



# Configuring Security Contexts

---

This chapter describes how to configure multiple security contexts, and includes the following sections:

- [Security Context Overview, page 4-1](#)
- [Enabling or Disabling Multiple Context Mode, page 4-9](#)
- [Configuring Resource Management, page 4-11](#)
- [Configuring Memory Partitions, page 4-16](#)
- [Configuring a Security Context, page 4-18](#)
- [Changing Between Contexts and the System Execution Space, page 4-22](#)
- [Managing Security Contexts, page 4-23](#)

## Security Context Overview

You can partition a single FWSM into multiple virtual devices, known as security contexts. Each context has its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, and management. Some features are not supported, including dynamic routing protocols.

This section provides an overview of security contexts, and includes the following topics:

- [Common Uses for Security Contexts, page 4-1](#)
- [Unsupported Features, page 4-2](#)
- [Context Configuration Files, page 4-2](#)
- [How the FWSM Classifies Packets, page 4-3](#)
- [Sharing Interfaces Between Contexts, page 4-6](#)
- [Management Access to Security Contexts, page 4-9](#)

## Common Uses for Security Contexts

You might want to use multiple security contexts in the following situations:

- You are a service provider and want to sell security services to many customers. By enabling multiple security contexts on the FWSM, you can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.

- You are a large enterprise or a college campus and want to keep departments completely separate.
- You are an enterprise that wants to provide distinct security policies to different departments.
- You have any network that requires more than one firewall.

## Unsupported Features

Multiple context mode does not support the following features:

- Dynamic routing protocols  
Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.
- Multicast

## Context Configuration Files

This section describes how the FWSM implements multiple context mode configurations and includes the following sections:

- [Context Configurations, page 4-2](#)
- [System Configuration, page 4-2](#)
- [Admin Context Configuration, page 4-2](#)

## Context Configurations

The FWSM includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. You can store context configurations on the internal Flash memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

## System Configuration

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the FWSM. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the *admin context*. The system configuration does include a specialized failover interface for failover traffic only.

## Admin Context Configuration

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users. The admin context must reside on Flash memory, and not remotely.

If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called `admin.cfg`. This context is named “admin.” If you do not want to use `admin.cfg` as the admin context, you can change the admin context.

## How the FWSM Classifies Packets

Each packet that enters the FWSM must be classified, so that the FWSM can determine to which context to send a packet. The FWSM uses only one global MAC address across all interfaces. A single MAC address is usually not a problem unless multiple contexts want to share an interface. A router cannot direct packets to IP addresses on the same network if all IP addresses resolve to the same MAC address. Moreover, the bridging table of the switch would constantly change as the MAC address moves from one interface to another. The purpose of the security context classifier is to resolve this situation.

This section includes the following topics:

- [Valid Classifier Criteria, page 4-3](#)
- [Invalid Classifier Criteria, page 4-4](#)
- [Classification Examples, page 4-4](#)

### Valid Classifier Criteria

If only one context is associated with the ingress interface, the FWSM classifies the packet into that context. In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

If multiple contexts share an interface, then the classifier intercepts the packet and performs a destination IP address lookup. All other fields are ignored; only the destination IP address is used. To use the destination address for classification, the classifier must have knowledge about the subnets located behind each security context. The classifier relies on active NAT sessions to determine the subnets in each context. Active NAT sessions are created either by **static** commands, which create a permanent session, or by active dynamic NAT sessions.

For example, the classifier gains knowledge about subnets 10.10.10.0, 10.20.10.0 and 10.30.10.0 when the context administrators configure **static** commands in each context:

- Context A:

```
static (inside,shared) 10.10.10.0 10.10.10.0 netmask 255.255.255.0
```

- Context B:

```
static (inside,shared) 10.20.10.0 10.20.10.0 netmask 255.255.255.0
```

- Context C:

```
static (inside,shared) 10.30.10.0 10.30.10.0 netmask 255.255.255.0
```

If you use dynamic NAT, an active NAT session is created when the real host creates a connection through the shared interface. For traffic returning to the host, the active NAT session is used to classify the packet.

To quickly identify possible overlaps between different contexts, a situation that leads to connectivity problems, enter the **show np 3 static** command in the system execution space.

**Note**

---

For management traffic destined for an interface, the interface IP address is used for classification.

---

## Invalid Classifier Criteria

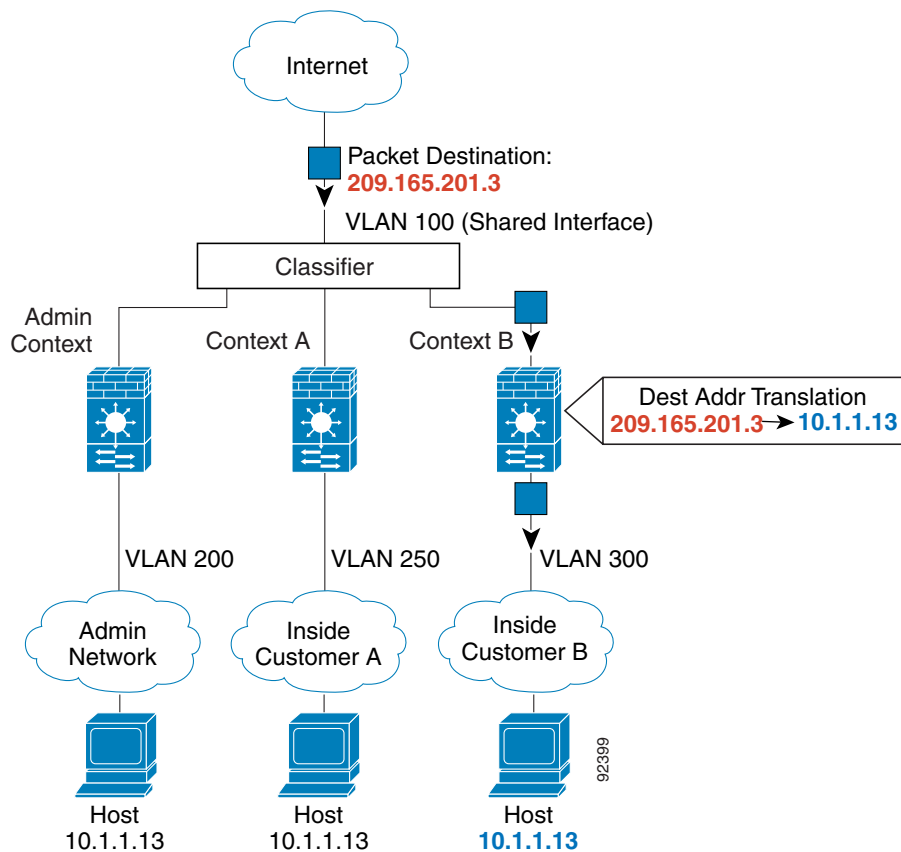
The following configurations are not used for packet classification:

- NAT exemption—The classifier does not use a NAT exemption configuration for classification purposes because NAT exemption does not identify the mapped (shared) interface.
- Routing table—The classifier does not use the routing table for classification. For example, if a context includes a static route that points to an external router as the next-hop to a subnet, and a different context includes a **static** command for the same subnet, then the classifier uses the **static** command to classify packets destined for that subnet and ignores the static route.

## Classification Examples

Figure 4-1 shows multiple contexts sharing an outside interface, while the inside interfaces are unique, allowing overlapping IP addresses. The classifier assigns the packet to Context B because Context B includes the address translation that matches the destination address.

**Figure 4-1** Packet Classification with a Shared Interface



Note that all new incoming traffic must be classified, even from inside networks. [Figure 4-2](#) shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is VLAN 300, which is assigned to Context B.

**Figure 4-2** Incoming Traffic from Inside Networks

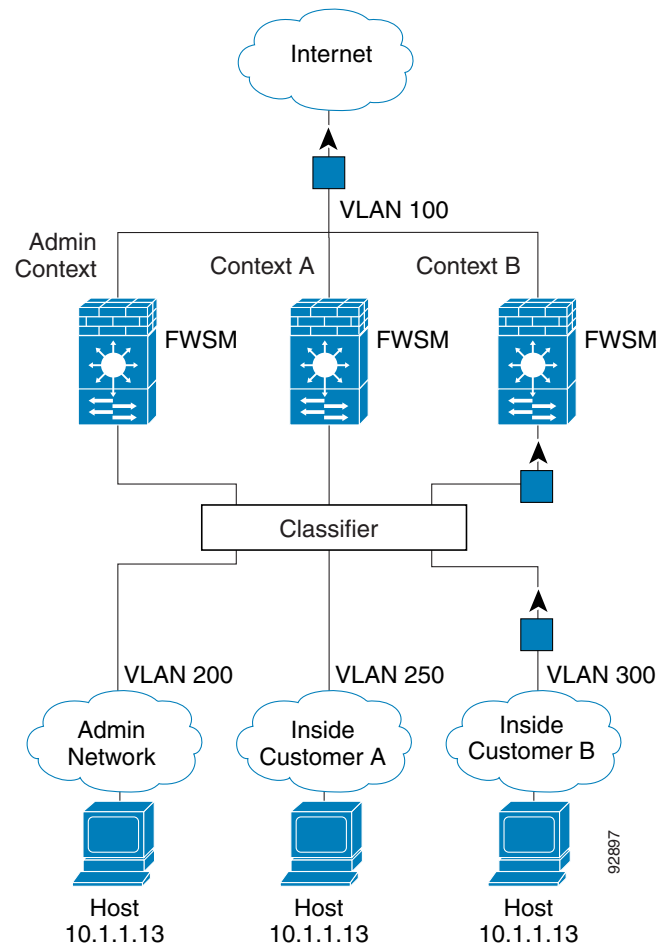
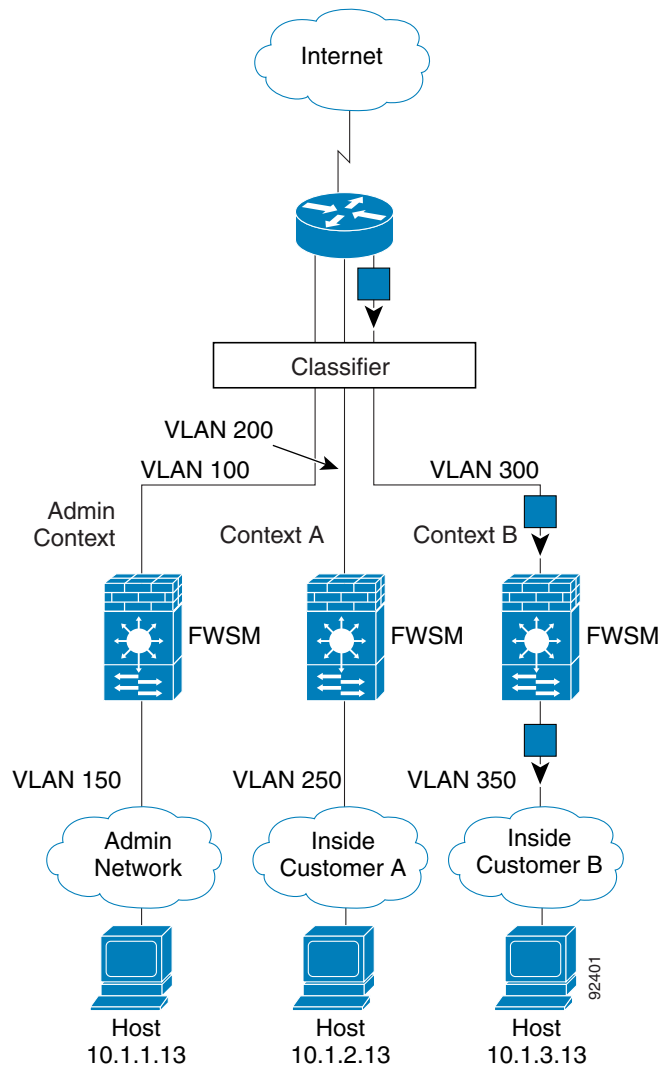


Figure 4-3 shows a transparent firewall with a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is VLAN 300, which is assigned to Context B.

**Figure 4-3** Transparent Firewall Contexts



## Sharing Interfaces Between Contexts

### Routed Mode Only

The FWSM lets you share an interface between contexts. However, packet classification requirements might make sharing interfaces impractical. Because the classifier relies on active NAT sessions to classify the destination addresses to a context, the classifier is limited by how you can configure NAT. If you do not want to perform NAT, you must use unique interfaces.

**Note**

The FWSM does not support sharing the outside interface of one context with the inside interface of another context (known as cascading contexts). Traffic that is outbound from one context (from a higher to a lower security interface) can only enter another context as inbound traffic (lower to higher security); it cannot be outbound for both contexts, or inbound for both contexts.

This section includes the following topics:

- [NAT and Origination of Traffic, page 4-7](#)
- [Sharing an Outside Interface, page 4-7](#)
- [Sharing an Inside Interface, page 4-7](#)

## NAT and Origination of Traffic

The type of NAT configured determines whether the traffic can originate on the shared interface or if it can only respond to an existing connection. When you use dynamic NAT, you cannot initiate a connection to the real addresses. Therefore, traffic from the shared interface must be in response to an existing connection. Static NAT, however, lets you initiate connections, so you can initiate connections on the shared interface.

## Sharing an Outside Interface

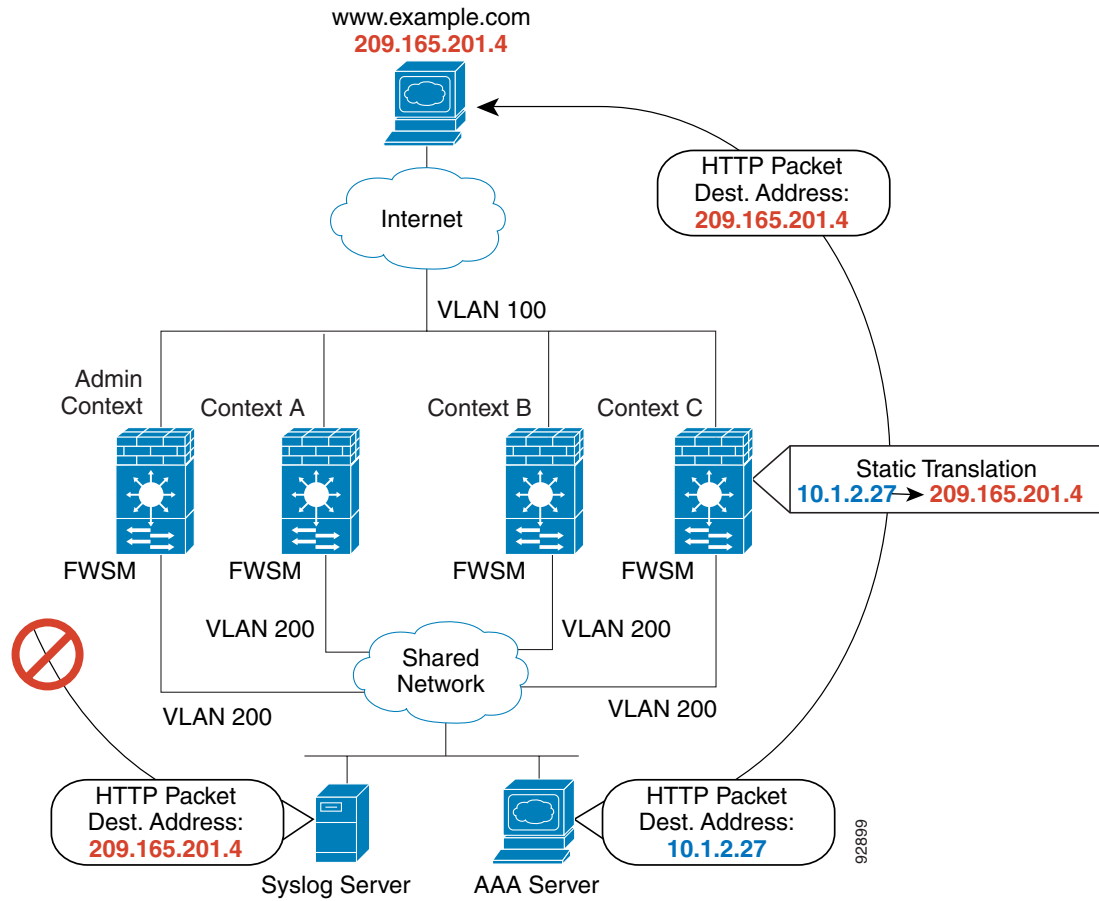
When you have an outside shared interface (connected to the Internet, for example), the destination addresses on the inside are limited, and are known by the system administrator, so configuring NAT for those addresses is easy, even if you want to configure static NAT.

## Sharing an Inside Interface

Configuring an inside shared interface poses a problem, however, if you want to allow communication between the shared interface and the Internet, where the destination addresses are unlimited. For example, if you want to allow inside hosts on the shared interface to initiate traffic to the Internet, then you need to configure static NAT statements for each Internet address. This requirement necessarily limits the kind of Internet access you can provide for users on an inside shared interface. (If you intend to statically translate addresses for Internet servers, then you also need to consider DNS entry addresses and how NAT affects them. For example, if a server sends a packet to `www.example.com`, then the DNS server needs to return the translated address. Your NAT configuration determines DNS entry management.)

Figure 4-4 shows two servers on an inside shared interface. One server sends a packet to the translated address of a web server, and the FWSM classifies the packet to go through Context C because it includes a static translation for the address. The other server sends the packet to the real untranslated address, and the packet is dropped because the FWSM cannot classify it.

Figure 4-4 Originating Traffic on a Shared Interface



## Management Access to Security Contexts

The FWSM provides system administrator access in multiple context mode as well as access for individual context administrators. The following sections describe logging in as a system administrator or as a context administrator:

- [System Administrator Access, page 4-9](#)
- [Context Administrator Access, page 4-9](#)

### System Administrator Access

You can access the FWSM as a system administrator in two ways:

- Session to the FWSM from the switch.  
From the switch, you access the system execution space.
- Access the admin context using Telnet, SSH, or ASDM.  
See [Chapter 21, “Configuring Management Access,”](#) to enable Telnet, SSH, and SDM access.

As the system administrator, you can access all contexts.

When you change to a context from admin or the system, your username changes to the default “enable\_15” username. If you configured command authorization in that context, you need to either configure authorization privileges for the “enable\_15” user, or you can log in as a different name for which you provide sufficient privileges in the command authorization configuration for the context. To log in with a username, enter the **login** command. For example, you log in to the admin context with the username “admin.” The admin context does not have any command authorization configuration, but all other contexts include command authorization. For convenience, each context configuration includes a user “admin” with maximum privileges. When you change from the admin context to context A, your username is altered, so you must log in again as “admin” by entering the **login** command. When you change to context B, you must again enter the **login** command to log in as “admin.”

The system execution space does not support any AAA commands, but you can configure its own enable password, as well as usernames in the local database to provide individual logins.

### Context Administrator Access

You can access a context using Telnet, SSH, or ASDM. If you log in to a non-admin context, you can only access the configuration for that context. You can provide individual logins to the context. See [Chapter 21, “Configuring Management Access,”](#) to enable Telnet, SSH, and SDM access and to configure management authentication.

## Enabling or Disabling Multiple Context Mode

Your FWSM might already be configured for multiple security contexts depending on how you ordered it from Cisco. If you are upgrading, however, you might need to convert from single mode to multiple mode by following the procedures in this section. ASDM does not support changing modes, so you need to change modes using the CLI.

This section includes the following topics:

- [Backing Up the Single Mode Configuration, page 4-10](#)
- [Enabling Multiple Context Mode, page 4-10](#)

- [Restoring Single Context Mode, page 4-10](#)

## Backing Up the Single Mode Configuration

When you convert from single mode to multiple mode, the FWSM converts the running configuration into two files. The original startup configuration is not saved, so if it differs from the running configuration, you should back it up before proceeding.

## Enabling Multiple Context Mode

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the FWSM converts the running configuration into two files: a new startup configuration that comprises the system configuration, and `admin.cfg` that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as `old_running.cfg` (in the root directory of the internal Flash memory). The original startup configuration is not saved. The FWSM automatically adds an entry for the admin context to the system configuration with the name “admin.”

To enable multiple mode, enter the following command:

```
hostname(config)# mode multiple
```

You are prompted to reboot the FWSM.

## Restoring Single Context Mode

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the FWSM; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device. For example, you can restore the old single-mode running configuration, if available, as the startup configuration. Because the system configuration does not have any network interfaces as part of its configuration, you must access the FWSM from a switch session to perform the copy.

To copy the old running configuration to the startup configuration and to change the mode to single mode, perform the following steps in the system execution space:

- 
- Step 1** To copy the backup version of your original running configuration to the current startup configuration, enter the following command in the system execution space:

```
hostname(config)# copy old_running.cfg startup-config
```

- Step 2** To set the mode to single mode, enter the following command in the system execution space:

```
hostname(config)# mode single
```

The FWSM reboots.

---

# Configuring Resource Management

By default, all security contexts have unlimited access to the resources of the FWSM, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context.

**Note**

---

The FWSM does not limit the bandwidth per context; however, the switch containing the FWSM can limit bandwidth per VLAN. See the switch documentation for more information.

---

This section includes the following topics:

- [Classes and Class Members Overview, page 4-11](#)
- [Configuring a Class, page 4-14](#)

## Classes and Class Members Overview

The FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class. This section includes the following topics:

- [Resource Limits, page 4-11](#)
- [Default Class, page 4-12](#)
- [Class Members, page 4-13](#)

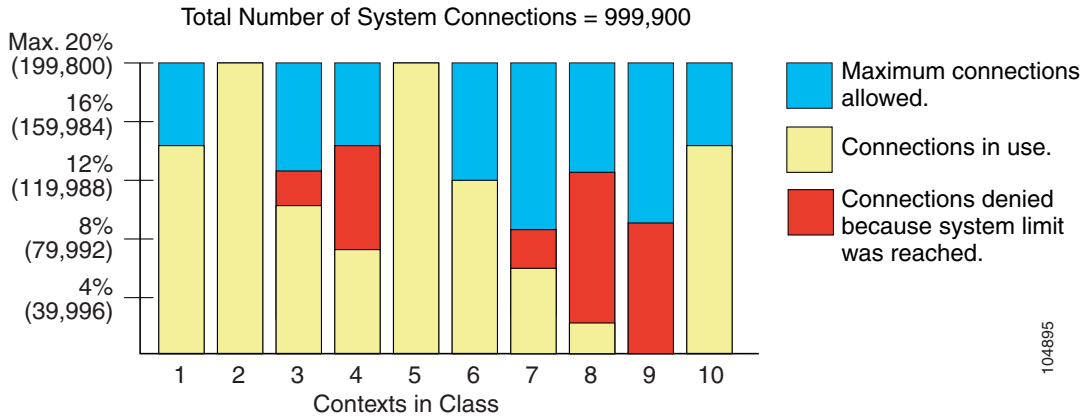
## Resource Limits

When you create a class, the FWSM does not set aside a portion of the resources for each context assigned to the class; rather, the FWSM sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can “use up” those resources, potentially affecting service to other contexts.

You can set the limit for all resources together as a percentage of the total available for the device. Also, you can set the limit for individual resources as a percentage or as an absolute value.

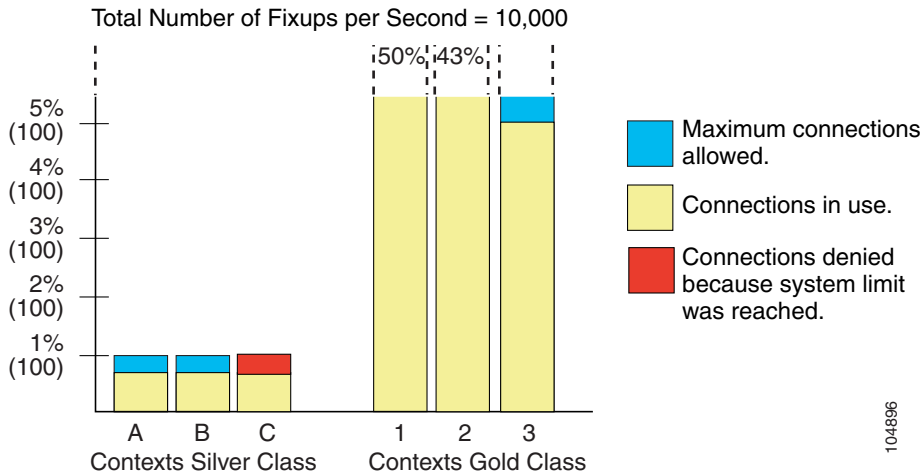
You can oversubscribe the FWSM by assigning more than 100 percent of the resources across all contexts. For example, you can set the Bronze class to limit connections to 20 percent per context, and then assign 10 contexts to the class for a total of 200 percent. If contexts concurrently use more than the system limit, then each context gets less than the 20 percent you intended. (See [Figure 4-5](#).)

Figure 4-5 Resource Oversubscription



The FWSM lets you assign unlimited access to one or more resources in a class, instead of a percentage or absolute number. When a resource is unlimited, contexts can use as much of the resource as the system has available. For example, Context A, B, and C are in the Silver Class, which limits each class member to 1 percent of the system inspections per second, for a total of 3 percent; but the three contexts are currently only using 2 percent combined. Gold Class has unlimited access to inspections. The contexts in the Gold Class can use more than the 97 percent of “unassigned” inspections; they can also use the 1 percent of inspections not currently in use by Context A, B, and C, even if that means that Context A, B, and C are unable to reach their 3 percent combined limit. (See Figure 4-6.) Setting unlimited access is similar to oversubscribing the FWSM, except that you have less control over how much you oversubscribe the system.

Figure 4-6 Unlimited Resources



## Default Class

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

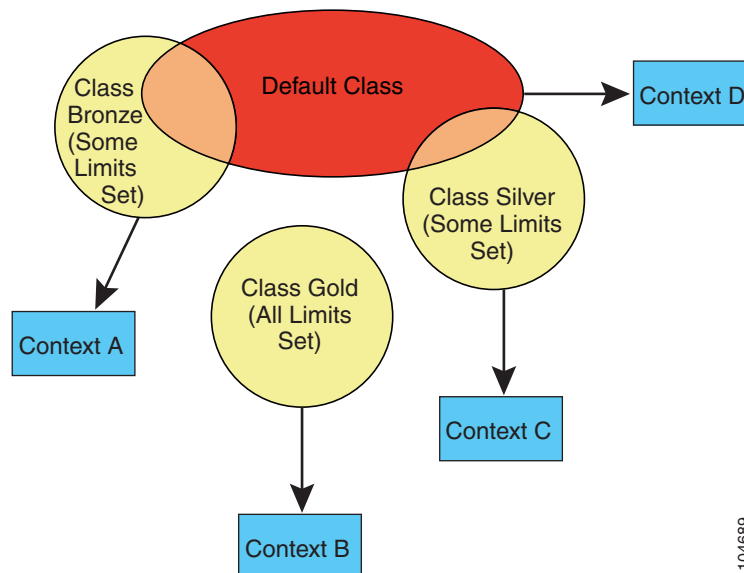
If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 2 percent limit for all concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with a 2 percent limit for *all* resources, the class uses no settings from the default class.

By default, the default class provides unlimited access to resources for all contexts, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- IPsec sessions—5 sessions.
- MAC addresses—65,535 entries.

Figure 4-7 shows the relationship between the default class and other classes. Contexts A and C belong to classes with some limits set; other limits are inherited from the default class. Context B inherits no limits from default because all limits are set in its class, the Gold class. Context D was not assigned to a class, and is by default a member of the default class.

**Figure 4-7 Resource Classes**



## Class Members

To use the settings of a class, assign the context to the class when you define the context. All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to default. You can only assign a context to one resource class. The exception to this rule is that limits that are undefined in the member class are inherited from the default class; so in effect, a context could be a member of default plus another class.

## Configuring a Class

To configure a class in the system configuration, perform the following steps. You can change the value of a particular resource limit by reentering the command with a new value.

- Step 1** To specify the class name and enter the class configuration mode, enter the following command in the system execution space:

```
hostname(config)# class name
```

The *name* is a string up to 20 characters long. To set the limits for the default class, enter **default** for the name.

- Step 2** To set the resource limits, see the following options:

- To set all resource limits (shown in [Table 4-1](#)), enter the following command:

```
hostname(config-resmgt)# limit-resource all {number% | 0}
```

The *number* is an integer greater than or equal to 1. **0** (without a percent sign (%)) sets the resources to the system limit. You can assign more than 100 percent if you want to oversubscribe the device.

- To set a particular resource limit, enter the following command:

```
hostname(config-resmgt)# limit-resource [rate] resource_name number[%]
```

For this particular resource, the limit overrides the limit set for **all**. Enter the **rate** argument to set the rate per second for certain resources. See [Table 4-1](#) for resources for which you can set the rate per second.

[Table 4-1](#) lists the resource types and the limits. See also the **show resource types** command.

**Table 4-1 Resource Names and Limits**

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
mac-addresses	N/A	65,535 concurrent	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.

Table 4-1 Resource Names and Limits (continued)

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
conns	N/A	999,900 concurrent 102,400 per second (rate)	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.  <b>Note</b> For concurrent connections, the FWSM allocates half of the limit to each of two network processors that accept connections. Typically, the connections are divided evenly between the NPs. However, in some circumstances, the connections are not evenly divided, and you might reach the maximum connection limit on one NP before reaching the maximum on the other. In this case, the maximum connections allowed is less than the limit you set. The NP distribution is controlled by the switch based on an algorithm. You can adjust this algorithm on the switch, or you can adjust the connection limit upward to account for the inequity.
fixups	N/A	10,000 per second (rate)	Application inspection.
hosts	N/A	262,144 concurrent	Hosts that can connect through the FWSM.
ipsec	1 minimum 5 maximum concurrent	10 concurrent	IPSec sessions.
asdm	1 minimum 5 maximum concurrent	80 concurrent	ASDM management sessions.  <b>Note</b> ASDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 80 ASDM sessions represents a limit of 160 HTTPS sessions.
ssh	1 minimum 5 maximum concurrent	100 concurrent	SSH sessions.
syslogs	N/A	30,000 per second (rate)	System log messages.  <b>Note</b> The FWSM can support 30,000 messages per second for messages sent to the FWSM terminal or buffer. If you send messages to a syslog server, the FWSM supports 25,000 per second.
telnet	1 minimum 5 maximum concurrent	100 concurrent	Telnet sessions.

Table 4-1 Resource Names and Limits (continued)

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
xlates	N/A	266,144 concurrent	Address translations.

For example, to set the default class limit for conns to 10 percent instead of unlimited, enter the following commands:

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold with all resources set to 5 percent, except for fixups, with a setting of 10 percent, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource all 5%
hostname(config-class)# limit-resource fixups 10%
```

To add a class called silver with all resources set to 3 percent, except for syslogs, with a setting of 500 per second, enter the following commands:

```
hostname(config)# class silver
hostname(config-class)# limit-resource all 3%
hostname(config-class)# limit-resource rate syslogs 500
```

## Configuring Memory Partitions

In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. By default, a context belongs to one of 12 partitions that offers a maximum of 12,130 rules, including ACEs, AAA rules, and others. The FWSM assigns contexts to the partitions in the order they are loaded at startup. For example, if you have 12 contexts, each context is assigned to its own partition, and can use 12,130 rules. If you add one more context, then context number 1 and the new context number 13 are both assigned to partition 1, and can use 12,130 rules divided between them; the other 11 contexts continue to use 12,130 rules each. If you delete contexts, the partition membership does not shift, so you might have some unequal distribution until you reboot, at which time the contexts are evenly distributed.



### Note

Rules are used up on a first come, first served basis, so one context might use more rules than another context.

See the [“Rule Limits” section on page A-5](#) for more information about rule limits.

Alternatively, you can manually assign a context to a partition. To assign a context to a partition, see the [“Configuring a Security Context” section on page 4-18](#). You can also reduce the number of partitions to better match the number of contexts you have.



### Note

Changing the number of partitions requires you to reload the FWSM.

To change the number of memory partitions, perform the following steps:

---

**Step 1** To set the number of partitions, enter the following command in the system execution space:

```
hostname(config)# resource acl-partition number_of_partitions
```

Where *number\_of\_partitions* is between 1 and 12.



**Note** If you assign a context to a partition, the partition numbering starts with 0. So if you have 12 partitions, the partition numbers are 0 through 11. See the [“Configuring a Security Context” section on page 4-18](#) to assign contexts to partitions.

---

If you later enter the **clear configure all** command to restore the default configuration, the **resource acl-partition** command is not changed back to the default. You must enter the **no resource acl-partition** command to restore the default for this command.

---

You see the following message:

```
WARNING: This command leads to re-partitioning of ACL Memory.  
It will not take affect until you save the configuration and reboot.
```

**Step 2** To reload the FWSM, enter the following command:

```
hostname(config)# reload
```

If you are using failover, wait a few seconds before reloading the standby unit as well; the standby unit does not reload automatically, and the memory partitions must match on both units. Traffic loss can occur because both units are down at the same time.

---

The following example shows how to verify the current mapping of contexts to memory partitions:

```
hostname(config)# show resource acl-partition
Total number of configured partitions = 2
Partition #0
  Mode                               :exclusive
  List of Contexts                    :bandn, borders
  Number of contexts                  :2(RefCount:2)
  Number of rules                     :0(Max:53087)
Partition #1
  Mode                               :non-exclusive
  List of Contexts                    :admin, momandpopA, momandpopB, momandpopC
                                      momandpopD
  Number of contexts                  :5(RefCount:5)
  Number of rules                     :6(Max:53087)
```

For information about exclusive and non-exclusive partitions, see the [“Configuring a Security Context” section on page 4-18](#).

## Configuring a Security Context

The security context definition in the system configuration identifies the context name, configuration file URL, interfaces that a context can use, and other context parameters.



### Note

To assign a context to a failover group for active/active failover, see the [“Using Active/Active Failover” section on page 13-23](#).

If you do not have an admin context (for example, if you clear the configuration) then you must first specify the admin context name by entering the following command:

```
hostname(config)# admin-context name
```

Although this context name does not yet exist in your configuration, you can subsequently enter the **context name** command to match the specified name to continue the admin context configuration.

To configure a context in the system configuration, perform the following steps:

**Step 1** To configure a context, enter the following command in the system execution space:

```
hostname(config)# context name
```

The *name* is a string up to 32 characters long. This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen.

“System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.

**Step 2** (Optional) To add a description for this context, enter the following command:

```
hostname(config-ctx)# description text
```

**Step 3** To specify the interfaces you can use in the context, enter the following command:

```
hostname(config-ctx)# allocate-interface vlnumber[-vlnumber] [map_name[-map_name]
[invisible | visible]]
```

You can enter this command multiple times to specify different ranges. If you remove an allocation with the **no** form of this command, then any context commands that include this interface are removed from the running configuration.

Enter a VLAN number or a range of VLANs, typically from 2 to 1000 and from 1025 to 4094 (see the switch documentation for supported VLANs). To see a list of VLANs assigned to the FWSM, use the **show vlan** command. You can allocate a VLAN that is not yet assigned to the FWSM, but you need to assign them from the switch if you want them to pass traffic. When you allocate an interface, the FWSM automatically adds the **interface** command for each VLAN in the system configuration.

You can assign the same VLANs to multiple contexts in routed mode, if desired. See the “[Sharing Interfaces Between Contexts](#)” section on page 4-6 for more information about shared VLAN limitations.

The *map\_name* is an alphanumeric alias for the interface that can be used within the context instead of the VLAN ID. If you do not specify a mapped name, the VLAN ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context.

A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names:

```
int0
```

```
inta
```

```
int_0
```

If you specify a range of VLAN IDs, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range:

```
int0-int10
```

- The numeric portion of the mapped name must include the same quantity of numbers as the **vlanx-vlany** statement. For example, both ranges include 100 interfaces:

```
vlan100-vlan199 int1-int100
```

If you enter **vlan100-vlan199 int1-int15** or **vlan100-vlan199 happy1-sad5**, for example, the command fails.

If you set a mapped name, specify **visible** to see the VLAN ID in addition to the mapped name in the **show interface** command. The default **invisible** keyword specifies to only show the mapped name.

The following example shows VLANs 100, 200, and 300 through 305 assigned to the context. The mapped names are int1 through int8.

```
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan200 int2
hostname(config-ctx)# allocate-interface vlan300-vlan305 int3-int8
```

**Step 4** To identify the URL from which the system downloads the context configuration, enter the following command:

```
hostname(config-ctx)# config-url url
```

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

**Note**

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

See the following URL syntax:

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

This URL indicates the internal Flash memory. The filename does not require a file extension, although we recommend using “.cfg”. If the configuration file is not available, you see the following message:

```
WARNING: Could not fetch the URL disk:/url
INFO: Creating context with default config
```

You can then change to the context, configure it at the CLI, and enter the **write memory** command to write the file to Flash memory.



**Note** The admin context file must be stored on the internal Flash memory.

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

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

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

The server must be accessible from the admin context. The filename does not require a file extension, although we recommend using “.cfg”. If the configuration file is not available, you see the following message:

```
WARNING: Could not fetch the URL ftp://url
INFO: Creating context with default config
```

You can then change to the context, configure it at the CLI, and enter the **write memory** command to write the file to the FTP server.

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

The server must be accessible from the admin context. The filename does not require a file extension, although we recommend using “.cfg”. If the configuration file is not available, you see the following message:

```
WARNING: Could not fetch the URL http://url
INFO: Creating context with default config
```

If you change to the context and configure the context at the CLI, you cannot save changes back to HTTP or HTTPS servers using the **write memory** command. You can, however, use the **copy tftp** command to copy the running configuration to a TFTP server.

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

The server must be accessible from the admin context. Specify the interface name if you want to override the route to the server address. The filename does not require a file extension, although we recommend using “.cfg”. If the configuration file is not available, you see the following message:

```
WARNING: Could not fetch the URL tftp://url
INFO: Creating context with default config
```

You can then change to the context, configure it at the CLI, and enter the **write memory** command to write the file to the TFTP server.

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

See the “[Changing the Security Context URL](#)” section on page 4-24 for more information about changing the URL.

For example, enter the following command:

```
hostname(config-ctx)# config-url ftp://joe:passwd1@10.1.1.1/configlets/test.cfg
```

**Step 5** (Optional) To assign the context to a resource class, enter the following command:

```
hostname(config-ctx)# member class_name
```

If you do not specify a class, the context belongs to the default class. You can only assign a context to one resource class.

For example, to assign the context to the gold class, enter the following command:

```
hostname(config-ctx)# member gold
```

**Step 6** (Optional) To map a context to a specific memory partition, enter the following command:

```
hostname(config-ctx)# allocate-acl-partition partition_number
```

The *partition\_number* is an integer from 0 to the number of partitions available, minus 1. The default is 12 partitions, so the range is 0 to 11. See the “[Configuring Memory Partitions](#)” section on page 4-16 to configure the number of memory partitions.

When you assign a context to a partition, then the partition becomes *exclusive*. An exclusive partition only includes contexts that you specifically assign to it. Partitions that do not have contexts specifically assigned to them are non-exclusive and contexts are allocated to them in a round-robin fashion.



**Note** If you assign contexts to all partitions, then they are all exclusive. However, if you later add a context that is not assigned to a partition, then contexts are allocated to exclusive partitions in a round-robin fashion, and the first best-fit exclusive partition available is used for the allocation of the new context. However, if none of the exclusive partitions can accommodate the rules of the new context, then it is assigned to partition 0 by default, even though partition 0 also cannot accommodate the context rules. The context rules will not load completely, so you need to manually adjust the way contexts are assigned to make room.

For example, to assign the context to the first partition, enter the following command:

```
hostname(config-ctx)# allocate-acl-partition 0
```

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

```
hostname(config)# admin-context administrator
```

```

hostname(config)# context administrator
hostname(config-ctx)# allocate-interface vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passwd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passwd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

```

## Changing Between Contexts and the System Execution Space

If you log in to the system execution space (or the admin context using Telnet or SSH), you can change between contexts and perform configuration and monitoring tasks within each context. The running configuration that you edit in a configuration mode, or that is affected by the **copy** or **write** commands, depends on your location. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the **show running-config** command. Only the current configuration displays. You can, however, save all context running configurations from the system execution space using the **write memory all** command.

For information about command authorization when you change between contexts, see the [“Management Access to Security Contexts”](#) section on page 4-9.

To change between the system execution space and a context, or between contexts, see the following commands:

- To change to a context, enter the following command:

```
hostname# changeto context name
```

The prompt changes to the following:

```
hostname/name#
```

- To change to the system execution space, enter the following command:

```
hostname/admin# changeto system
```

The prompt changes to the following:

```
hostname#
```

# Managing Security Contexts

This section describes how to manage security contexts, and includes the following topics:

- [Removing a Security Context, page 4-23](#)
- [Changing the Admin Context, page 4-23](#)
- [Changing the Security Context URL, page 4-24](#)
- [Reloading a Security Context, page 4-24](#)
- [Monitoring Security Contexts, page 4-25](#)

## Removing a Security Context

You can only remove a context by editing the system configuration. You cannot remove the current admin context, unless you remove all contexts using the **clear context** command.

**Note**

If you use failover, there is a delay between when you remove the context on the active unit or group and when the context is removed on the standby unit or group. You might see an error message indicating that the number of interfaces on the active and standby units are not consistent; this error is temporary and can be ignored.

Use the following commands for removing contexts:

- To remove a single context, enter the following command in the system execution space:

```
hostname(config)# no context name
```

- To remove all contexts (including the admin context), enter the following command in the system execution space:

```
hostname(config)# clear context
```

## Changing the Admin Context

The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users.

You can set any context to be the admin context, as long as the configuration file is stored in the internal Flash memory. To set the admin context, enter the following command in the system execution space:

```
hostname(config)# admin-context context_name
```

Any remote management sessions, such as Telnet, SSH, or HTTPS, that are connected to the admin context are terminated. You must reconnect to the new admin context.

**Note**

A few system commands identify an interface name that belongs to the admin context. If you change the admin context, and that interface name does not exist in the new admin context, be sure to update any system commands that refer to the interface.

## Changing the Security Context URL

You cannot change the security context URL without reloading the configuration from the new URL.

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

To change the URL for a context, perform the following steps:

- Step 1** If you do not want to merge the configuration, change to the context and clear its configuration by entering the following commands. If you want to perform a merge, skip to Step 2.

```
hostname# changeto context name
hostname/name# configure terminal
hostname/name(config)# clear configure all
```

- Step 2** If required, change to the system execution space by entering the following command:

```
hostname/name(config)# changeto system
```

- Step 3** To enter the context configuration mode for the context you want to change, enter the following command:

```
hostname(config)# context name
```

- Step 4** To enter the new URL, enter the following command:

```
hostname(config)# config-url new_url
```

The system immediately loads the context so that it is running.

## Reloading a Security Context

You can reload the context in two ways:

- Clear the running configuration and then import the startup configuration.
  - This action clears most attributes associated with the context, such as connections and NAT tables.
- Remove the context from the system configuration.

This action clears additional attributes, such as memory allocation, which might be useful for troubleshooting. However, to add the context back to the system requires you to respecify the URL and interfaces.

This section includes the following topics:

- [Reloading by Clearing the Configuration, page 4-25](#)
- [Reloading by Removing and Readding the Context, page 4-25](#)

## Reloading by Clearing the Configuration

To reload the context by clearing the context configuration, and reloading the configuration from the URL, perform the following steps:

---

**Step 1** To change to the context that you want to reload, enter the following command:

```
hostname# changeto context name
```

**Step 2** To access configuration mode, enter the following command:

```
hostname/name# configure terminal
```

**Step 3** To clear the running configuration, enter the following command:

```
hostname/name(config)# clear configure all
```

This command clears all connections.

**Step 4** To reload the configuration, enter the following command:

```
hostname/name(config)# copy startup-config running-config
```

The FWSM copies the configuration from the URL specified in the system configuration. You cannot change the URL from within a context.

---

## Reloading by Removing and Readding the Context

To reload the context by removing the context and then readding it, perform the steps in the following sections:

1. [“Removing a Security Context” section on page 4-23](#)
2. [“Configuring a Security Context” section on page 4-18](#)

## Monitoring Security Contexts

This section describes how to view and monitor context information, and includes the following topics:

- [Viewing Context Information, page 4-26](#)
- [Viewing Resource Allocation, page 4-27](#)
- [Viewing Resource Usage, page 4-29](#)
- [Monitoring SYN Attacks in Contexts, page 4-31](#)

## Viewing Context Information

From the system execution space, you can view a list of contexts including the name, allocated interfaces, and configuration file URL.

From the system execution space, view all contexts by entering the following command:

```
hostname# show context [name | detail | count]
```

The **detail** option shows additional information. See the following sample displays for more information.

If you want to show information for a particular context, specify the *name*.

The **count** option shows the total number of contexts.

The following is sample output from the **show context** command. The following sample display shows three contexts:

```
hostname# show context

Context Name      Class      Interfaces      Mode      URL
*admin            default   Vlan100,101    Routed    disk:/admin.cfg
contexta          Gold      Vlan200,201    Transparent disk:/contexta.cfg
contextb          Silver    Vlan300,301    Routed    disk:/contextb.cfg
Total active Security Contexts: 3
```

Table 4-2 shows each field description.

**Table 4-2** *show context Fields*

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Class	Shows the resource class to which the context belongs.
Interfaces	Shows the interfaces assigned to the context.
Mode	Shows the firewall mode for each context, either Routed or Transparent.
URL	Shows the URL from which the FWSM loads the context configuration.

The following is sample output from the **show context detail** command:

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk:/admin.cfg
  Real Interfaces: Vlan100
  Mapped Interfaces: Vlan100
  Class: default, Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: disk:/ctx.cfg
  Real Interfaces: Vlan10,20,30
  Mapped Interfaces: int1, int2, int3
  Class: default, Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Vlan100,10,20,30
  Class: default, Flags: 0x00000019, ID: 257

Context "null", is a system resource
```

```

Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Class: default, Flags: 0x00000009, ID: 258

```

See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information about the **detail** output.

The following is sample output from the **show context count** command:

```

hostname# show context count
Total active contexts: 2

```

## Viewing Resource Allocation

From the system execution space, you can view the allocation for each resource across all classes and class members.

To view the resource allocation, enter the following command:

```
hostname# show resource allocation [detail]
```

This command shows the resource allocation, but does not show the actual resources being used. See the “[Viewing Resource Usage](#)” section on page 4-29 for more information about actual resource usage.

The **detail** argument shows additional information. See the following sample displays for more information.

The following sample display shows the total allocation of each resource as an absolute value and as a percentage of the available system resources:

```

hostname# show resource allocation
Resource          Total          % of Avail
Conns [rate]      35000         35.00%
Fixups [rate]     35000         35.00%
Syslogs [rate]   10500         35.00%
Conns             305000        30.50%
Hosts             78842         30.07%
IPsec             7             35.00%
SSH               35            35.00%
Telnet            35            35.00%
Xlates           91749         34.99%
All               unlimited

```

[Table 4-3](#) shows each field description.

**Table 4-3** *show resource allocation Fields*

Field	Description
Resource	The name of the resource that you can limit.
Total	The total amount of the resource that is allocated across all contexts. The amount is an absolute number of concurrent instances or instances per second. If you specified a percentage in the class definition, the FWSM converts the percentage to an absolute number for this display.
% of Avail	The percentage of the total system resources that is allocated across all contexts.

The following sample display shows the **detail** option:

```

hostname# show resource allocation detail
Resource Origin:
  A Value was derived from the resource 'all'
  C Value set in the definition of this class
  D Value set in default class
Resource      Class      Mmbrs  Origin  Limit      Total      Total %
Conns [rate]  default   all    CA      unlimited
              gold      1      C       34000      34000      20.00%
              silver   1      CA      17000      17000      10.00%
              bronze  0      CA      8500       8500
All Contexts: 3
              51000      30.00%

Fixups [rate] default   all    CA      unlimited
              gold      1      DA      unlimited
              silver   1      CA      10000     10000      10.00%
              bronze  0      CA      5000      5000
All Contexts: 3
              10000     10.00%

Syslogs [rate] default   all    CA      unlimited
              gold      1      C       6000      6000      20.00%
              silver   1      CA      3000      3000      10.00%
              bronze  0      CA      1500      1500
All Contexts: 3
              9000      30.00%

Conns         default   all    CA      unlimited
              gold      1      C       200000    200000    20.00%
              silver   1      CA      100000    100000    10.00%
              bronze  0      CA      50000     50000
All Contexts: 3
              300000    30.00%

Hosts         default   all    CA      unlimited
              gold      1      DA      unlimited
              silver   1      CA      26214     26214     9.99%
              bronze  0      CA      13107     13107
All Contexts: 3
              26214     9.99%

IPSec         default   all    C       5
              gold      1      D       5          5          50.00%
              silver   1      CA      1          1          10.00%
              bronze  0      CA      unlimited
All Contexts: 3
              11         110.00%

SSH           default   all    C       5
              gold      1      D       5          5          5.00%
              silver   1      CA      10         10         10.00%
              bronze  0      CA      5          5
All Contexts: 3
              20         20.00%

Telnet        default   all    C       5
              gold      1      D       5          5          5.00%
              silver   1      CA      10         10         10.00%
              bronze  0      CA      5          5
All Contexts: 3
              20         20.00%

Xlates        default   all    CA      unlimited
              gold      1      DA      unlimited
              silver   1      CA      23040     23040     10.00%
              bronze  0      CA      11520     11520
All Contexts: 3
              23040     10.00%

mac-addresses default   all    C       65535
              gold      1      D       65535     65535     100.00%

```

silver	1	CA	6553	6553	9.99%
bronze	0	CA	3276		
All Contexts:	3			137623	209.99%

Table 4-4 shows each field description.

**Table 4-4** show resource allocation detail Fields

Field	Description
Resource	The name of the resource that you can limit.
Class	The name of each class, including the default class. The All contexts field shows the total values across all classes.
Mmbrs	The number of contexts assigned to each class.
Origin	The origin of the resource limit, as follows: <ul style="list-style-type: none"> <li>• A—You set this limit with the <b>all</b> option, instead of as an individual resource.</li> <li>• C—This limit is derived from the member class.</li> <li>• D—This limit was not defined in the member class, but was derived from the default class. For a context assigned to the default class, the value will be “C” instead of “D.”</li> </ul> The FWSM can combine “A” with “C” or “D.”
Limit	The limit of the resource per context, as an absolute number. If you specified a percentage in the class definition, the FWSM converts the percentage to an absolute number for this display.
Total	The total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.
% of Avail	The percentage of the total system resources that is allocated across all contexts in the class. If the resource is unlimited, this display is blank.

## Viewing Resource Usage

From the system execution space, you can view the resource usage for each context and display the system resource usage.

From the system execution space, view the resource usage for each context by entering the following command:

```
hostname# show resource usage [context context_name | top n | all | summary | system]
[resource {resource_name | all} | detail] [counter counter_name [count_threshold]]
```

By default, **all** context usage is displayed; each context is listed separately.

Enter the **top n** keyword to show the contexts that are the top *n* users of the specified resource. You must specify a single resource type, and not **resource all**, with this option.

The **summary** option shows all context usage combined.

The **system** option shows all context usage combined, but shows the system limits for resources instead of the combined context limits.

For the **resource** *resource\_name*, see [Table 4-1](#) for available resource names. See also the **show resource type** command. Specify **all** (the default) for all types.

The **detail** option shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.

The **counter** *counter\_name* is one of the following keywords:

- **current**—Shows the active concurrent instances or the current rate of the resource.
- **denied**—Shows the number of instances that were denied because they exceeded the resource allocation.
- **peak**—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **all**—(Default) Shows all statistics.

The *count\_threshold* sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify **all** for the counter name, then the *count\_threshold* applies to the current usage.


**Note**

To show all resources, set the *count\_threshold* to **0**.

The following is sample output from the **show resource usage context** command, which shows the resource usage for the admin context:

```
hostname# show resource usage context admin
```

Resource	Current	Peak	Limit	Denied	Context
Telnet	1	1	5	0	admin
Conns	44	55	N/A	0	admin
Hosts	45	56	N/A	0	admin

The following is sample output from the **show resource usage summary** command, which shows the resource usage for all contexts and all resources. This sample shows the limits for 6 contexts.

```
hostname# show resource usage summary
```

Resource	Current	Peak	Limit	Denied	Context
Syslogs [rate]	1743	2132	12000 (U)	0	Summary
Conns	584	763	100000 (S)	0	Summary
Xlates	8526	8966	93400	0	Summary
Hosts	254	254	262144	0	Summary
Conns [rate]	270	535	42200	1704	Summary
Fixups [rate]	270	535	100000 (S)	0	Summary

U = Some contexts are unlimited and are not included in the total.  
 S = System limit: Combined context limits exceed the system limit; the system limit is shown.

The following is sample output from the **show resource usage system counter all 0** command, which shows the resource usage for all contexts, but it shows the system limit instead of the combined context limits:

```
hostname# show resource usage system counter all 0
```

Resource	Current	Peak	Limit	Denied	Context
Telnet	0	0	100	0	System
SSH	0	0	100	0	System
ASDM	0	0	80	0	System
IPSec	0	0	10	0	System
Syslogs [rate]	0	0	30000	0	System
Conns	0	0	1000000	0	System

Xlates	0	0	262144	0 System
Hosts	0	0	262144	0 System
Conns [rate]	0	0	170000	0 System
Fixups [rate]	0	0	100000	0 System
Mac-addresses	0	0	65535	0 System

## Monitoring SYN Attacks in Contexts

The FWSM prevents SYN attacks using TCP Intercept. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the FWSM acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the FWSM receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

You can monitor the rate of attacks for individual contexts using the **show perfmon** command; you can monitor the amount of resources being used by TCP intercept for individual contexts using the **show resource usage detail** command; you can monitor the resources being used by TCP intercept for the entire system using the **show resource usage summary detail** command.

The following is sample output from the **show perfmon** command that shows the rate of TCP intercepts for a context called admin.

```
hostname/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates           0/s          0/s
Connections      0/s          0/s
TCP Conns        0/s          0/s
UDP Conns        0/s          0/s
URL Access       0/s          0/s
URL Server Req   0/s          0/s
WebSns Req       0/s          0/s
TCP Fixup        0/s          0/s
HTTP Fixup       0/s          0/s
FTP Fixup        0/s          0/s
AAA Authen       0/s          0/s
AAA Author       0/s          0/s
AAA Account      0/s          0/s
TCP Intercept    322779/s     322779/s
```

The following is sample output from the **show resource usage detail** command that shows the amount of resources being used by TCP Intercept for individual contexts. (Sample text in italics shows the TCP intercept information.)

```
hostname(config)# show resource usage detail

Resource          Current      Peak      Limit      Denied Context
memory            843732      847288   unlimited  0 admin
chunk:channels    14          15       unlimited  0 admin
chunk:fixup       15          15       unlimited  0 admin
chunk:hole        1           1        unlimited  0 admin
chunk:ip-users    10          10       unlimited  0 admin
chunk:list-elem   21          21       unlimited  0 admin
chunk:list-hdr    3           4        unlimited  0 admin
chunk:route       2           2        unlimited  0 admin
chunk:static      1           1        unlimited  0 admin
tcp-intercept-rate 328787      803610   unlimited  0 admin
np-statics       3           3        unlimited  0 admin
```

statics	1	1	unlimited	0	admin
ace-rules	1	1	N/A	0	admin
console-access-rul	2	2	N/A	0	admin
fixup-rules	14	15	N/A	0	admin
memory	959872	960000	unlimited	0	c1
chunk:channels	15	16	unlimited	0	c1
chunk:dbgtrace	1	1	unlimited	0	c1
chunk:fixup	15	15	unlimited	0	c1
chunk:global	1	1	unlimited	0	c1
chunk:hole	2	2	unlimited	0	c1
chunk:ip-users	10	10	unlimited	0	c1
chunk:udp-ctrl-blk	1	1	unlimited	0	c1
chunk:list-elem	24	24	unlimited	0	c1
chunk:list-hdr	5	6	unlimited	0	c1
chunk:nat	1	1	unlimited	0	c1
chunk:route	2	2	unlimited	0	c1
chunk:static	1	1	unlimited	0	c1
<i>tcp-intercept-rate</i>	<i>16056</i>	<i>16254</i>	<i>unlimited</i>	<i>0</i>	<i>c1</i>
globals	1	1	unlimited	0	c1
np-statics	3	3	unlimited	0	c1
statics	1	1	unlimited	0	c1
nats	1	1	unlimited	0	c1
ace-rules	2	2	N/A	0	c1
console-access-rul	2	2	N/A	0	c1
fixup-rules	14	15	N/A	0	c1
memory	232695716	232020648	unlimited	0	system
chunk:channels	17	20	unlimited	0	system
chunk:dbgtrace	3	3	unlimited	0	system
chunk:fixup	15	15	unlimited	0	system
chunk:ip-users	4	4	unlimited	0	system
chunk:list-elem	1014	1014	unlimited	0	system
chunk:list-hdr	1	1	unlimited	0	system
chunk:route	1	1	unlimited	0	system
block:16384	510	885	unlimited	0	system
block:2048	32	34	unlimited	0	system

The following sample output shows the resources being used by TCP intercept for the entire system. (Sample text in italics shows the TCP intercept information.)

```
hostname(config)# show resource usage summary detail
Resource           Current      Peak      Limit      Denied Context
memory             238421312  238434336 unlimited 0 Summary
chunk:channels     46          48 unlimited 0 Summary
chunk:dbgtrace     4           4 unlimited 0 Summary
chunk:fixup        45          45 unlimited 0 Summary
chunk:global       1           1 unlimited 0 Summary
chunk:hole         3           3 unlimited 0 Summary
chunk:ip-users     24          24 unlimited 0 Summary
chunk:udp-ctrl-blk 1           1 unlimited 0 Summary
chunk:list-elem    1059        1059 unlimited 0 Summary
chunk:list-hdr     10          11 unlimited 0 Summary
chunk:nat          1           1 unlimited 0 Summary
chunk:route        5           5 unlimited 0 Summary
chunk:static       2           2 unlimited 0 Summary
block:16384        510         885      8192(S)   0 Summary
block:2048         32          35      1000(S)   0 Summary
tcp-intercept-rate 341306    811579 unlimited 0 Summary
globals            1           1      1051(S)   0 Summary
np-statics         6           6      4096(S)   0 Summary
statics            2           2      2048(S)   0 Summary
nats               1           1      2048(S)   0 Summary
ace-rules          3           3     116448(S) 0 Summary
console-access-rul 4           4      4356(S)   0 Summary
fixup-rules        43          44      8032(S)   0 Summary
```

S = System: Total exceeds the system limit; the system limit is shown

