This study aid describes the purpose of security contexts and explains how to enable, configure, and manage multiple contexts.

Security Context Overview

This topic provides an overview of security contexts.

You can partition a single security appliance into multiple virtual firewalls, known as security contexts. Each context has its own configuration that identifies the security policy, interfaces, and almost all the options you can configure on a standalone firewall. The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the security appliance. When the system needs to access network resources, it uses one of the contexts that is designated as the admin context. VPN and dynamic routing protocols are not supported.

You can partition a single security appliance into multiple virtual firewalls, known as security contexts. Each context is an independent firewall, with its own security policy, interfaces, and administrators. Having multiple contexts is similar to having multiple standalone firewalls. Each context has its own configuration that identifies the security policy, interfaces, and almost all the options you can configure on a standalone firewall. If desired, you can allow individual context administrators to implement the security policy on a context. Some resources are controlled by the overall system administrator, such as VLANs and system resources, so that one context cannot affect other contexts inadvertently.

The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the security appliance. The system administrator has privileges to manage all contexts. 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 into the admin context, that user has system administrator rights and can access the system execution space and all other contexts. Typically, the admin context provides network access to network-wide resources, such as a syslog server or context configuration server.
You might want to use multiple security contexts in the following situations:

- You are a service provider and want to sell firewall services to many customers.
- 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 a network that requires more than one firewall.
In this example, a service provider is using a single security appliance divided into multiple contexts to deliver the same service as multiple stand-alone small security appliances. By enabling multiple security contexts on the security appliance, the service provider can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
Packet Classification

Each packet that enters the security appliance must be classified so that the security appliance can determine to which context to send a packet. The security appliance checks for the following characteristics:

- Unique interfaces
- MAC addresses
- NAT configuration (IP address)

The security appliance uses the characteristic that is unique and not shared across contexts.

- Routed mode allows shared interfaces
- Transparent mode does not allow shared interfaces.

In multicontext mode, you can map one physical interface to only one context interface when physical interface isolation from other contexts is required. You can also map one physical interface to several context interfaces so the contexts share a single physical interface. This might be practical in enterprise environment where each context is designated to a different department. Most likely, the enterprise will have a single path to the Internet and every department will share that path, provided by one physical interface. And in most cases, the inside interfaces are not shared because inside networks tend to be isolated and protected from every other network.

When a security appliance is in multicontext mode, a classifier is used to sort out which context should actually process each inbound packet. A classifier works in only one direction.

In classifying the packets, the security appliance uses the characteristic of each packet that is unique and not shared across contexts. The security appliance classifier uses the following criteria to classify packets:

- **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, the classifier uses the interface MAC address. You can 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 different contexts without unique MAC addresses. You can set the MAC addresses manually when you configure each interface, or you can automatically generate MAC addresses.
Network Address Translation (NAT) configuration: If multiple contexts share an interface and you do not configure unique MAC addresses, 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 of the subnets located behind each security context. The classifier relies on the NAT configuration to determine the subnets in each context; it matches the destination IP address to either a global IP address configured in a static NAT entry or found in the xlate table.

The recommended method is that you use unique MAC addresses if you plan to share an outside interface. In the figure, three contexts share the security appliance outside interface and the MAC address for each context is unique. Therefore, the security appliance uses the MAC address to determine where to send the inbound packet.
Classification via MAC Address

The classifier assigns the packet to Context B because Context B includes the MAC address to which the router sends the packet to.

The figure shows an example of packet classification using unique MAC address on a shared outside interface. Each context will have an unique IP address from the same shared subnet and each context is assigned an unique MAC address. In this example, the incoming packet destined for 172.19.6.7 behind Context B is sent from the upstream router to the security appliance using the 000c.f142.4cdc MAC address. The classifier assigns the packet to Context B because Context B uses that MAC address to which the upstream router sends the packet.

Note
If the inbound packet destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each context.
Classification via NAT Configuration

The classifier assigns the packet to Context B because Context B includes the address translation that matches the destination address.

Customer A
10.3.4.5 Translated to 172.19.3.4

Customer B
10.2.2.3 Translated to 172.19.2.4

Customer C
10.3.4.5 Translated to 172.19.3.4

Customer C
10.4.6.7 Translated to 172.19.4.4

This figure shows an example of multiple contexts sharing an outside interface without unique MAC addresses assigned to each context. In this example, the incoming packet destined for 172.19.3.4 is sent from the upstream router to the security appliance using the 000c.f142.aaaa MAC address which is shared by all three contexts. The classifier will not know which context to forward the packet to based on the MAC address. In this case, the security appliance is configured to perform static NAT to translate the inside source IP address behind each context. The classifier assigns the packet to Context B because Context B includes the static network address translation that matches the destination IP address (172.19.3.4). The security appliance is configured to statically translate the inside host 10.3.4.5 IP address behind Context B to the 172.19.3.4 IP address.
Enabling Multiple Context Mode

This topic describes how to enable multiple contexts on the security appliance.

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, so it differs from the running configuration. You should back up the startup configuration before converting to multiple mode. The security appliance automatically adds an entry for the admin context to the system configuration with the name "admin." The `show flash` command output below shows the old_running.cfg file and the configuration file for the admin context, admin.cfg being stored in flash once the security appliance converted to multicontext mode.

```
asaP# show flash
-#- -- length-- ----date/time-------- path
 6  14524416  Dec 06 2007 19:18:52 asa802-k8.bin
 7    5546    Jan 28 2008 08:30:43 old_running.cfg
 9    3525    Jan 28 2008 08:30:45 admin.cfg
```
Context Configuration Files

Context configuration files have the following characteristics:

- Each context has its own configuration file.
- The security appliance also includes a system configuration that identifies basic settings for the security appliance, including a list of contexts.

The security appliance houses the system configuration, admin context, and optional additional contexts. The system configuration identifies basic settings for the security appliance, including a list of contexts, interfaces allocated to each context, and individual context configuration storage location. It is the startup configuration for the multimode security appliance. Resources are defined and allocated in the system configuration. In the following example, the `show context` command output indicates the system configuration has two contexts defined, the admin and the Context A context.

```
asal# show context
Context Name Class    Interfaces          URL
*admin       default  GigabitEthernet0/0  disk0:/admin.cfg
               GigabitEthernet0/1
contextA     default  GigabitEthernet0/2  disk0:/contextA.cfg
               GigabitEthernet0/3

Total active Security Contexts: 2
```

The system configuration is the startup configuration for a security appliance running in multiple mode. Like the single-mode configuration, the multiple-mode system configuration resides as the startup configuration in the flash memory partition.
Individual context configurations are stored on the local disk partition on the flash memory card, or you can download them from a TFTP, FTP, or HTTPS server. Individual context configuration parameters are written to these individual cfg files. As shown in the example above and in the `show flash` command output below, Context A configuration parameters are written to the contextA.cfg file in flash (disk0) of the security appliance.

```
asap# show flash
-#-  -- length-- ----date/time---------- path
 6    14524416 Dec 06 2007 08:30:29 asa802-k8.bin
 7    5546 Jan 28 2008 08:30:43 old_running.cfg
 9    3625 Jan 28 2008 08:30:45 admin.cfg
10    1714 Jan 28 2008 09:46:41 contextA.cfg
```

Each context has its own configuration file that identifies the security policy, interfaces, and almost all the options you can configure on a standalone firewall. The following example shows the configuration of interface g0/3 for asa1, contextA. (Note that the command line prompt indicates the context name after the hostname when in context configuration mode.)

```
asal/contextA(config)# show run interface
!
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.0.2.1 255.255.255.0
```
The Admin Context

The admin context has the following characteristics:

- The system configuration has no traffic-passing interfaces, and uses the policies and interfaces of the admin context to communicate with other devices.
- Used to fetch configurations for other contexts and send system-level syslogs.
- Users logged in to the admin context are able to change to the system configuration and create new contexts.
- Aside from its significance to the system, it could be used as a regular context.

The system configuration does not include any network interfaces or network settings for itself; instead, when the system needs to access network resources, it uses one of the contexts that are designated as the admin context. If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically and its configuration is stored in the admin.cfg file on flash.

The admin context has the following characteristics:

- The system configuration has no traffic-passing interfaces, and uses the policies and interfaces of the admin context to communicate with other devices.
- The admin context is used to retrieve configurations for other contexts and send system-level syslogs.
- Users logged in to the admin context are able to change to the system configuration and create new contexts.
- Aside from its significance to the system, it could be used as a regular context.
Enabling and Disabling Multiple Context Mode

ciscoasa(config)#

mode {single | multiple} [noconfirm]

- Selects the context mode as follows:
  - multiple: Sets multiple context mode (mode with security contexts)
  - single: Sets single context mode (mode without security contexts)
  - noconfirm: Sets the mode without prompting you for confirmation

When you change the context mode using the mode command, you are prompted to reboot.

To set the security context mode to single or multiple, use the mode command in global configuration mode. In single mode, the security appliance has a single configuration and behaves as a single device. In multiple mode, you can create multiple contexts, each with its own configuration. The number of contexts allowed depends on your license.

When converting from single mode to multiple mode, some of the configurations (like interface configurations and etc.) are automatically imported to the admin context configuration from the single mode configuration. After you enable multiple mode at the CLI, you can use Cisco ASDM to create security contexts.

When converting from multiple mode to single mode, the single mode startup configuration inherited from the system configuration in multiple mode is not a complete functioning configuration for a single mode device. Copy a full single-mode startup configuration (if available) to the security appliance after the security appliance reboots into single mode.

Note: The security appliance needs to reboot whenever you change the mode.
In Cisco ASDM, you can verify the security appliance context mode on the General tab of the Device Dashboard within a context. Context Mode changes from "Single" to "Multiple." The administrator can ease migrating between contexts by enabling the device list (seen on following page). The device list is available under the View > Device drop-down menu.
When you convert the security appliance to multiple mode, the device list displays the system configuration icon and the admin context. As you create contexts, they, too, are displayed in the device list.
Configuring Security Contexts

This topic describes how to configure a security context.

Context Configuration Tasks

- Create a name for the context.
- Allocate interfaces to the context.
- Specify the location of the context startup configuration.
- (Optional) Assign resources to the context.
- (Optional) Assign an IPS virtual sensor to the context.
- (Optional) Assign MAC addresses to context interfaces.

After you enable multiple mode at the CLI, you can use Cisco ASDM to create security contexts. If you do not have an admin context (for example, if you clear the configuration), the first context you add must be the admin context. After you create the admin context, you can create other contexts.

To create and configure security contexts, perform the following tasks:

- Create a context name.
- Allocate interfaces to the context.
- Specify, as a URL, the location of the context startup configuration.
- (Optional) Assign resources to the context.
- (Optional) Assign an IPS virtual sensor to the context.
- (Optional) Assign MAC addresses to context interfaces.
Initially, a new context has no access to security appliance interfaces; you must assign interfaces to the context.

Before traffic can pass through the context interface, you must enable the physical interface in the system configuration.

In routed mode, you can assign the same interfaces to multiple contexts.

The system configuration is the startup configuration for a multiple mode security appliance. Security contexts must be created and configured in the system configuration. If you allocate an interface to a context, the interface is enabled by default in the context. However, before traffic can pass through the context interface, you must enable the physical interface in the system configuration.

A context can use physical interfaces or subinterfaces. In transparent firewall mode, you can only use two interfaces per context. If your security appliance model includes a management interface, you can configure that interface for management traffic in addition to two network interfaces. You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.
Specify the Location of the Context Startup Configuration

- Each context has its own configuration file.
- Until you specify the location of the context startup configuration, the context is not operational.
- The location is specified as a URL.
- You can specify the following URL types:
  - disk0/flash: Configurations stored on the flash file system of the device
  - disk1: Configurations stored on the compact flash memory card of the device
  - tftp: TFTP server-based configurations
  - ftp: FTP server-based configurations
  - https: Webserver-based configurations (read-only)

Each context on the security appliance has its own configuration file. Until you specify the location of the context configuration file, the context is not operational. You must specify the location as a URL. A remote URL must be accessible from the admin context. Use one of the following URL types with the syntax shown:

- **disk0:⌈path⌉filename**
  For the Cisco ASA 5500 series adaptive security appliance, this URL indicates the internal Flash memory. You can also use flash instead of disk0; they are aliased.

- **disk1:⌈path⌉filename**
  For the Cisco ASA 5500 series adaptive security appliance, this URL indicates the external Flash memory card.

- **flash:⌈path⌉filename**
  This URL indicates the internal Flash memory.

- **ftp:⌈user:@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

- **http[s]:⌈user:@server:[port]⌈path⌉filename**

- **tftp:⌈user:@server:[port]⌈path⌉filename:[int=interface_name]**

Specify the interface name if you want to override the route to the server address.

**Note** The admin context file must be stored on the flash memory DIMM.
When you add a context URL, the system immediately loads and runs the context. If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure.

If you change a context URL, the security appliance merges the new configuration from the configuration file in the new URL location with the current 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, the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then load the new configuration from the new URL. If the running configuration is blank, the new configuration is used.

Re-entering the same URL also merges the saved configuration from the configuration file in the URL location with the running configuration.
To create a security context, complete the following steps:

**Step 1** Choose **Security Contexts** from the Context Management menu. The Security Contexts panel is displayed.

**Step 2** Click **Add**. The Add Context window opens.

As shown in the figure, the security appliance currently has only the admin context configured. The admin context is using the default resource class and has three interfaces allocated. Its config URL is disk0:/admin.cfg.
In the Add Context configuration window, define the new context name, allocate interfaces to the context, define the resource class (covered later), and specify the config URL for the context.

**Step 3** In the Security Context field, enter the context name as a string up to 32 characters long. The name is case sensitive. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. The names “System” and “Null” (in upper- or lowercase letters) are reserved names and cannot be used. In the figure, the name contextA is entered.

**Step 4** In the Interface Allocation area, click **Add** to assign an interface to the context. The Add Interface Allocation window opens. This window enables you to assign the physical interface to the context and optionally assign an alias (mapped name) name to the interface.

**Step 5** From the Physical Interface drop-down list, choose an 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, you must choose a subinterface. In the figure, GigabitEthernet0/0 is chosen.

**Step 6** (Optional) From the 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 the Use Aliased Name in Context check box to set an aliased name for this interface. This name will be used in the context configuration instead of the interface ID. If you enable this option, enter the aliased name in the Name field. An aliased name must start with a letter, end with a letter, and have as interior characters only letters, digits, or an underscore. To add an optional digit after the name, set the digit in the Range field. 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 the Show Hardware Properties in Context check box.

Step 9  Click OK. The Add Context window becomes active.

Step 10  (Optional) To assign a resource class to the context, choose a class name from the Resource Class drop-down list. In the figure, the class MEDIUM-RESOURCE-SET is chosen.

Step 11  To set the context configuration location, choose a file system type from the Config URL drop-down list and enter a path in the field. The filename does not require a file extension, although ".cfg" is recommended. In the figure, /CONTEXT1.cfg is entered.

Step 12  (Optional) For external file systems, set the username and password by clicking Login.

Step 13  (Optional) To set the failover group for active/active failover, choose the group name from the Failover Group drop-down list. Failover is discussed in another lesson.

Step 14  (Optional) Add a description in the Description field.

Step 15  Click OK.

Step 16  Click Apply in the Security Contexts panel.

---

Note  If you use IPS virtual sensors, you can assign a sensor to the context in the IPS Sensor Allocation area. For detailed information about IPS and virtual sensors, refer to the "Configuring IPS" section of the Cisco ASDM 6.0 User Guide on Cisco.com.
As explained earlier in this study aid, each packet that enters the security appliance must be classified so that the security appliance can determine to which context to send a packet. Classification is simple if only one context is associated with the ingress interface; the security appliance classifies the packet into that context. However, classification is more complicated when contexts share an interface. One of the methods that can be used for packet classification in this situation is the MAC address method. You can assign a different MAC address to each context that shares an interface to enable MAC address classification.

The default MAC address in a security appliance is the burned-in MAC address of the physical interface. Subinterfaces inherit the physical interface MAC address. You can enable automatic MAC address assignment by checking the Mac-Address Auto check box in the Configurations > Context Management > Security Contexts panel as shown in the figure. This causes the security appliance to automatically assign private MAC addresses to each shared context interface.

In the rare circumstance that the automatically generated MAC address conflicts with another private MAC address in your network, you can manually set different MAC addresses for the contexts that are sharing an interface. Manual configuration of the MAC address on the shared interface within each context can be done by using Cisco ASDM or by using the `mac-address` command in interface configuration mode within each context. The `mac-address` command works for physical interfaces and subinterfaces.
The running configuration that you edit via the Cisco ASDM Configuration menus 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.

After the context has been activated, it is configured much the same as any security appliance standalone device, as illustrated in the interface configuration shown in the figure. Individual device configuration changes made in the context are stored in the configuration file specified by the `config-url` command for that context. The location of the startup configuration file cannot be changed or viewed from within the context.

You can use the `write memory all` command in the system execution space to save all context configurations, including the system configuration at the same time. After the security appliance saves your contexts, it displays a message indicating how many contexts were saved. Sometimes a context is not saved, and one of the following error messages is displayed:

- The context 'CONTEXTX' could not be saved due to Unavailability of resources: This message is displayed when the security appliance memory is low.
- The context 'CONTEXTX' could not be saved due to non-reachability of destination: This message is displayed when the remote destination is unreachable.
- Unable to save the configuration for the following contexts as these contexts are locked—context 'X', context 'Y', context 'Z': This message is displayed when the context is locked.

Note: A context is only locked if another user is already saving the configuration or is in the process of deleting the context.
Unable to save the configuration for the following contexts as these contexts have read-only config-urls—context 'X', context 'Y', context 'Z': This message is displayed when the startup configuration is read-only. This message report is printed at the end of all other messages.

The context 'CONTEXTX' could not be saved due to Unknown errors: This message is displayed when contexts are not saved because of bad sectors in the flash memory.
Resource Management

- Limits the use of resources per context
- Prevents one or more contexts from using too many resources and causing other contexts to be denied the use of resources
- Enables you to configure limits for the following resources:
  - ASDM connections
  - Connections
  - Hosts
  - SSH sessions
  - Telnet sessions
  - Xlate objects
  - Application inspections (rate only)
  - Syslogs per second (rate only)

By default, all security contexts have unlimited access to the resources of the security appliance. Sometimes certain contexts utilize resources to the point of potentially affecting service to other contexts. You can configure resource management to limit the use of resources by any given context.

The security appliance manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class. You can configure limits for the following resources:

- **ASDM**: ASDM sessions. The system limit is 32. There is also a limit of five Cisco ASDM sessions per context.

  **Note**: Cisco 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, 32 Cisco ASDM sessions represent a limit of 64 HTTPS sessions.

- **Connections**: TCP or User Datagram Protocol (UDP) connections between any two hosts, including connections between one host and multiple other hosts. You can also set the rate per second for this resource. The system connection limits vary among security appliance platforms, but there is no system limit on the rate.

- **Hosts**: Hosts that can connect through the security appliance. There is no system limit.

- **SSH**: Secure Shell (SSH) sessions. The system limit is 100. There is also a limit of five SSH sessions per context.

- **Telnet**: Telnet sessions. The system limit is 100. There is also a limit of five Telnet sessions per context.

- **Xlate objects**: Address translations. There is no system limit.

- **Inspects**: Rate of application inspections per second. There is no system limit.
- **Syslogs**: Rate of system log messages per second. There is no system limit.
- **MAC addresses**: For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. The system limit is 65,535.

You can set the limit for an individual resource as an absolute value or as a percentage. However, for resources that do not have a system limit, you cannot set the percentage; you can only set an absolute value. If you assign an absolute value to a resource across all contexts that exceed the practical limit of the security appliance, the performance of the security appliance might be impaired.

You can 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.
All contexts belong to the default class if they are not assigned to another resource 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, the context member uses the default class for those limits.

For example, if you create a class with a two percent limit for all concurrent connections, but you set no other limits, 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 Telnet, SSH, and Cisco ASDM sessions, which are set to the maximum of five sessions allowed per context. You can change the default class settings.

The figure shows the relationship between the default class and other classes. CONTEXT A and C belong to classes with some limits configured; other limits are inherited from the default class. CONTEXT B inherits no limits from the default class because all limits are set in its class, the GOLD class. Context D is not assigned to a class and is, by default, a member of the default class.
If you plan to configure resource management, begin by configuring resource classes. Complete the following steps to use Cisco ASDM to configure resource classes:

**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** Click the Configuration button in the Cisco ASDM toolbar.

**Step 3** Click **Context Management** in the navigation pane.

**Step 4** Choose **Resource Class** from the Context Management menu. The Resource Class panel is displayed.

**Step 5** Click **Add**. The Add Resource Class window opens.

From this configuration window, the default resource class settings can be examined or edited also.
From the Add Resource Class configuration window, define the name of the new resource class and the resource limits:

**Step 6**  
In the Resource Class field, enter a class name up to 20 characters in length. In the figure, the name MEDIUM-RESOURCE-SET is entered.

**Step 7**  
In the Count Limited Resources area, set the resources limits for the resource class. These limits override the default resource class limits. Any limits not specified will be inherited from the default resource class. You can set one or more of the following limits:

- **ASDM Sessions**: Sets the limit for concurrent Cisco 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 Cisco ASDM sessions represents a limit of 64 HTTPS sessions, divided between all contexts. In the figure, Cisco ASDM sessions are limited to four sessions.

- **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. In the figure, connections for this resource class are limited to 20 percent.
Hosts: Specifies the number of hosts that can simultaneously connect through the security appliance. Select the check box to enable this limit. There is no system limit. If you set the limit to 0, it is unlimited. In the figure, the hosts limit is not set so it will be inherited from the default resource class.

Xlates: Sets the limit for address translations. Select the check box to enable this limit. There is no system limit. If you set the limit to 0, it is unlimited. In the figure, the xlates limit is not set so it will be inherited from the default resource class.

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. In the figure, Telnet sessions are limited to five.

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 drop-down 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 drop-down list. The system has a maximum of 100 sessions divided between all contexts. In the figure, SSH sessions are limited to five.

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 drop-down list. You can assign more than 100 percent if you want to oversubscribe the device. You can also set the limit as an absolute value by entering an integer between 0 and 65535 and selecting Absolute from the drop-down list.

Step 8 In the Rate Limited Resources area, set the rate limit for resources. These limits override the default resource class limits. Any limits not specified will use the value from the default resource class. In the figure, the rate limits are not set so the limits will be inherited from the default resource class. If the default class does not set a limit, 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.
- **Inspects/sec**: Sets the limit for application inspections per second. Select the check box to enable this limit. There is no system 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. There is no system limit. If you set the limit to 0, it is unlimited.

Step 9 Click **OK**.

Step 10 Click **Apply**.

**Note** From the Edit Resource Class configuration window (not shown in the figure), selecting **Show Actual Class Limits** will show the limits inherited from the default resource class.
Managing Security Contexts
This topic describes how security contexts are managed.

In Cisco ASDM, use the Device List to move between contexts. You can move from one context to another by simply double-clicking the context to which you want to move.
From the Cisco ASDM Monitoring menus, you can monitor the following features for each context:

- Interfaces
- Content security and control (CSC)
- Routing
- Properties
- Logging
To monitor resource usage of all contexts from the system execution space, complete 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.

Step 4 Click the resource type to view the resource usage for all contexts. You can view resource usage for the following resource types:

- **ASDM**: Usage of Cisco ASDM connections. The Cisco ASDM panel displays the following information about Cisco ASDM connections for each context.
  - **Existing Connections (#)**: Number of existing connections
  - **Existing Connections (%)**: Connections used by this context as a percentage of the total number of connections used by all contexts
  - **Peak Connections (#)**: Peak number of connections since the statistics were last cleared, either using the clear resource usage command or because the device rebooted

- **Telnet**: Usage of Telnet connections. The Telnet panel displays the following information about Telnet connections for each context:
  - **Existing Connections (#)**: Number of existing connections
  - **Existing Connections (%)**: Connections used by this context as a percentage of the total number of connections used by all contexts
  - **Peak Connections (#)**: Peak number of connections since the statistics were last cleared, either using the clear resource usage command or because the device rebooted
SSH: Usage of SSH connections. The SSH panel displays the following information about SSH connections for each context:

- **Existing Connections (#)**: Number of existing connections
- **Existing Connections (%)**: Connections used by this context as a percentage of the total number of connections used by all contexts
- **Peak Connections (#)**: Peak number of connections since the statistics were last cleared, either using the clear resource usage command or because the device rebooted

Xlates: Usage of network address translations. The Xlates panel displays the following information about address translations for each context:

- **Xlates (#)**: Number of current xlates
- **Xlates (%)**: Xlates used by this context as a percentage of the total number of xlates used by all contexts
- **Peak (#)**: Peak number of xlates since the statistics were last cleared, either using the clear resource usage command or because the device rebooted

NATs: Number of NAT rules. The NAT panel displays the following information about NAT rules for each context:

- **NATs (#)**: Current number of NAT rules
- **NATs (%)**: NAT rules used by this context as a percentage of the total number of NAT rules used by all contexts
- **Peak NATs (#)**: Peak number of NAT rules since the statistics were last cleared, either using the clear resource usage command or because the device rebooted

Syslogs: Rate of system log messages. The Syslogs panel displays the following information about Syslog messages for each context:

- **Syslog Rate (#/sec)**: Current rate of system log messages
- **Syslog Rate (%)**: 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)**: 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 5 Click **Refresh** to refresh the view.

The figure shows the SSH panel, which displays usage of SSH connections for each context. Statistics are shown for CONTEXT1, CONTEXT2, and the admin context.

In this example, CONTEXT1 has five existing connections, which make up 100 percent of the total number of SSH connections used by all contexts. The peak number of connections since the statistics were last cleared is 64.
Removing a Security Context

You can only remove a context by editing the system configuration. To use Cisco ASDM to remove a context, complete the following steps:

**Step 1**  
From the system configuration, click **Configuration** in the Cisco ASDM toolbar.

**Step 2**  
Choose **Context Management** from the navigation pane.

**Step 3**  
Choose **Security Contexts** from the Context Management menu. The Security Contexts panel is displayed.

**Step 4**  
Select the context you want to delete.

**Step 5**  
Click **Delete**.

**Step 6**  
Click **Apply**.

You cannot remove the current admin context unless you remove all contexts. To clear all context configurations in the system configuration, you can use the `clear configure context` CLI command in global configuration mode. Contexts can be created or removed without a reboot.