



# Terminal and Session Commands on the Virtual Firewall

---

This module describes the commands that allow you to configure virtual terminal line settings, as well as Telnet and SSH sessions.



## 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*.

---

# clear line

To close a specified virtual terminal session (VTY) session, use the **clear line** command in EXEC mode.

**clear line** *vtty\_name*

## Syntax Description

<i>vtty_name</i>	Name of a VTY session. Enter a maximum of 64 characters.
------------------	--

## 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*.

## Examples

The following example shows how to terminate the VTY session VTY1:

```
firewall/Admin# clear line VTY1
```

## Related Commands

Command	Description
<a href="#">line vty</a>	Configures the virtual terminal line settings.

# clear ssh

To clear an SSH session or clear the public keys of all SSH hosts, use the **clear ssh** command in EXEC mode.

```
clear ssh {session_id | hosts}
```

## Syntax Description

<i>session_id</i>	Identifier of the SSH session to clear, terminating the session
<b>hosts</b>	Clears the public keys of all trusted SSH hosts

## 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 obtain the specific SSH session ID value, use the **show ssh session-info** command.

## Examples

The following example shows how to clear the SSH session with the identifier 345:

```
firewall/Admin# clear ssh 345
```

## Related Commands

Command	Description
<a href="#">clear telnet</a>	Clears a Telnet session.
<a href="#">show ssh</a>	Displays the information relating to SSH keys and sessions.
<a href="#">ssh key</a>	Generates the SSH private key and the corresponding public key for use by the SSH server.
<a href="#">ssh maxsessions</a>	Controls the maximum number of SSH sessions allowed for each context.

# clear telnet

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

**clear telnet** *session\_id*

<b>Syntax Description</b>	<i>session_id</i>	Identifier of the Telnet session to clear, terminating the session.
---------------------------	-------------------	---

<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.

**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 obtain the specific Telnet session identification number, use the [show telnet](#) command.

**Examples** The following example shows how to clear the Telnet session with the identification number of 236:

```
firewall/Admin# clear telnet 236
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">clear ssh</a>	Clears an SSH session or clears the public keys of all SSH hosts.
	<a href="#">show telnet</a>	Displays the information related to the Telnet session.
	<a href="#">telnet</a>	Initiates a Telnet session with another network device.

# line vty

To configure the virtual terminal line settings, use the **line vty** command in configuration mode. To reset the line configuration mode parameter to its default setting, use the **no** form of this command.

**line vty**

**no line vty**

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

**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*.

**Examples** The following example shows how to enter line configuration mode:

```
firewall/Admin(config)# line vty
firewall/Admin(config-line)#
```

Related Commands	Command	Description
	<a href="#">clear line</a>	Closes a specified virtual terminal (VTY) session.

# session-limit

To configure the maximum number of terminal sessions per line, use the **session-limit** command in line configuration mode. To disable a setting for the configured virtual terminal line, use the **no** form of this command.

**session-limit** *number*

**no session-limit** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of terminal sessions per line. Enter an integer from 1 to 251.
---------------------------	---------------	---

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

<b>Command Modes</b>	Line configuration Admin context only
----------------------	--

<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>	This command has no user role feature restrictions. 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> .
-------------------------	--

**Examples** The following example shows how to configure a virtual terminal line:

```
firewall/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
firewall/Admin(config)#
firewall/Admin(config)# line vty
firewall/Admin(config-line)# session-limit 23
```

The following example shows how to disable a setting for the configured virtual terminal line:

```
firewall/Admin(config-line)# no session-limit 23
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<a href="#">clear line</a>	Closes a specified virtual terminal (VTY) session.
	<a href="#">line vty</a>	Configures the virtual terminal line settings.

# show ssh

To display the information relating to SSH keys and sessions, use the **show ssh** command in EXEC mode.

```
show ssh {key [dsa | rsa | rsa1] | maxsessions [context_name] | session-info [context_name]}
```

## Syntax Description

<b>key</b>	Displays the host key pair details for all SSH keys.
<b>dsa</b>	(Optional) Displays only the details of the DSA key pair for the SSH version 2 protocol.
<b>rsa</b>	(Optional) Displays only the details of the RSA key pair for the SSH version 2 protocol.
<b>rsa1</b>	(Optional) Displays only the details of the RSA1 key pair for the SSH version 1 protocol.
<b>maxsessions</b>	Displays the maximum number of SSH sessions that the VFW application allows. Context administrators may also view SSH session information associated with a particular context.
<i>context_name</i>	(Optional) Name of an existing context containing the SSH session information that the context administrator wants to view. Only the global administrator can view Telnet information associated with a particular context. The <i>context_name</i> argument is case-sensitive and is visible only from the Admin context.
<b>session-info</b>	Displays session information, including session ID, remote host IP address, and active time.

## 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*.

From the Admin context, this argument allows you to display just the SSH information associated with a specific user-created context.

**Examples**

The following example shows how to display all the loaded SSH keys:

```
firewall/Admin# show ssh key
```

The following example shows how to display the maximum number of SSH sessions that the VFW application permits for the context C2:

```
firewall/Admin # show ssh maxsessions C2
```

```
Maximum Sessions Allowed is 2(SSH Server is enabled)
```

**Related Commands**

Command	Description
<a href="#">class-map</a>	Creates a Layer 3 and Layer 4 class map and enters class map configuration mode.
<a href="#">clear ssh</a>	Clears an SSH session or clears the public keys of all SSH hosts.
<a href="#">ssh key</a>	Generates the SSH private key and the corresponding public key for use by the SSH server.
<a href="#">ssh maxsessions</a>	Controls the maximum number of SSH sessions allowed for each context.

# show telnet

To display the information related to the Telnet session, use the **show telnet** command in EXEC mode.

```
show telnet [maxsessions] [context_name]
```

Syntax Description	maxsessions	(Optional) Displays the maximum number of enabled Telnet sessions.
	context_name	(Optional) Name of an existing context. Use the <i>context_name</i> argument to display Telnet information that pertains only to the specified context. The <i>context_name</i> 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 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*.

If you do not include the optional **maxsessions** keyword, the VFW application displays the following Telnet information:

- Session ID—Unique session identifier for the Telnet session
- Remote host—IP address and port of the remote Telnet client
- Active time—Time since the Telnet connection request was received by the VFW application

**Examples** The following example shows how to display the current Telnet information:

```
firewall/Admin# show telnet
```

Related Commands	Command	Description
	<a href="#">class-map</a>	Creates a Layer 3 and Layer 4 class map and enters class map configuration mode.

■ show telnet

Command	Description
<a href="#">clear telnet</a>	Clears a Telnet session.
<a href="#">telnet</a>	Initiates a Telnet session with another network device.

# show terminal

To display the console terminal settings, use the **show terminal** command in EXEC mode.

**show terminal [internal info]**

<b>Syntax Description</b>	<b>internal info</b> (Optional) Displays terminal internal information.
---------------------------	---

**Defaults** No default behavior or values

**Command Modes** 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.

**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*.

**Examples** The following example shows how to display the console terminal settings:

```
firewall/Admin# show terminal
```

**Related Commands** This command has no related commands.

# ssh

To initiate a Secure Shell (SSH) session with another device, use the **ssh** command in EXEC mode.

```
ssh {hostname | user@hostname}
```

Syntax Description	Parameter	Description
	<i>hostname</i>	Name or IP address of the host to access. If no user name is specified, the default is "Admin". Maximum number of characters is 64.
	<i>user</i>	Username on a host.

**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*.

**Examples** The following example shows how to initiate an SSH session with the host 196.168.12.10:

```
firewall/Admin# ssh 196.168.12.10
```

The following example shows how to initiate an SSH session with USER1 on HOST1:

```
firewall/Admin# ssh USER1@HOST1
```

Related Commands	Command	Description
	<a href="#">class-map</a>	Creates a Layer 3 and Layer 4 class map and enters class map configuration mode.
	<a href="#">clear ssh</a>	Clears an SSH session or clears the public keys of all SSH hosts.
	<a href="#">parameter-map type</a>	Creates a connection, HTTP, or SSL type parameter map.
	<a href="#">show ssh</a>	Displays the information relating to SSH keys and sessions.

Command	Description
<a href="#">ssh key</a>	Generates the SSH private key and the corresponding public key for use by the SSH server.
<a href="#">ssh maxsessions</a>	Controls the maximum number of SSH sessions allowed for each context.

# ssh key

To generate the SSH private key and the corresponding public key for use by the SSH server, use the **ssh key** command in configuration mode. To remove an SSH key pair, use the **no** form of this command.

```
ssh key {dsa | rsa | rsa1} [bits [force]]
```

```
no ssh key {dsa | rsa | rsa1}
```

## Syntax Description

<b>dsa</b>	Generates the DSA key pair for the SSH version 2 protocol.
<b>rsa</b>	Generates the RSA key pair for the SSH version 2 protocol.
<b>rsa1</b>	Generates the RSA1 key pair for the SSH version 1 protocol.
<b>bits</b>	(Optional) Number of bits for the key pair. For DSA, enter an integer from 768 to 2048. For RSA and RSA1, enter an integer from 768 to 4096. The greater the number of bits you specify, the longer it takes to generate the key. The default is 768.
<b>force</b>	(Optional) Forces the generation of a DSA or RSA key even when previous keys exist. If the SSH key pair option is already generated for the required version, use the <b>force</b> keyword to overwrite the previously generated key pair.

## 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*.

Before you generate the key, set the hostname and the domain name. These settings are used in the key.

The global administrator performs the key generation in the Admin context. All contexts associated with the VFW application share the common key. There is only a single host-key pair.

If you are the administrator or another user authorized in the Admin context, use the **changeto** command in EXEC mode to move to the Admin context. An administrator can perform all allowable functions within the Admin context.

Ensure that you have an SSH host key pair with the appropriate version before enabling the SSH service. The SSH service accepts three types of key pairs for use by SSH versions 1 and 2. Generate the SSH host key pair according to the SSH client version used.

### Examples

The following example shows how to generate an RSA1 key pair in the Admin context:

```
firewall/Admin(config)# ssh key rsa1 1024  
  
generating rsa1 key  
.....  
generated rsa1 key
```

The following example shows how to remove the SSH host key pair:

```
firewall/Admin(config)# no ssh key rsa1
```

### Related Commands

Command	Description
<a href="#">match protocol</a>	Configures the class map to identify the network management protocols that can be received by the VFW application.
<a href="#">ssh maxsessions</a>	Controls the maximum number of SSH sessions allowed for each context.

# ssh maxsessions

To control the maximum number of SSH sessions allowed for each context, use the **ssh maxsessions** command in configuration mode. To revert to the default number of SSH sessions, use the **no** form of this command.

**ssh maxsessions** *max\_sessions*

**no ssh maxsessions**

## Syntax Description

<i>max_sessions</i>	Maximum number of concurrent SSH sessions allowed for the associated context. The range is 1 to 4 SSH sessions per user context; 1 to 16 SSH sessions for the Admin context. The defaults are 4 (user context) and 16 (Admin context).
---------------------	--

## 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*.

By default, the VFW application supports four concurrent SSH management sessions for each user context and sixteen concurrent SSH management sessions for the Admin context. The VFW application supports a total maximum of 256 concurrent SSH sessions.

## Examples

The following example shows how to configure the maximum number of concurrent SSH sessions in the Admin context to 3:

```
firewall/Admin(config)# ssh maxsessions 3
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">match protocol</a>	Configures the class map to identify the network management protocols that can be received by the VFW application.
<a href="#">ssh key</a>	Generates the SSH private key and the corresponding public key for use by the SSH server.

# telnet

To initiate a Telnet session with another network device, use the **telnet** command in EXEC mode.

```
telnet ip_address [port]
```

Syntax Description		
<i>ip_address</i>		IP address of the network host. Enter an IP address in dotted-decimal notation.
<i>port</i>		(Optional) Port number on the network host. The range is from 0 to 2147483647

**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*.

**Examples** The following example shows how to open a Telnet session with another network device:

```
firewall/Admin# telnet 192.126.2.1
```

Related Commands	Command	Description
	<a href="#">class-map</a>	Creates a Layer 3 and Layer 4 class map and enters class map configuration mode.
	<a href="#">clear telnet</a>	Clears a Telnet session.
	<a href="#">parameter-map type</a>	Creates a connection, HTTP, or SSL type parameter map.
	<a href="#">show telnet</a>	Displays the information related to the Telnet session.

# telnet maxsessions

To control the maximum number of Telnet sessions allowed for each context, use the **telnet maxsessions** command in configuration mode. To revert to the default number of Telnet sessions, use the **no** form of this command.

**telnet maxsessions** *sessions*

**no telnet maxsessions**

## Syntax Description

*sessions* Maximum number of concurrent Telnet sessions allowed for the associated context. The range is 1 to 4 Telnet sessions per user context; 1 to 16 Telnet sessions for the Admin context. The defaults are 4 (user context) and 16 (Admin context).

## Defaults

By default, the VFW application supports four concurrent Telnet management sessions for each user context and sixteen concurrent Telnet management sessions for the Admin context.

## 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*.

The VFW application supports a total maximum of 256 concurrent Telnet sessions.

## Examples

The following example shows how to configure the maximum number of concurrent Telnet sessions to 3 in the Admin context:

```
firewall/Admin(config)# telnet maxsessions 3
```

The following example shows how to revert to the default of 16 Telnet sessions for the Admin context:

```
firewall/Admin(config)# no telnet maxsessions
```

Related Commands	Command	Description
	<a href="#">clear telnet</a>	Clears a Telnet session.
	<a href="#">match protocol</a>	Configures the class map to identify the network management protocols that can be received by the VFW application.
	<a href="#">show telnet</a>	Displays the information related to the Telnet session.
	<a href="#">telnet</a>	Initiates a Telnet session with another network device.

# terminal

To configure the terminal display settings, use the **terminal** command in EXEC mode.

```
terminal {length lines | monitor | no | session-timeout minutes | terminal-type text |
width characters}
```

## Syntax Description

<b>length</b> <i>lines</i>	Sets the number of lines displayed on the current terminal screen. This command is specific only to the console port. Telnet and SSH sessions set the length automatically. Valid entries are from 0 to 511. The default is 24 lines. A selection of 0 instructs the VFW application to scroll continuously (no pausing).
<b>monitor</b>	Displays syslog output on the terminal for the current terminal and session. To enable the various levels of syslog messages to the terminal, use the <b>logging monitor</b> command in configuration mode.
<b>no</b>	Negates a command or sets it back to its default value.
<b>session-timeout</b> <i>minutes</i>	Specifies the session timeout value in minutes to configure the automatic logout time for the current terminal session on the VFW application. When you exceed the time limit configured by this command, the VFW application closes the session and exits. The range is 0 to 525600. The default is 5 minutes. You can set the <b>terminal session-timeout</b> value to 0 to disable this feature so that the terminal remains active until you choose to exit the VFW application. The VFW application does not save this change in the configuration file.
<b>terminal-type</b> <i>text</i>	Specifies the name and type of the terminal used to access the VFW application. If a Telnet or SSH session specifies an unknown terminal type, the VFW application uses the VT100 terminal by default. Specify a text string from 1 to 80 alphanumeric characters.
<b>width</b> <i>characters</i>	Sets the number of characters displayed on the current terminal screen. This command is specific only to the console port. Telnet and SSH sessions set the width automatically. Valid entries are 24 to 512. The default is 80 columns.

## Defaults

The default terminal length is 24 lines.  
The default session timeout is 5 minutes.  
The default terminal width is 80 columns.

## 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*.

Use the **show terminal** command to display the current terminal settings.

All terminal parameter-setting commands are set locally and do not remain in effect after you end a session. You must perform this task at the EXEC prompt at each session to see the debugging messages.

**Examples**

The following example shows how to specify the VT100 terminal, set the number of screen lines to 35, and set the number of characters to 250:

```
firewall/Admin# terminal terminal-type vt220
firewall/Admin# terminal length 35
firewall/Admin# terminal width 250
```

The following example shows how to specify a terminal timeout of 600 minutes for the current session:

```
firewall/Admin# terminal session-timeout 600
```

The following example shows how to set the width to 100 columns:

```
firewall/Admin# terminal width 100
```

The following example shows how to set the width to its default of 80 columns:

```
firewall/Admin# terminal no width
```

The following example shows how to start the current terminal monitoring session:

```
firewall/Admin# terminal monitor
```

The following example shows how to stop the current terminal monitoring session:

```
firewall/Admin# terminal no monitor
```

**Related Commands**

Command	Description
<a href="#">parameter-map type</a>	Creates a connection, HTTP, or SSL type parameter map.