



## Virtualization Commands on the Virtual Firewall

---

You can operate your VFW application in a single context or in multiple contexts. Multiple contexts use the concept of virtualization to partition your VFW application into multiple virtual devices or contexts. Each context contains its own set of policies, interfaces, resources, and administrators. Virtualization commands provide you with the tools to more closely and efficiently manage the system resources and users of the VFW application, and the services you provide to your customers.



### Note

---

The commands described in this module are SanOS (Linux) commands used on the VFW application. Before you can access any of these commands, you must attach from the route processor to the VFW application using the **service firewall attach location** command. For more information, see the [“Attaching to the VFW Application”](#) section in *Cisco IOS XR Virtual Firewall Configuration Guide*.

---

# add-object

To associate a configuration object with a domain, use the **add-object** command in domain configuration mode. To remove an object added to the domain, use the **no** form of this command.

```
add-object { access-list extended | all | class-map | interface | parameter-map | policy-map }
           name
```

```
no add-object { access-list extended | all | class-map | interface | parameter-map | policy-map }
           name
```

## Syntax Description

<b>access-list extended</b>	Specifies an existing extended access control list that you want to associate with the domain.
<b>all</b>	Specifies that all configuration objects in the context are added to the domain.
<b>class-map</b>	Specifies an existing class map for flow classification that you want to associate with the domain.
<b>interface</b>	Specifies an existing interface that you want to associate with the domain.
<b>parameter-map</b>	Specifies an existing parameter map that you want to associate with the domain.
<b>policy-map</b>	Specifies an existing policy map that you want to associate with the domain.
<i>name</i>	Identifier of the specified object. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

## Defaults

No default behavior or values

## Command Modes

Domain configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

After you have created a domain, you can associate configurable objects with that domain (for example, an interface). To associate a configurable object with a domain, use the **add-object** command in domain configuration mode.

---

**Examples**

The following example shows how to associate an interface called xyz with a domain D1:

```
firewall/Admin(config)# domain D1  
firewall/Admin(config-domain)# add-object interface xyz
```

---

**Related Commands**

Command	Description
<a href="#">domain</a>	Creates a domain and enters domain configuration mode.
<a href="#">show domain</a>	Displays the information about the configured domains in the VFW application.

# changeto

To move from one context on the VFW application to another, use the **changeto** command in EXEC mode.

**changeto** *context\_name*

## Syntax Description

<i>context_name</i>	Name of an existing context. This argument is case-sensitive.
---------------------	---

## Defaults

No default behavior or values

## Command Modes

EXEC

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the **changeto** feature in your user role (as found in all the predefined user roles). For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Only users authorized in the Admin context can use the **changeto** command to navigate between the various contexts. Context administrators, who have access to multiple contexts, must explicitly log in to the other contexts to which they have access.

The command prompt indicates the context you are currently in (see the following example).

## Examples

The following example shows how to change from the Admin context to the context CTX1:

```
firewall/Admin# changeto CTX1
firewall/CTX1#
```

## Related Commands

Command	Description
<a href="#">context</a>	Creates a context.
<a href="#">show context</a>	Displays the context configuration information.

# clear user

To clear a user session, use the **clear user** command in EXEC mode.

**clear user** *name*

<b>Syntax Description</b>	<i>name</i> Name of the user to log out.
---------------------------	--

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

<b>Usage Guidelines</b>	<p>This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the <a href="#">“Configuring Virtualization on the Virtual Firewall”</a> module in <i>Cisco IOS XR Virtual Firewall Configuration Guide</i>.</p> <p>To display the list of users that are currently logged in to the VFW application, use the <a href="#">show users</a> command.</p>
-------------------------	--

<b>Examples</b>	<p>The following example shows how to log out the user USER1:</p> <pre>firewall/Admin# clear user USER1</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.
	<a href="#">username</a>	Defines a user and its associated password, role, and domain.

# context

To create a context, use the **context** command in configuration mode. To remove a context, use the **no** form of this command.

**context** *name*

**no context** *name*

## Syntax Description

<b>name</b>	Name that designates a context. Enter an unquoted text string with no spaces and a maximum of 64 characters.
-------------	--

## Defaults

No default behavior or values

## Command Modes

Configuration  
Admin context only

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **context** command to create a context. The CLI prompt changes to (config-context). A context provides a user view into the VFW application and determines the resources available to a user.

By default, the VFW application allows you to create and use five user-configured contexts plus the default admin context. To use a maximum of 251 contexts (admin context plus 250 user contexts), you must purchase an additional license from Cisco Systems.

## Examples

The following example shows how to create a context called C1:

```
firewall/Admin(config)# context C1
firewall/Admin(config-context)#
```

Related Commands	Command	Description
	<a href="#">changeto</a>	Moves from one context on the VFW application to another.
	<a href="#">show context</a>	Displays the context configuration information.
	<a href="#">show user-account</a>	Displays user account information.
	<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.

## description (context)

To enter a description for a role or context, use the description command in the appropriate configuration mode. To remove the role description from the configuration, use the **no** form of this command.

**description** *text*

**no description**

### Syntax Description

<i>text</i>	Description of the role. Enter a description as an unquoted text string with a maximum of 256 characters.
-------------	---

### Defaults

No default behavior or values

### Command Modes

Context configuration  
Role configuration

### Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

### Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

This command has no usage guidelines.

### Examples

The following example shows how to provide additional description about a role:

```
firewall/C1(config-role)# description DEFINES TECHNICIAN ROLE
```

The following example shows how to remove the description from the configuration:

```
firewall/C1(config)# no description DEFINES TECHNICIAN ROLE
```

### Related Commands

This command has no related commands.

# domain

To create a domain and access domain configuration mode, use the **domain** command in configuration mode. To remove a domain from the configuration, use the **no** form of this command.

**domain** *name*

**no domain** *name*

## Syntax Description

<i>name</i>	Unique identifier of a domain in a context. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
-------------	---

## Defaults

No default behavior or values

## Command Modes

Configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

A domain does not restrict the context configuration that you can display using the **show running-config** command. You can still display the running configuration for the entire context. However, a domain can restrict your access to the configurable objects within a context by adding to the domain only a limited subset of all the objects available to a context.

## Examples

The following example shows how to create a domain named D1 and access domain configuration mode:

```
firewall/Admin(config)# domain D1
firewall/Admin(config-domain)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show domain</a>	Displays the information about the configured domains in the VFW application.
<a href="#">show running-config</a>	Displays the running configuration information associated with the current context.

# member

To associate a context with a resource class, use the **member** command in context configuration mode. To remove a context from a resource class, use the **no member** form of this command.

**member** *class*

**no member** *class*

## Syntax Description

<i>class</i>	Name of an existing resource class. Enter the class name as an unquoted text string with a maximum of 64 alphanumeric characters.
--------------	---

## Defaults

No default behavior or values

## Command Modes

Context configuration  
Admin context only

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

You can associate a context with only one resource class. If you do not explicitly associate a context with a resource class, the VFW application associates the context with the default resource class.

## Examples

The following example shows how to disassociate a context from a resource class:

```
firewall/Admin(config-context)# no member RC1
```

## Related Commands

Command	Description
<a href="#">show context</a>	Displays the context configuration information.
<a href="#">resource-class</a>	Creates a resource class and enters resource configuration mode.

# limit-resource

To limit system resources for all members of a resource class, use the **limit-resource** command in resource-class configuration mode. To restore the default resource settings for all resources or individual resources for all members (contexts) of a resource class, use the **no** form of this command.

```
limit-resource { acl-memory | all | buffer { syslog } | conc-connections | mgmt-connections |
proxy-connections | rate { bandwidth | connections | inspect-conn | mgmt-traffic | syslog } |
regex | xlates } { minimum number } { maximum { equal-to-min | unlimited } }
```

```
no limit-resource { acl-memory | all | buffer { syslog } | conc-connections | mgmt-connections |
proxy-connections | rate { bandwidth | connections | inspect-conn | mgmt-traffic | syslog } |
regex | xlates } { minimum number } { maximum { equal-to-min | unlimited } }
```

## Syntax Description

<b>acl-memory</b>	Limits memory allocated for ACLs.
<b>all</b>	Limits all resources to the specified value for all contexts assigned to this resource class.
<b>buffer syslog</b>	Limits the amount of buffering for syslog messages.
<b>conc-connections</b>	Limits the number of simultaneous connections.
<b>mgmt-connections</b>	Limits the number of management connections.
<b>proxy-connections</b>	Limits the number of proxy connections.
<b>rate</b>	Limits the resource as a number per second for: <ul style="list-style-type: none"> <li>• <b>bandwidth</b>—Limits context throughput in bytes per second</li> <li>• <b>connections</b>—Limits the number of connections of any kind per second</li> <li>• <b>inspect conn</b>—Limits the number of application protocol inspection connections per second for FTP and RTSP only</li> <li>• <b>mgmt-traffic</b>—Limits the management traffic in bytes per second</li> <li>• <b>syslog</b>—Limits the number of syslog messages per second</li> </ul>
<b>regex</b>	Limits the amount of regular expression memory.
<b>xlates</b>	Limits the number of network and port address translations entries.
<b>minimum</b> <i>number</i>	Specifies the lowest acceptable value. Enter an integer from 0.00 to 100.00 percent (two-decimal places of granularity). The <i>number</i> argument specifies a percentage value for all contexts that are members of the class. When used with the <b>rate</b> keyword, the <i>number</i> argument specifies a value per second.
<b>maximum</b> { <b>equal-to-min</b>   <b>unlimited</b> }	Specifies the maximum resource value: either the same as the minimum value or no limit.

## Command Modes

Resource configuration  
Admin context only

**Command History**

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

**Usage Guidelines**

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

You can limit all resources or individual resources for all members (contexts) of a resource class. For example, you can limit only concurrent connections or probes or sticky table entries, to name a few.

If you lower the limits for one context (context A) to increase the limits of another context (context B), you may experience a delay in the configuration change. This is because the VFW application does not lower the limits of context A until the resources are no longer being used by the context.

The limit you set for individual resources using the **limit-resource** command overrides the limit you set for all resources using the **limit-resource all** command.

**Examples**

The following example shows how to allocate 20 percent of all resources (minimum and maximum) to all member contexts of the resource class:

```
firewall/C1(config)# resource-class RC1
firewall/C1(config-resource)# limit-resource all minimum 20% maximum equal-to-min
```

The following example shows how to restore resource allocation to the default values of 0 percent minimum and 100 percent maximum for all resources to all member contexts:

```
(config-resource)# no limit-resource all
```

**Related Commands**

Command	Description
<a href="#">resource-class</a>	Creates a resource class and enters resource configuration mode.

# resource-class

To create a resource class and enter resource configuration mode, use the **resource-class** command in configuration mode. To remove the resource-class setting, use the **no** form of this command.

**resource-class** *name*

**no resource-class** *name*

## Syntax Description

<i>name</i>	Name assigned to the resource class. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. You can also use the resource class called <b>default</b> .
-------------	--

## Defaults

No default behavior or values

## Command Modes

Configuration  
Admin context only

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **resource-class** command to create a resource class and enter resource configuration mode. The CLI prompt changes to (config-resource). Use a resource class to allocate and limit system resources among contexts in your VFW application. The default resource class allocates 100 percent of all configurable system resources to each context. By creating a resource class, you can prevent oversubscription by limiting the percentage of resources available to each context. After you create and configure a resource class, use the **member** command in context configuration mode to assign a context to the class.

## Examples

The following example shows how to create a resource-class called RC1:

```
firewall/C1(config)# resource-class RC1
firewall/C1(config-resource)
```

Related Commands	Command	Description
	<a href="#">member</a>	Associates a context with a resource class.
	<a href="#">show resource allocation</a>	Displays the allocation for each resource across all resource classes and class members.
	<a href="#">show resource usage</a>	Displays the resource usage for each context.
	<a href="#">show user-account</a>	Displays user account information.
	<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.

# role

To assign a user role to a user and enter role configuration mode, use the **role** command in configuration mode. To remove the user role assignment, use the **no** form of this command.

**role** *name*

**no role** *name*

## Syntax Description

<i>name</i>	Identifier associated with a user role. Enter an unquoted text string with no spaces and a maximum of 64 characters.
-------------	--

## Defaults

No default behavior or values

## Command Modes

Configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To assign a user role to a user and enter role configuration mode, use the **role** command. User roles determine the privileges a user has, the commands a user can enter, and the actions that a user can perform in a particular context. You can apply the roles you create only in the context in which you create them.

If you do not assign a user role to a new user, the default user role is Network-Monitor. For users that you create in the admin context, the default scope of access is the entire device. For users that you create in other contexts, the default scope of access is the entire context. If you need to restrict a user’s access, you must assign a role-domain pair using the **username** command.

## Examples

The following example shows how to create a role:

```
firewall/C1(config)# role TECHNICIAN
firewall/C1(config-role)#
```

Related Commands	Command	Description
	<a href="#">show role</a>	Displays the configured user roles (predefined and user-configured).
	<a href="#">show user-account</a>	Displays user account information.
	<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.
	<a href="#">username</a>	Defines a user and its associated password, role, and domain.

# rule

To assign privileges on a per-feature basis to a role, use the **rule** command in role configuration mode. You can limit the features that a user has access to and the commands the user can enter for that feature by configuring rules for roles. To remove the rule from a user role, use the **no** form of this command.

```
rule number {permit | deny} {create | modify | debug | monitor} [feature {AAA | access-list | config-copy | connection | fault-tolerant | inspect | interface | nat | syslog}]
```

```
no rule number {permit | deny} {create | modify | debug | monitor} [feature {AAA | access-list | config-copy | connection | fault-tolerant | inspect | interface | nat | syslog}]
```

## Syntax Description

<i>number</i>	Identifier of the rule and order of precedence. Enter a unique integer from 1 to 16. The rule number determines the order in which the VFW application applies the rules, with a higher-numbered rule applied after a lower-numbered rule.
<b>permit</b>	Allows the role to perform the operations defined by the rest of the command keywords.
<b>deny</b>	Disallows the role to perform the operations defined by the rest of the command keywords.
<b>create</b>	Specifies commands for the creation of new objects or the deletion of existing objects (includes <b>modify</b> , <b>debug</b> , and <b>monitor</b> commands).
<b>debug</b>	Specifies commands for debugging problems (includes <b>monitor</b> commands).
<b>modify</b>	Specifies commands for modifying existing configurations (includes <b>debug</b> and <b>monitor</b> commands).
<b>monitor</b>	Specifies commands for monitoring resources an objects ( <b>show</b> commands).
<b>feature</b>	(Optional) Specifies a particular VFW application feature for which you are configuring this rule. The available features are listed below: <ul style="list-style-type: none"> <li>• <b>AAA</b>—Specifies commands for authentication, authorization, and accounting.</li> <li>• <b>access-list</b>—Specifies commands for access control lists (ACLs). Includes ACL configuration, class maps for ACL, policy maps containing ACL class maps.</li> <li>• <b>config-copy</b>—Specifies commands for copying the running-config to the startup-config, startup-config to the running-config, and copying both config files to the flash disk (disk0:) or a remote server.</li> <li>• <b>connection</b>—Specifies commands for network connections.</li> <li>• <b>fault-tolerant</b>—Specifies commands for redundancy.</li> <li>• <b>inspect</b>—Specifies commands for packet inspection used in data-center security.</li> <li>• <b>interface</b>—Specifies all interface commands.</li> <li>• <b>nat</b>—Specifies commands for network address translation (NAT) associated with a class map in a policy map used in data-center security.</li> <li>• <b>syslog</b>—Specifies the system logging facility setup commands.</li> </ul>

**Defaults** No default behavior or values

**Command Modes** Role configuration

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

Use the **rule** command to assign privileges on a per-feature basis to a role. You can limit the features that a user has access to and the commands the user can enter for that feature by configuring rules for roles.

**Examples** The following example shows how to configure a rule that allows a role to create an interface:

```
firewall/C1(config)# role TECHNICIAN
firewall/C1(config-role)# rule 1 permit create interface
```

Related Commands	Command	Description
	<a href="#">show role</a>	Displays the configured user roles (predefined and user-configured).
	<a href="#">show user-account</a>	Displays user account information.
	<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.
	<a href="#">username</a>	Defines a user and its associated password, role, and domain.

# show context

To display the context configuration information, use the **show context** command in EXEC mode.

**show context** [*context\_name* | **Admin**]

Syntax Description	
<i>context_name</i>	(Optional) Name of user-created context. The VFW application displays just the specified context configuration information. The <i>context_name</i> argument is case-sensitive, and is visible only from the admin context.
<b>Admin</b>	(Optional) Displays just the admin context configuration information. This keyword is visible only from the admin context.

Defaults	
	No default behavior or values

Command Modes	
	EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command has no user role feature restrictions. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

The VFW application displays different information for this command depending on the context you are in when executing the command:

- **admin context**—When you are in the admin context and use the **show context** command without specifying a context, the VFW application displays the configuration information for the admin context and all user-created contexts.
- **user-created context**—When you are in a user-created context and execute the **show context** command, the VFW application displays only the configuration information of the current context.

**Examples** The following example shows sample output from the show context command:

```
firewall/Admin# show context

Number of Contexts = 3

Name: Admin , Id: 0
Description:
Resource-class: default
FT Auto-sync running-cfg configured state: enabled
```

```
FT Auto-sync running-cfg actual state: disabled
FT Auto-sync startup-cfg configured state: enabled
FT Auto-sync startup-cfg actual state: disabled
```

```
Name: ctx1 , Id: 1
Description:
Resource-class: default
```

```
Name: ctx2 , Id: 2
Description:
Resource-class: default
```

The following example shows how to display the configuration information for the user context ctx1:

```
firewall/Ctx1# show context ctx1
```

#### Related Commands

Command	Description
<a href="#">changeto</a>	Moves from one context on the VFW application to another.
<a href="#">context</a>	Creates a context.

# show domain

To display the information about the configured domains in the VFW application, use the **show domain** command in EXEC mode.

```
show domain [name]
```

<b>Syntax Description</b>	<i>name</i>	(Optional) Name of an existing context domain. Specify a domain name to display the detailed configuration report relating to just the specified domain.
---------------------------	-------------	--

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

<b>Usage Guidelines</b>	This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the <a href="#">“Configuring Virtualization on the Virtual Firewall”</a> module in <i>Cisco IOS XR Virtual Firewall Configuration Guide</i> .
-------------------------	---

To display the complete domain configuration report that lists all the configured domains, execute the **show domain** command without including the *name* argument.

<b>Examples</b>	The following example shows how to use the <b>show domain</b> command:
-----------------	--

```
firewall/Admin# show domain D1
```

Related Commands	Command	Description
	<a href="#">domain</a>	Creates a domain and enters domain configuration mode.

# show resource allocation

To display the allocation for each resource across all resource classes and class members, use the **show resource allocation** command in EXEC mode.

## show resource allocation

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

The **show resource allocation** command shows the resource allocation, but does not show the actual resources being used. To display information about actual resource usage, use the [show resource usage](#) command.

**Examples** The following example shows how to display the allocation for each resource:

```
firewall/Admin# show resource allocation
```

Related Commands	Command	Description
	<a href="#">show resource usage</a>	Displays the resource usage for each context.

## show resource usage

To display the resource usage for each context, use the **show resource usage** command in EXEC mode.

```
show resource usage [all | [[context name | summary | top number] [resource {acl-memory | all
| conc-connections | mgmt-connections | proxy-connections | rate {bandwidth | connections
| inspect-conn | mac-miss | mgmt-traffic | ssl-connections | syslog} | xlates}]]] [counter [all
| current | denied | peak [count_threshold]]]
```

Syntax	Description
<b>all</b>	(Optional) Displays resource usage for each context individually. This is the default setting.
<b>context</b> <i>context_name</i>	(Optional) Displays resource usage for the specified context. The <i>context_name</i> argument is case-sensitive.
<b>summary</b>	(Optional) Displays total resource usage for all contexts together. For example, the denied column shows the items that have been denied for each context limit.
<b>top</b> <i>number</i>	(Optional) Displays the greatest <i>n</i> users of a single resource arranged from highest to lowest percentage of resources used. You must specify a single resource type and cannot use the <b>resource all</b> keywords with this option.
<b>resource</b>	(Optional) Displays statistics for one of the following specified resources:
<b>acl-memory</b>	Displays ACL memory usage.
<b>all</b>	Displays resource usage for all resources used by the specified context or contexts.
<b>concurrent-connections</b>	Displays resource usage for the number of simultaneous connections.
<b>mgmt-connections</b>	Displays resource usage for the number of management connections.
<b>proxy-connections</b>	Displays resource usage for proxy connections.
<b>rate</b>	Displays the rate per second for the specified connections or syslog messages.
<b>bandwidth</b>	Displays bandwidth in bytes per second.
<b>connections</b>	Displays connections per second.
<b>inspect-conn</b>	Displays RTSP/FTP inspection connections per second.
<b>mac-miss</b>	Displays mac miss traffic punted to CP packets per second.
<b>mgmt-traffic</b>	Displays management traffic bytes per second.
<b>ssl-connections</b>	Displays SSL connections.
<b>syslog</b>	Displays syslog message buffer usage.
<b>ssl-connections</b>	Displays resource usage for Secure Sockets Layer connections.
<b>xlates</b>	Displays resource usage by NAT and PAT entries.
<b>counter</b>	(Optional) Specifies one of the following keywords as the counter name:
<b>all</b>	(Optional) Displays all statistics. This is the default setting.
<b>current</b>	(Optional) Displays the active concurrent instances or the current rate of the resource.
<b>denied</b>	(Optional) Displays the number of denied uses of the resource, since the resource statistics were last cleared.

<b>peak</b>	(Optional) Displays the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the <b>clear resource usage</b> command or because the device rebooted.
<i>count_threshold</i>	(Optional) Number above which resources are shown. Enter an integer from 0 to 4294967295. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify <b>all</b> for the counter name, then the <i>count_threshold</i> applies to the current usage. To show all resources, set the <i>count_threshold</i> to <b>0</b> .

**Defaults**

No default behavior or values

**Command Modes**

EXEC

Admin context

**Command History**

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

**Usage Guidelines**

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

You must be in the admin context to use the **show resource usage** command.

**Examples**

The following example shows how to display the resource usage for context C1:

```
firewall/Admin# show resource usage context C1 resource
```

**Related Commands**

Command	Description
<a href="#">show resource allocation</a>	Displays the allocation for each resource across all resource classes and class members.

# show role

To display the configured user roles (predefined and user-configured), use the **show role** command in EXEC mode.

```
show role [role_name]
```

<b>Syntax Description</b>	<i>role_name</i> (Optional) Name of an existing role.
---------------------------	---

<b>Defaults</b>	No default behavior or values
-----------------	-------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

<b>Usage Guidelines</b>	This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the <a href="#">“Configuring Virtualization on the Virtual Firewall”</a> module in <i>Cisco IOS XR Virtual Firewall Configuration Guide</i> .
-------------------------	---

To configure roles, use the **role** command in configuration mode.

<b>Examples</b>	The following example shows sample output from the <b>show role</b> command:
-----------------	--

```
firewall/Admin# show role

Role: Admin (System-defined)
Description: Administrator
Number of rules: 4
-----
Rule    Type    Permission    Feature
-----
 1.    Permit    Create        all
 2.    Permit    Create        user access
 3.    Permit    Create        system
 4.    Permit    Create        changeto

Role: Network-Admin (System-defined)
Description: Admin for L3 (IP and Routes) and L4 VIPs
Number of rules: 5
-----
Rule    Type    Permission    Feature
-----
 1.    Permit    Create        interface
```

```

2.  Permit  Create      connection
3.  Permit  Create      nat
4.  Permit  Create      config_copy
5.  Permit  Create      changeto

```

```

Role: Security-Admin (System-defined)
Description: Administrator for all security features
Number of rules: 8

```

```

-----
Rule   Type   Permission  Feature
-----
1.    Permit  Create      access-list
2.    Permit  Create      inspect
3.    Permit  Create      connection
4.    Permit  Modify      interface
5.    Permit  Create      aaa
6.    Permit  Create      nat
7.    Permit  Create      config_copy
8.    Permit  Create      changeto

```

```

Role: Network-Monitor (System-defined)
Description: Monitoring for all features
Number of rules: 2

```

```

-----
Rule   Type   Permission  Feature
-----
1.    Permit  Monitor     all
2.    Permit  Monitor     changeto

```

---

**Related Commands**

Command	Description
<a href="#">role</a>	Assigns a user role to a user and enters role configuration mode.

---

# show user-account

To display user account information, use the **show user-account** command in EXEC mode.

```
show user-account [user_name]
```

Syntax Description	<i>user_name</i>	(Optional) Name of user.
--------------------	------------------	--------------------------

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To display the user account information for all users, do not specify a user with the optional *user\_name* argument.

**Examples** The following example shows sample output from the **show user-account** command:

```
firewall/Admin# show user-account
user:ciscoSupport
    this user account has no expiry date
    roles: Network-Monitor
    domain: default-domain
    Context: Admin
user:admin
    this user account has no expiry date
    roles: Admin
    domain: default-domain
    Context: Admin
user:www
    this user account has no expiry date
    roles: Admin
    domain: default-domain
    Context: Admin
```

Related Commands	Command	Description
	<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.
	<a href="#">username</a>	Defines a user and its associated password, role, and domain.

# show users

To display the information for users that are currently logged in to the VFW application, use the **show users** command in EXEC mode.

```
show users [user_name]
```

<b>Syntax Description</b>	<i>user_name</i> (Optional) Name of user.
---------------------------	---

**Defaults** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
	Release 3.6.0	No modification.
	Release 3.7.0	No modification.

**Usage Guidelines** This command requires the AAA feature in your user role. For details about role-based access control (RBAC) and user roles, see the [“Configuring Virtualization on the Virtual Firewall”](#) module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

To display the information for all users that are currently logged in to the VFW application, do not specify a user with the optional *user\_name* argument.

**Examples** The following example shows sample output from the **show users** command:

```
firewall/Admin# show users
```

```
User      Context Line      Login Time (Location)  Role      Domain(s)
*admin   Admin   pts/0      Feb 26 07:32          Admin     default-domain
```

Related Commands	Command	Description
	<a href="#">clear user</a>	Clears a user session.
	<a href="#">show user-account</a>	Displays user account information.
	<a href="#">username</a>	Defines a user and its associated password, role, and domain.

# username

To define a user and its associated password, role and domain, use the **username** command in configuration mode. To remove the username from the configuration, use the **no** form of this command.

```
username user_name [password [0 | 5] password] [expire date] [role role_name [domain dname1
dname2 . . . dname10]]
```

```
no username user_name [password [0 | 5] password] [expire date] [role role_name [domain
dname1 dname2 . . . dname10]]
```

## Syntax Description

<i>user_name</i>	Identifier of the user you are creating. Enter an unquoted text string with no spaces and a maximum of 24 characters.
<b>password</b>	(Optional) Indicates that a password follows.
<b>0</b>	(Optional) Specifies a clear-text password.
<b>5</b>	(Optional) Specifies an MD5-hashed strong encryption password.
<i>password</i>	Password in clear text, encrypted text, or MD5 strong encryption, depending on the numbered keyword you enter. If you do not enter a numbered keyword, the password is in clear text by default. If you enter the <b>password</b> keyword, you must enter a password. Enter a password as an unquoted text string with a maximum of 32 characters.
<b>expire</b> <i>date</i>	(Optional) Specifies the expiration date of the user account. Enter the expiration date in the format <i>yyyy-mm-dd</i> .
<b>role</b> <i>role_name</i>	(Optional) Specifies an existing role that you want to assign to the user.
<b>domain</b> <i>dname1</i> <i>dname2</i> . . . <i>dname10</i>	Specifies the domains in which the user can operate. You can enter multiple domain names up to a maximum of 10, including <b>default-domain</b> .

## Defaults

No default behavior or values

## Command Modes

Configuration

## Command History

Release	Modification
Release 3.5.0	This command was introduced on the multiservice blade (MSB) for the Cisco XR 12000 Series Router.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

## Usage Guidelines

This command requires the admin user role. For details about role-based access control (RBAC) and user roles, see the “[Configuring Virtualization on the Virtual Firewall](#)” module in *Cisco IOS XR Virtual Firewall Configuration Guide*.

If you do not assign a role to a new user, the default role is Network-Monitor. For users that you create in the admin context, the default scope of access is the entire device. For users that you create in other contexts, the default scope of access is the entire context. If you need to restrict a user's access, you must assign a role-domain pair.

### Examples

The following example shows how to define two new users:

```
firewall/Admin(config)# username USER1 password MYSECRET expire 2005-12-31 role TECHNICIAN
domain D1 default-domain
firewall/Admin(config)# username USER2 password HERSECRET expire 2005-12-31 role Admin
domain default-domain D2
```

### Related Commands

Command	Description
<a href="#">clear user</a>	Clears a user session.
<a href="#">show role</a>	Displays the configured user roles (predefined and user-configured).
<a href="#">show user-account</a>	Displays user account information.
<a href="#">show users</a>	Displays the information for users that are currently logged in to the VFW application.