



## CHAPTER 9

# Configuring Security Contexts

---

This chapter describes how to use security contexts and enable multiple context mode. This chapter includes the following sections:

- [Security Context Overview, page 9-1](#)
- [Enabling or Disabling Multiple Context Mode at the CLI, page 9-9](#)
- [Configuring Resource Classes, page 9-10](#)
- [Configuring Security Contexts, page 9-19](#)

## Security Context Overview

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with 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, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. 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.

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

- [Common Uses for Security Contexts, page 9-2](#)
- [Unsupported Features, page 9-2](#)
- [Context Configuration Files, page 9-2](#)
- [How the Security Appliance Classifies Packets, page 9-2](#)
- [Management Access to Security Contexts, page 9-8](#)

## 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 security appliance, 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 security appliance.

## 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.
- VPN
- Multicast routing. Multicast bridging is supported.
- Threat Detection

## Context Configuration Files

Each context has its own configuration file that identifies the security policy, interfaces, and, for supported features, 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.

In addition to individual security contexts, the security appliance also includes a system configuration that identifies basic settings for the security appliance, including a list of contexts. Like the single mode configuration, this configuration resides as the startup configuration.

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 a 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. 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 Security Appliance Classifies Packets

Each packet that enters the security appliance must be classified, so that the security appliance can determine to which context to send a packet. This section includes the following topics:

- [Valid Classifier Criteria, page 9-3](#)

- [Invalid Classifier Criteria, page 9-4](#)
- [Classification Examples, page 9-4](#)

**Note**

If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each context.

## Valid Classifier Criteria

This section describes the criteria used by the classifier, and includes the following topics:

- [Unique Interfaces, page 9-3](#)
- [Unique MAC Addresses, page 9-3](#)
- [NAT Configuration, page 9-3](#)

### Unique Interfaces

If only one context is associated with the ingress interface, the security appliance 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.

### Unique MAC Addresses

If multiple contexts share an interface, then the classifier uses the interface MAC address. The security appliance lets you assign a different MAC address in each context to the same shared interface, whether it is a shared physical interface or a shared subinterface. By default, shared interfaces do not have unique MAC addresses; the interface uses the physical interface burned-in MAC address in every context. An upstream router cannot route directly to a context without unique MAC addresses. You can set the MAC addresses manually when you configure each interface (see [Add/Edit Interface > Advanced](#)), or you can automatically generate MAC addresses (see [Security Contexts](#)).

### NAT Configuration

If you do not have unique MAC addresses, 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 the NAT configuration to determine the subnets in each context. The classifier matches the destination IP address to either a **static** command or a **global** command. In the case of the **global** command, the classifier does not need a matching **nat** command or an active NAT session to classify the packet. Whether the packet can communicate with the destination IP address after classification depends on how you configure NAT and NAT control.

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
```

**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 a mapped interface.
- Routing table—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 9-1 shows multiple contexts sharing an outside interface. The classifier assigns the packet to Context B because Context B includes the MAC address to which the router sends the packet.

**Figure 9-1** Packet Classification with a Shared Interface using MAC Addresses

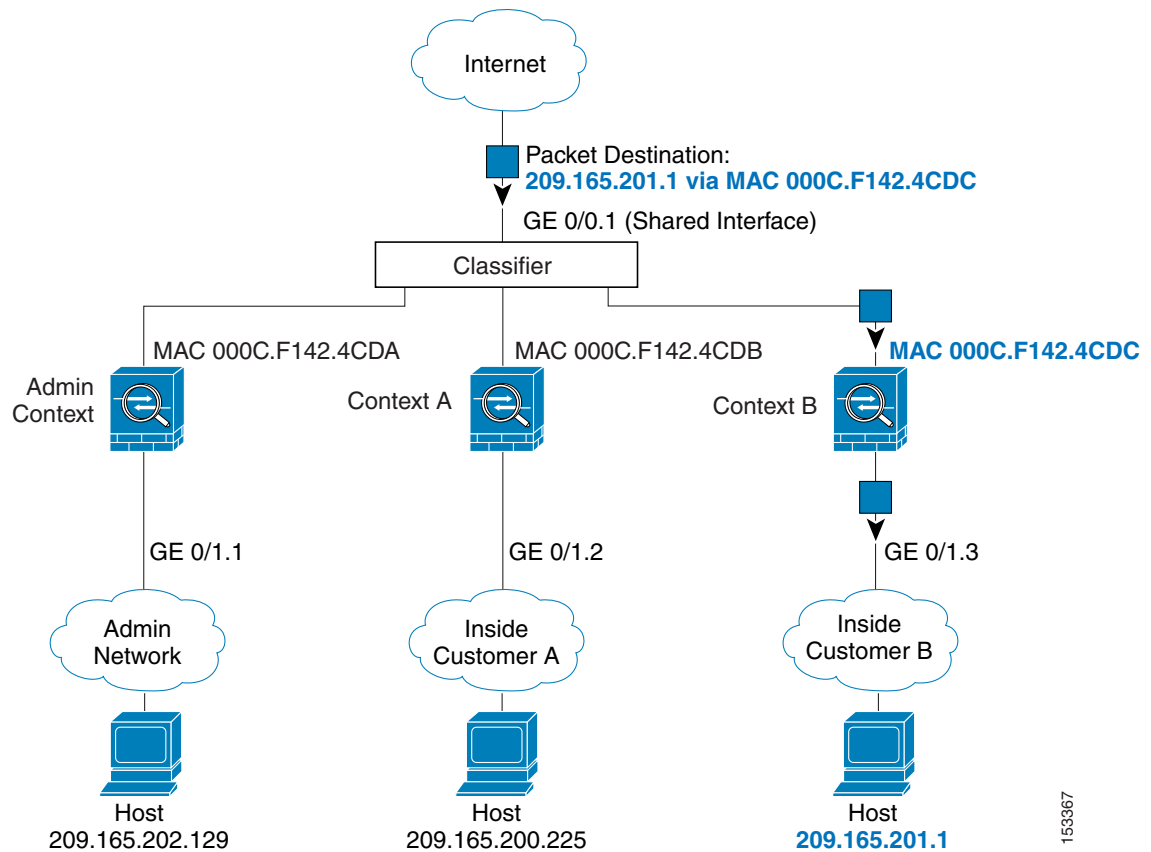
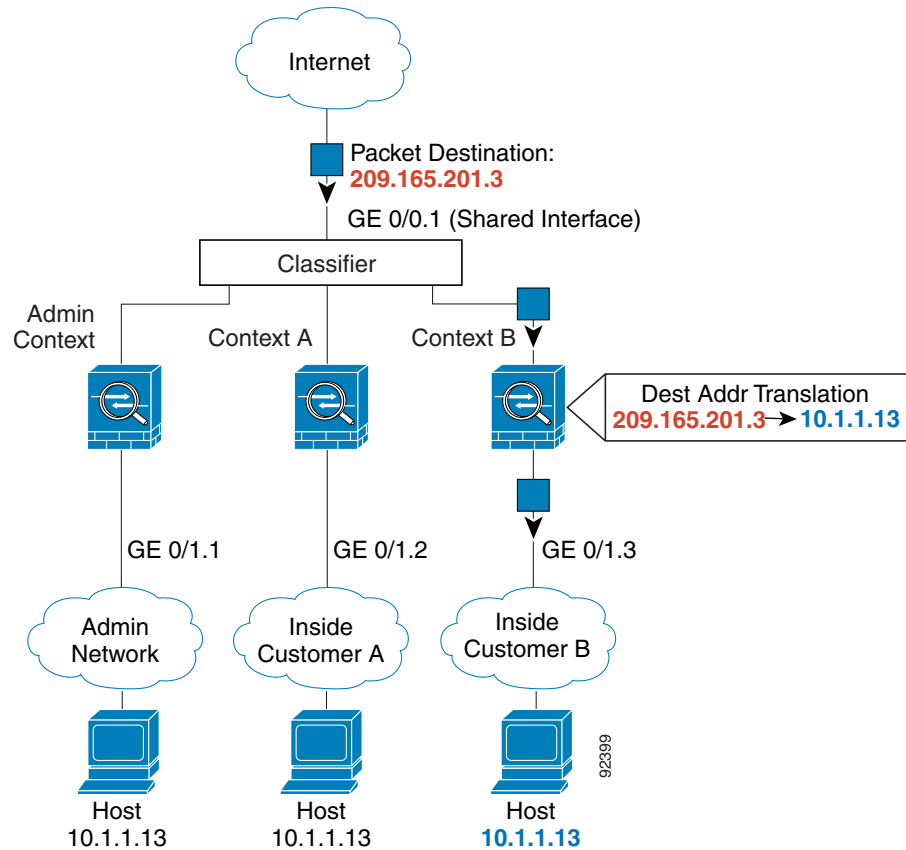


Figure 9-2 shows multiple contexts sharing an outside interface without MAC addresses assigned. The classifier assigns the packet to Context B because Context B includes the address translation that matches the destination address.

Figure 9-2 Packet Classification with a Shared Interface using NAT



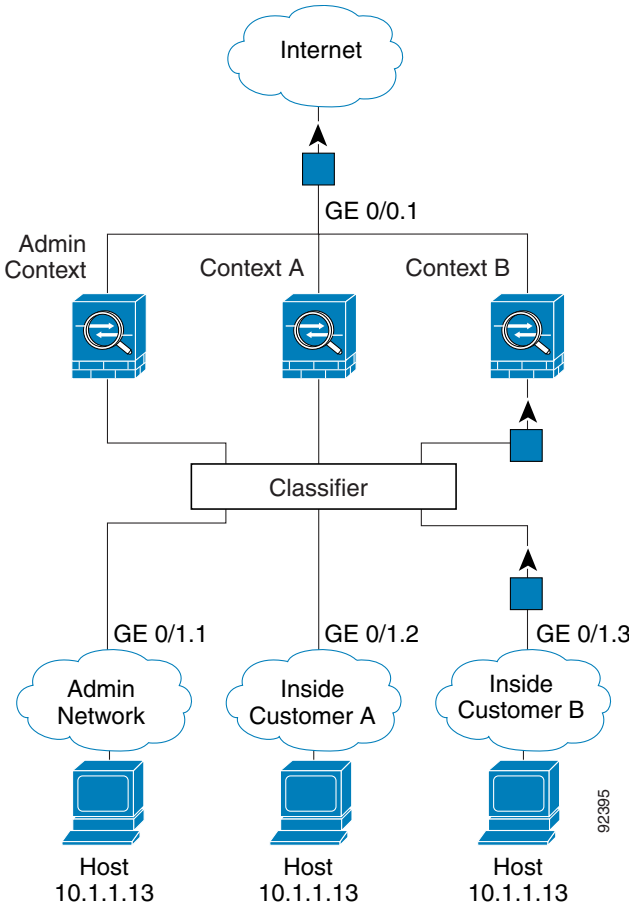
Note that all new incoming traffic must be classified, even from inside networks. Figure 9-3 shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 0/1.3, which is assigned to Context B.



**Note**

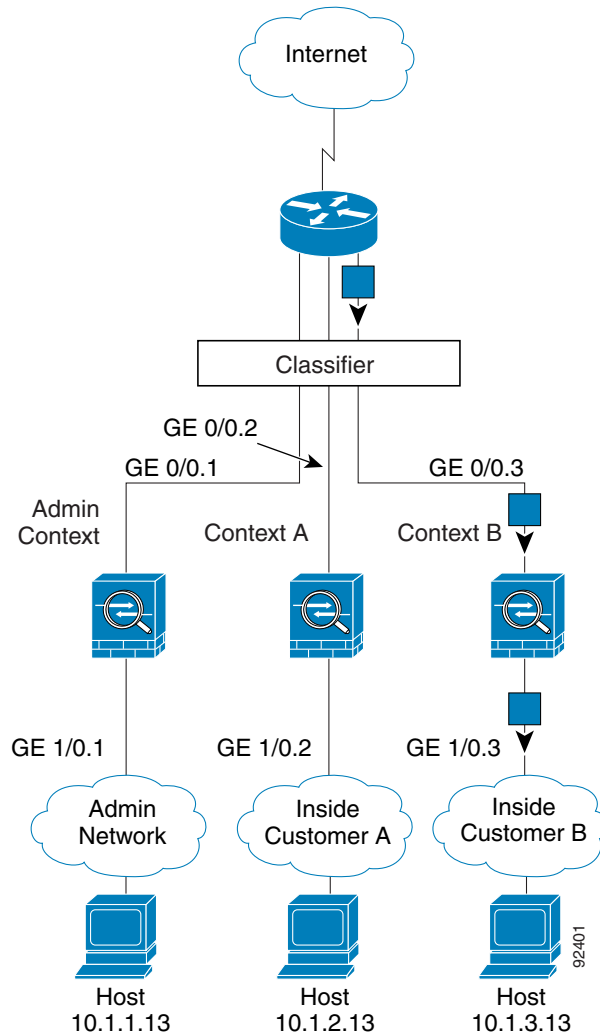
If you share an *inside* interface and do not use unique MAC addresses, the classifier imposes some major restrictions. The classifier relies on the address translation configuration to classify the packet within a context, and you must translate the *destination* addresses of the traffic. Because you do not usually perform NAT on outside addresses, sending packets from inside to outside on a shared interface is not always possible; the outside network is large, (the Web, for example), and addresses are not predictable for an outside NAT configuration. If you share an inside interface, we suggest you use unique MAC addresses.

Figure 9-3 Incoming Traffic from Inside Networks



For transparent firewalls, you must use unique interfaces. [Figure 9-4](#) 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 Gigabit Ethernet 1/0.3, which is assigned to Context B.

**Figure 9-4** Transparent Firewall Contexts



## Cascading Security Contexts

Placing a context directly in front of another context is called cascading contexts; the outside interface of one context is the same interface as the inside interface of another context. You might want to cascade contexts if you want to simplify the configuration of some contexts by configuring shared parameters in the top context.

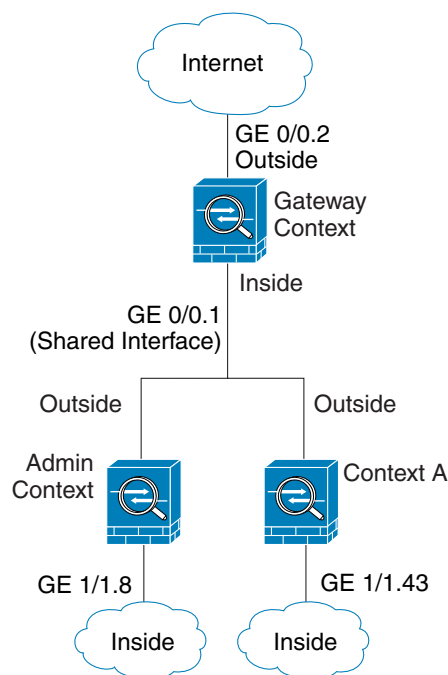


### Note

Cascading contexts requires that you configure unique MAC addresses for each context interface. Because of the limitations of classifying packets on shared interfaces without MAC addresses, we do not recommend using cascading contexts without unique MAC addresses.

Figure 9-5 shows a gateway context with two contexts behind the gateway.

**Figure 9-5 Cascading Contexts**



## Management Access to Security Contexts

The security appliance 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 9-8](#)
- [Context Administrator Access, page 9-9](#)

### System Administrator Access

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

- Access the security appliance console.  
From the console, you access the system execution space.
- Access the admin context using Telnet, SSH, or ASDM.  
See [Chapter 13, “Configuring Management Access,”](#) to enable Telnet, SSH, and ASDM 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 13, “Configuring Management Access,”](#) to enable Telnet, SSH, and SDM access and to configure management authentication.

# Enabling or Disabling Multiple Context Mode at the CLI

Your security appliance 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 9-9](#)
- [Enabling Multiple Context Mode, page 9-9](#)
- [Restoring Single Context Mode, page 9-10](#)

## Backing Up the Single Mode Configuration

When you convert from single mode to multiple mode, the security appliance 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 security appliance 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 security appliance 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 security appliance.

## 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 security appliance; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device. Because the system configuration does not have any network interfaces as part of its configuration, you must access the security appliance from the console 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 flash: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 security appliance reboots.

---

## Configuring Resource Classes

By default, all security contexts have unlimited access to the resources of the security appliance, 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.

This section includes the following topics:

- [Classes and Class Members Overview, page 9-10](#)
- [Adding a Resource Class, page 9-13](#)
- [Monitoring Context Resource Usage, page 9-15](#)
- [Resource Class Field Descriptions, page 9-16](#)

## Classes and Class Members Overview

The security appliance 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 9-11](#)
- [Default Class, page 9-12](#)
- [Class Members, page 9-13](#)

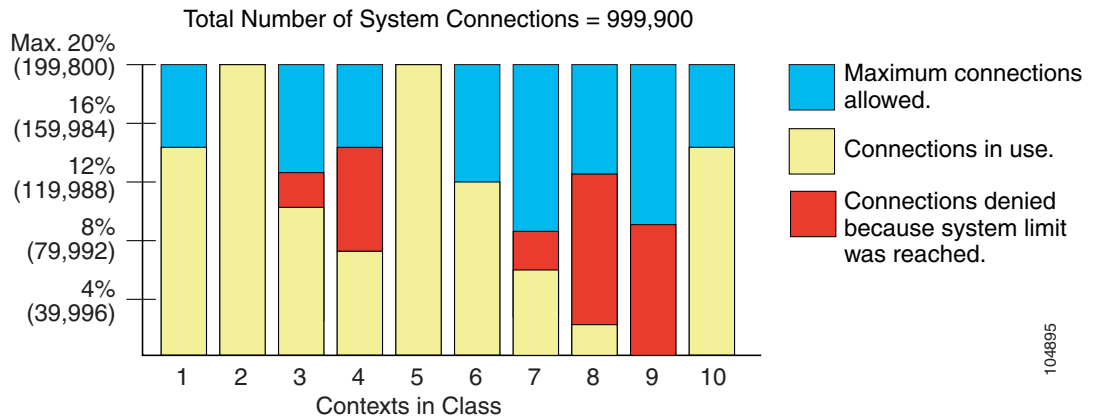
## Resource Limits

When you create a class, the security appliance does not set aside a portion of the resources for each context assigned to the class; rather, the security appliance 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 individual resources, as a percentage (if there is a hard system limit) or as an absolute value.

You can oversubscribe the security appliance by assigning more than 100 percent of a resource 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 9-6](#).)

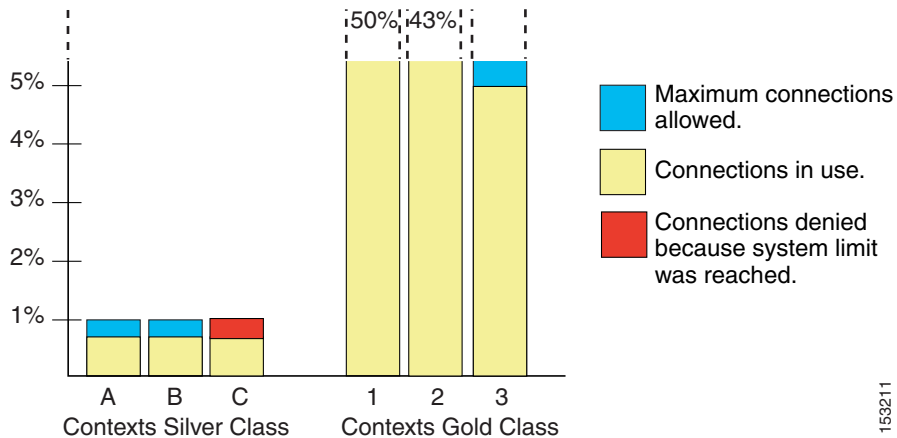
**Figure 9-6 Resource Oversubscription**



If you assign an absolute value to a resource across all contexts that exceeds the practical limit of the security appliance, then the performance of the security appliance might be impaired.

The security appliance 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 or that is practically available. For example, Context A, B, and C are in the Silver Class, which limits each class member to 1 percent of the connections, for a total of 3 percent; but the three contexts are currently only using 2 percent combined. Gold Class has unlimited access to connections. The contexts in the Gold Class can use more than the 97 percent of “unassigned” connections; they can also use the 1 percent of connections 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 9-7](#).) Setting unlimited access is similar to oversubscribing the security appliance, except that you have less control over how much you oversubscribe the system.

Figure 9-7 Unlimited Resources



153211

## 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.

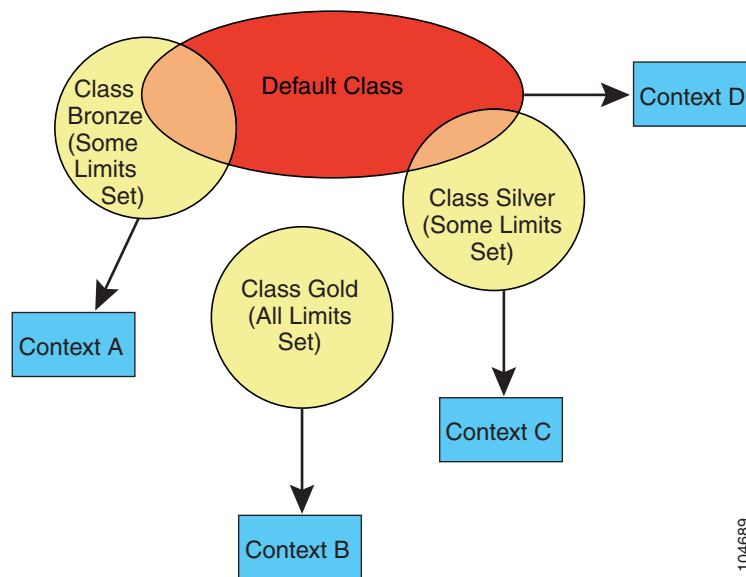
If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 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 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 9-8 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 9-8** Resource Classes



104689

## 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.

## Adding a Resource Class

To add a resource class, perform the following steps:

- Step 1** If you are not already in the System configuration mode, in the Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Resource Class pane, click **Add**.  
The Add Resource Class dialog box appears.
- Step 3** In the Resource Class field, enter a class name up to 20 characters in length.
- Step 4** In the Count Limited Resources area, set the concurrent limits for resources.

For resources that do not have a system limit, you cannot set the percentage; you can only set an absolute value. If you do not set a limit, the limit is inherited from the default class. If the default class does not set a limit, then the resource is unlimited, or the system limit if available.

You can set one or more of the following limits:

- **Hosts**—Sets the limit for concurrent hosts that can connect through the security appliance. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **Telnet**—Sets the limit for concurrent Telnet sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 100 sessions divided between all contexts.
- **ASDM Sessions**—Sets the limit for concurrent ASDM sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 80 sessions divided between all contexts. 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 32 ASDM sessions represents a limit of 64 HTTPS sessions, divided between all contexts.
- **Connections**—Sets the limit for concurrent TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 0 (system limit) and the system limit for your model, and selecting **Absolute** from the list. See the *Cisco ASDM Release Notes* for the connection limit for your model.
- **Xlates**—Sets the limit for address translations. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **SSH**—Sets the limit for SSH sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 100 sessions divided between all contexts.
- **MAC Entries**—(Transparent mode only) Sets the limit for MAC address entries in the MAC address table. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 0 (system limit) and 65535 and selecting **Absolute** from the list.

**Step 5** In the Rate Limited Resources area, set the rate limit for resources.

If you do not set a limit, the limit is inherited from the default class. If the default class does not set a limit, then it is unlimited by default.

You can set one or more of the following limits:

- **Conns/sec**—Sets the limit for connections per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **Syslogs/sec**—Sets the limit for system log messages per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- **Inspects/sec**—Sets the limit for application inspections per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.

**Step 6** Click **OK**.

---

## Monitoring Context Resource Usage

To monitor resource usage of all contexts from the system execution space, perform the following steps:

**Step 1** If you are not already in the System mode, in the Device List pane, double-click **System** under the active device IP address.

**Step 2** Click the **Monitoring** button on the toolbar.

**Step 3** Click **Context Resource Usage**.

Click each resource type to view the resource usage for all contexts:

- **ASDM**—Shows the usage of ASDM connections.
  - Context—Shows the name of each context.
  - Existing Connections (#)—Shows the number of existing connections.
  - Existing Connections (%)—Shows the connections used by this context as a percentage of the total number of connections used by all contexts.
  - Peak Connections (#)—Shows the peak number of connections since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **Telnet**—Shows the usage of Telnet connections.
  - Context—Shows the name of each context.
  - Existing Connections (#)—Shows the number of existing connections.
  - Existing Connections (%)—Shows the connections used by this context as a percentage of the total number of connections used by all contexts.
  - Peak Connections (#)—Shows the peak number of connections since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **SSH**—Shows the usage of SSH connections.
  - Context—Shows the name of each context.
  - Existing Connections (#)—Shows the number of existing connections.
  - Existing Connections (%)—Shows the connections used by this context as a percentage of the total number of connections used by all contexts.
  - Peak Connections (#)—Shows the peak number of connections since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **Xlates**—Shows the usage of network address translations.
  - Context—Shows the name of each context.
  - Xlates (#)—Shows the number of current xlates.
  - Xlates (%)—Shows the xlates used by this context as a percentage of the total number of xlates used by all contexts.
  - Peak (#)—Shows the peak number of xlates since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **NATs**—Shows the number of NAT rules.

- Context—Shows the name of each context.
- NATs (#)—Shows the current number of NAT rules.
- NATs (%)—Shows the NAT rules used by this context as a percentage of the total number of NAT rules used by all contexts.
- Peak NATs (#)—Shows the peak number of NAT rules since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.
- **Syslogs**—Shows the rate of system log messages.
  - Context—Shows the name of each context.
  - Syslog Rate (#/sec)—Shows the current rate of system log messages.
  - Syslog Rate (%)—Shows the system log messages generated by this context as a percentage of the total number of system log messages generated by all contexts.
  - Peak Syslog Rate (#/sec)—Shows the peak rate of system log messages since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted.

**Step 4** Click **Refresh** to refresh the view.

---

## Resource Class Field Descriptions

This section includes the field descriptions for Resource Class screens, and includes the following topics:

- [Resource Class, page 9-16](#)
- [Add/Edit Resource Class, page 9-17](#)

## Resource Class

The Resource Class pane shows the configured classes and information about each class. It also lets you add, edit, or delete a class.

### Fields

- Class—Shows the class name.
- All Resources—Shows the limit for all resources that you do not set individually, which can only be 0, which means unlimited.
- Connections—Shows the limit for TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts.
- Hosts—Shows the limit for hosts that can connect through the security appliance.
- Xlates—Shows the limit for address translations.
- Telnet—Shows the limit for Telnet sessions, by default 5.
- SSH—Shows the limit for SSH sessions, by default 5.
- ASDM Sessions—Shows the limit for ASDM management sessions, by default 5. 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 32 ASDM sessions represents a limit of 64 HTTPS sessions, divided between all contexts.

- **MAC**—Shows the limit for MAC addresses in the MAC address table in transparent firewall mode, by default 65535.
- **Conns/sec**—Shows the limit for connections per second.
- **Fixups/sec**—Shows the limit for application inspections per second.
- **Syslogs/sec**—Shows the limit for system log messages per second.
- **Contexts**—Shows the contexts assigned to this class.
- **Add**—Adds a class.
- **Edit**—Edits a class.
- **Delete**—Deletes a class. You cannot delete the default class. If you delete a class to which you assigned contexts, the contexts revert to using the default class.

### Modes

The following table shows the modes in which this feature is available:

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

## Add/Edit Resource Class

The Add/Edit Resource Class dialog box lets you add or edit a resource class.

### Fields

- **Resource Class**—Sets the class name as a string up to 20 characters in length.
- **Count Limited Resources**—Sets the concurrent limits for resources. For resources that do not have a system limit, you cannot set the percentage; you can only set an absolute value. If you do not set a limit, the limit is inherited from the default class. If the default class does not set a limit, then the resource is unlimited, or the system limit if available.
  - **Hosts**—Sets the limit for concurrent hosts that can connect through the security appliance. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
  - **Telnet**—Sets the limit for concurrent Telnet sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 100 sessions divided between all contexts.
  - **ASDM Sessions**—Sets the limit for concurrent ASDM sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 80 sessions divided between all contexts. 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 32 ASDM sessions represents a limit of 64 HTTPS sessions, divided between all contexts.

- Connections—Sets the limit for concurrent TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 0 (system limit) and the system limit for your model, and selecting **Absolute** from the list. See the *Cisco ASDM Release Notes* for the connection limit for your model.
- Xlates—Sets the limit for address translations. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- SSH—Sets the limit for SSH sessions. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 1 and 5 and selecting **Absolute** from the list. The system has a maximum of 100 sessions divided between all contexts.
- MAC Entries—(Transparent mode only) Sets the limit for MAC address entries in the MAC address table. Select the check box to enable this limit. You can set the limit as a percentage by entering any integer greater than 1 and selecting **Percent** from the list. You can assign more than 100 percent if you want to oversubscribe the device. Or you can set the limit as an absolute value by entering an integer between 0 (system limit) and 65535 and selecting **Absolute** from the list.
- Rate Limited Resources—Sets the rate limit for resources. If you do not set a limit, the limit is inherited from the default class. If the default class does not set a limit, then it is unlimited by default.
  - Conns/sec—Sets the limit for connections per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
  - Syslogs/sec—Sets the limit for system log messages per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
  - Inspects/sec—Sets the limit for application inspections per second. Select the check box to enable this limit. If you set the limit to 0, it is unlimited.
- Show Actual Class Limits—(Non-default classes only) When you edit a class, this button shows the limits you set plus any inherited limits from the default class for limits you did not set.

### Modes

The following table shows the modes in which this feature is available:

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

# Configuring Security Contexts

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

- [Adding a Security Context, page 9-19](#)
- [Automatically Assigning MAC Addresses, page 9-20](#)
- [Security Context Field Descriptions, page 9-21](#)

## Adding a Security Context

To add a security context, perform the following steps:

- 
- Step 1** If you are not already in the System configuration mode, in the Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Security Contexts pane, click **Add**.  
The Add Context dialog box appears.
- Step 3** In the Security Context field, enter the context name as a string up to 32 characters long.  
This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. “System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.
- Step 4** In the Interface Allocation area, click the **Add** button to assign an interface to the context.
- Step 5** From the Interfaces > Physical Interface drop-down list, choose an interface.  
You can assign the main interface, in which case you leave the subinterface ID blank, or you can assign a subinterface or a range of subinterfaces associated with this interface. In transparent firewall mode, only interfaces that have not been allocated to other contexts are shown. If the main interface was already assigned to another context, then you must choose a subinterface.
- Step 6** (Optional) In the Interfaces > Subinterface Range (optional) drop-down list, choose a subinterface ID.  
For a range of subinterface IDs, choose the ending ID in the second drop-down list, if available.  
In transparent firewall mode, only subinterfaces that have not been allocated to other contexts are shown.
- Step 7** (Optional) In the Aliased Names area, check **Use Aliased Name in Context** to set an aliased name for this interface to be used in the context configuration instead of the interface ID.
- In the Name field, sets the aliased name.  
An aliased name must start with a letter, end with a letter, and have as interior characters only letters, digits, or an underscore. This field lets you specify a name that ends with a letter or underscore; to add an optional digit after the name, set the digit in the Range field.
  - (Optional) In the Range field, set the numeric suffix for the aliased name.  
If you have a range of subinterfaces, you can enter a range of digits to be appended to the name.
- Step 8** (Optional) To enable context users to see physical interface properties even if you set an aliased name, check **Show Hardware Properties in Context**.
- Step 9** Click **OK** to return to the Add Context dialog box.
- Step 10** (Optional) If you use IPS virtual sensors, then assign a sensor to the context in the IPS Sensor Allocation area.  
For detailed information about IPS and virtual sensors, see [Chapter 39, “Configuring IPS.”](#)

- Step 11** (Optional) To assign this context to a resource class, choose a class name from the Resource Assignment > Resource Class drop-down list.
- You can add or edit a resource class directly from this area. See the [“Configuring Resource Classes” section on page 9-10](#) for more information.
- Step 12** To set the context configuration location, identify the URL by choosing a file system type from the Config URL drop-down list and entering a path in the field.
- For example, the combined URL for FTP has the following format:
- ```
ftp://server.example.com/configs/admin.cfg
```
- Step 13** (Optional) For external filesystems, set the username and password by clicking **Login**.
- Step 14** (Optional) To set the failover group for active/active failover, choose the group name in the Failover Group drop-down list.
- Step 15** (Optional) Add a description in the Description field.
- 

## Automatically Assigning MAC Addresses

This section describes how to assign unique MAC addresses to context interfaces, and includes the following sections:

- [MAC Address Overview, page 9-20](#)
- [Enabling Automatic MAC Address Assignment, page 9-21](#)

### MAC Address Overview

To allow contexts to share interfaces, we suggest that you assign unique MAC addresses to each context interface. The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. The destination address is matched with the context NAT configuration, and this method has some limitations compared to the MAC address method. See the [“How the Security Appliance Classifies Packets” section on page 9-2](#) for information about classifying packets.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

For use with failover, the security appliance generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption.

When you assign an interface to a context, the new MAC address is generated immediately. If you enable this option after you create context interfaces, then MAC addresses are generated for all interfaces immediately after you apply the option. If you disable this option, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

The MAC address is generated using the following format:

- Active unit MAC address: *12\_slot.port\_subid.contextid*.
- Standby unit MAC address: *02\_slot.port\_subid.contextid*.

For platforms with no interface slots, the slot is always 0. The *port* is the interface port. The *subid* is an internal ID for the subinterface, which is not viewable. The *contextid* is an internal ID for the context. For example, the interface GigabitEthernet 0/1.200 in the context with the ID 1 has the following generated MAC addresses, where the internal ID for subinterface 200 is 31:

- Active: 1200.0131.0001
- Standby: 0200.0131.0001

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See the “[Configuring an Interface](#)” section on page 5-5 to manually set the MAC address.

## Enabling Automatic MAC Address Assignment

To enable automatic MAC address assignment, perform the following steps.

- 
- Step 1** If you are not already in the System configuration mode, in the Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Security Contexts pane, check **Mac-Address auto**.
- 

## Security Context Field Descriptions

This section includes the field descriptions for Resource Class screens, and includes the following topics:

- [Security Contexts](#), page 9-21
- [Add/Edit Context](#), page 9-22
- [Add/Edit Interface Allocation](#), page 9-24

## Security Contexts

### Fields

- Context—Shows the context name.
- Interfaces—Shows the interfaces and subinterfaces assigned to the context. If you assigned an alias for the interface name to show in a context, then the aliased name is shown in parentheses. If you specified a range of subinterfaces, the range displays with a dash between the first and last subinterface numbers.
- Resource—Shows the resource class for each context.
- Config URL—Shows the context configuration location.
- Group—Shows the failover group to which this context belongs.
- Description—Shows a description of the context.
- Add—Adds a context.
- Edit—Edits a context.
- Delete—Deletes a context.

- **Mac-Address auto**—Automatically assigns private MAC addresses to each shared context interface.

To allow contexts to share interfaces, we suggest that you assign unique MAC addresses to each context interface. The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. The destination address is matched with the context NAT configuration, and this method has some limitations compared to the MAC address method. See the [“How the Security Appliance Classifies Packets” section on page 9-2](#) for information about classifying packets.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

For use with failover, the security appliance generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption.

When you assign an interface to a context, the new MAC address is generated immediately. If you enable this option after you create context interfaces, then MAC addresses are generated for all interfaces immediately after you apply the option. If you disable this option, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

The MAC address is generated using the following format:

Active unit MAC address: *12\_slot.port\_subid.contextid*.

Standby unit MAC address: *02\_slot.port\_subid.contextid*.

For platforms with no interface slots, the slot is always 0. The *port* is the interface port. The *subid* is an internal ID for the subinterface, which is not viewable. The *contextid* is an internal ID for the context. For example, the interface GigabitEthernet 0/1.200 in the context with the ID 1 has the following generated MAC addresses, where the internal ID for subinterface 200 is 31:

Active: 1200.0131.0001

Standby: 0200.0131.0001

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See the [“Configuring an Interface” section on page 5-5](#) to manually set the MAC address.

### Modes

The following table shows the modes in which this feature is available:

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

## Add/Edit Context

### Fields

- **Security Context**—Sets the context name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named “customerA” and “CustomerA,” for example. “System” or “Null” (in upper or lower case letters) are reserved names, and cannot be used.

- Interface Allocation—Shows the interfaces and subinterfaces assigned to this context.
  - Interface—Shows the interface IDs. If you specified a range of subinterfaces, the range displays with a dash between the first and last subinterface numbers.
  - Aliased Name—Shows the aliased name for this interface to be used in the context configuration instead of the interface ID.
  - Visible—Shows whether context users can see physical interface properties even if you set an aliased name.
  - Add—Adds an interface to the context.
  - Edit—Edits the interface properties.
  - Delete—Deletes an interface.
- IPS Sensor Allocation—You can assign one or more IPS virtual sensors to each context. Then, when you configure the context to send traffic to the AIP SSM, you can specify a sensor that is assigned to the context; you cannot specify a sensor that you did not assign to the context. If you do not assign any sensors to a context, then the default sensor configured on the AIP SSM is used. You can assign the same sensor to multiple contexts. See the [“Using Virtual Sensors” section on page 39-3](#) for more information.
  - Sensor Name—Shows the assigned sensors. You can only assign sensors that are available on the AIP SSM.
  - Mapped Sensor Name—Shows the mapped name for the sensor. This sensor name can be used within the context instead of the actual sensor name. If you do not specify a mapped name, the sensor name is used within the context. For security purposes, you might not want the context administrator to know which sensors are being used by the context. Or you might want to genericize the context configuration. For example, if you want all contexts to use sensors called “sensor1” and “sensor2,” then you can map the “highsec” and “lowsec” sensors to sensor1 and sensor2 in context A, but map the “medsec” and “lowsec” sensors to sensor1 and sensor2 in context B.
  - Add—Adds a sensor.
  - Delete—Deletes a sensor.
  - Default Sensor—Assigns a default sensor to the security context. If you do not specify a sensor name when you configure IPS within the context configuration, the context uses this default sensor. You can only configure one default sensor per context. If you do not specify a sensor as the default, and the context configuration does not include a sensor name, then traffic uses the default sensor on the AIP SSM.
- Resource Assignment—Assigns the context to a resource class.
  - Resource Class—Select a class from the list.
  - Edit—Edits the selected resource class.
  - New—Adds a resource class.
- Config URL—Specifies the context configuration location, as a URL. Choose the file system type in the list, and then enter the server (for remote file systems), path, and filename in the field. For example, the combined URL for FTP has the following format:  
`ftp://server.example.com/configs/admin.cfg`
- Login—Sets the username and password for remote file systems.
- Failover Group—Sets the failover group for active/active failover.
- Description—Sets an optional description for the context.

**Modes**

The following table shows the modes in which this feature is available:

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

**Add/Edit Interface Allocation****Fields**

- Interfaces—Specifies the physical interface and subinterface IDs.
  - Physical Interface—Sets the physical interface to assign to the context. You can assign the main interface, in which case you leave the subinterface ID blank, or you can assign a subinterface or a range of subinterfaces associated with this interface. In transparent firewall mode, only interfaces that have not been allocated to other contexts are shown. If the main interface was already assigned to another context, then you must choose a subinterface.
  - Sub Interface Range (Optional)—Sets the subinterface ID or a range of subinterface IDs. To specify a single subinterface, choose the ID in the first list. To specify a range, choose the ending ID in the second list, if available. In transparent firewall mode, only subinterfaces that have not been allocated to other contexts are shown.
- Aliased Names—Sets an aliased name for this interface to be used in the context configuration instead of the interface ID.
  - Use Aliased Name in Context—Enables aliased names in the context.
  - Name—Sets the aliased name. An aliased name must start with a letter, end with a letter, and have as interior characters only letters, digits, or an underscore. This field lets you specify a name that ends with a letter or underscore; to add an optional digit after the name, set the digit in the Range field.
  - Range—Sets the numeric suffix for the aliased name. If you have a range of subinterfaces, you can enter a range of digits to be appended to the name.
- Show Hardware Properties in Context—Enables context users to see physical interface properties even if you set an aliased name.

**Modes**

The following table shows the modes in which this feature is available:

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