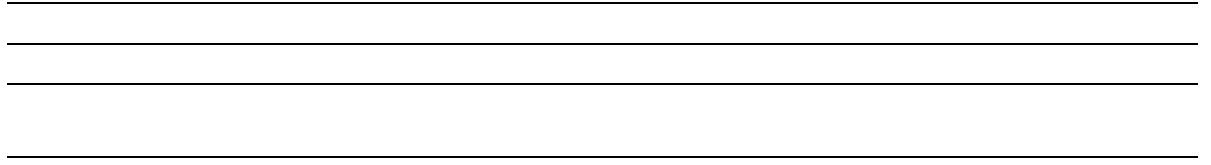
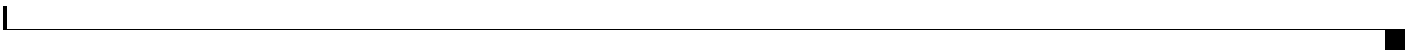
Command Modes

Command History

Usage Guidelines

Examples

`irstGroup`



| none}

no vpn-idle-timeout

none

group-policy FirstGroup attributes
vpn-idle-timeout 30

group-policy

vpn-session-timeout

vpn-sessiondb logoff

vpn-sessiondb logoff remote | l2l | email-proxy | protocol protocol-name | username
IPaddr groupname indexnumber

indexnumber

IPaddr

username

protocol-name

groupname

vpn-sessiondb logoff protocol IPSec

vpn-sessiondb max-session-limit

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification

Usage Guidelines

Examples



vpn-session-timeout

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification

Examples

Related Commands

■ vpn-session-timeout

vpn-simultaneous-logins

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification

Usage Guidelines

Examples

vpn-tunnel-protocol

vpn-tunnel-protocol IPSec

no vpn-tunnel-protocol [IPSec]

IPSec

webvpn

who

Syntax Description

Defaults

Command Modes

Command History

Usage Guidelines

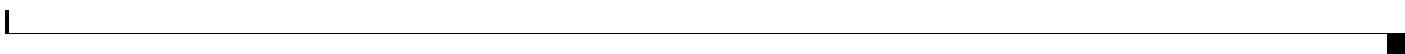
Examples

```
0: 100.0.0.2
hostname#
0: 100.0.0.2
hostname#
```

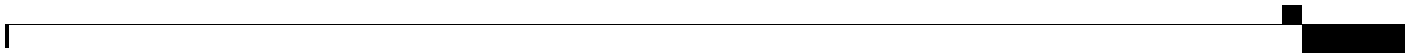


hostname(config)#
hostname(config-group-policy)#





hostname#
Erase configuration in flash memory? [confirm]





'Saving context 'b' ... (1/3 contexts saved) '

The context 'context a' could not be saved due to Unavailability of resources



The context 'context a' could not be saved due to non-reachability of destination

Unable to save the configuration for the following contexts as these contexts are locked.
context 'a' , context 'x' , context 'z' .

Unable to save the configuration for the following contexts as these contexts have read-only config-urls:
context 'a' , context 'b' , context 'c' .

The context 'context a' could not be saved due to Unknown errors

```
hostname#  
Building configuration...  
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454  
  
19319 bytes copied in 3.570 secs (6439 bytes/sec)  
[OK]  
hostname#
```





hostname#
hostname#

hostname#

hostname#
hostname#

Horizontal line

Horizontal line

Horizontal line

Horizontal line

Two horizontal lines

Horizontal line



Two horizontal lines

```
hostname#  
Building configuration...  
[OK]  
hostname#
```

```
hostname#
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

