Contents

Information center commands

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

diagnostic-logfile save

Use **diagnostic-logfile save** to manually save diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

Syntax

diagnostic-logfile save

Views

Any view

Predefined user roles

network-admin

Usage guidelines

You can specify the directory to save the diagnostic log file by using the **info-center diagnostic-logfile directory** command.

The system clears the diagnostic log file buffer after saving the buffered diagnostic logs to the diagnostic log file.

If the diagnostic log file buffer is empty, this command displays a success message even though no logs are saved to the diagnostic log file.

Examples

Manually save diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

```
<Sysname> diagnostic-logfile save
The contents in the diagnostic log file buffer have been saved to the file
flash:/diagfile/diagfile.log.
```

Related commands

info-center diagnostic-logfile enable

info-center diagnostic-logfile directory

display diagnostic-logfile summary

Use **display diagnostic-logfile summary** to display the diagnostic log file configuration.

Syntax

display diagnostic-logfile summary

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the diagnostic log file configuration.

```
<Sysname> display diagnostic-logfile summary
  Diagnostic log file: Enabled.
  Diagnostic log file size quota: 10 MB
  Diagnostic log file directory: flash:/diagfile
  Writing frequency: 24 hour 0 min 0 sec
```

Table 1 Command output

Field	Description
Diagnostic log file	Status of the diagnostic log file: • **Enabled**—Diagnostic logs can be output to the diagnostic log file. • **Disabled**—Diagnostic logs cannot be output to the diagnostic log file.
Diagnostic log file size quota	Maximum size for the diagnostic log file, in MB.
Log file directory	Directory where the diagnostic log file is saved.
Writing frequency	Interval at which the system saves diagnostic logs from the buffer to the diagnostic log file.

display info-center

Use **`display info-center`** to display information center configuration.

Syntax

`display info-center`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information center configuration.

```
<Sysname> display info-center
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
    192.168.0.1,
    port number: 5000, host facility: local7
Log buffer: Enabled
    Max buffer size 1024, current buffer size 512,
    Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
```

```
Log host: Date
Other output destination: Date
```

display logbuffer

Use **display logbuffer** to display log buffer information and buffered logs..

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize* | **slot** *slot-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

reverse: Displays log entries chronologically, with the most recent entry at the top. If you do not specify this keyword, the command displays log entries chronologically, with the oldest entry at the top.

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information for all levels.

Table 2 Log levels

Severity value	Level	Description	Keyword in commands
0	Emergency	The system is unusable. For example, the system authorization has expired.	**emergency**
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.	**alert**
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.	**critical**
3	Error	Error condition. For example, the link state changes.	**error**
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.	**warning**
5	Notification	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.	**notification**
6	Informational	Informational message. For example, a command or a **ping** operation is executed.	**informational**
7	Debugging	Debugging message.	**debugging**

size *buffersize*: Specifies the number of latest logs to be displayed. The value range is 1 to 1024. If you do not specify this option, the command displays all logs in the log buffer.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display log buffer information and buffered logs.

```
<Sysname> display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 718
Current messages: 512
%Jun 17 15:57:09:578 2016 Sysname SYSLOG/7/SYS_RESTART:System restarted --
…
```

Table 3 Command output

Field	Description
Log buffer	Status of the log buffer: • **Enabled**—Logs can be output to the log buffer. • **Disabled**—Logs cannot be output to the buffer.
Max buffer size	Maximum buffer size supported by the device.
Actual buffer size	Maximum buffer size configured by using the **info-center logbuffer size** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Related commands

info-center logbuffer

reset logbuffer

display logbuffer summary

Use **display logbuffer summary** to display the log buffer summary.

Syntax

display logbuffer summary [**level** *severity* | **slot** *slot-number*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

level *severity*: Specifies a severity level in the range of 0 to 7. If you do not specify a severity level, this command displays log information of all levels in the log buffer. For more information about log levels, see Table 2.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays information for all member devices.

Examples

Display the summary of the log buffer.

```
<Sysname> display logbuffer summary
  Slot EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     1     0     0     0     7     0    34    38     0
```

Table 4 Command output

Field	Description
EMERG	Represents emergency. For more information, see Table 2.
ALERT	Represents alert. For more information, see Table 2.
CRIT	Represents critical. For more information, see Table 2.
ERROR	Represents error. For more information, see Table 2.
WARN	Represents warning. For more information, see Table 2.
NOTIF	Represents notification. For more information, see Table 2.
INFO	Represents informational. For more information, see Table 2.
DEBUG	Represents debug. For more information, see Table 2.

display logfile summary

Use **`display logfile summary`** to display the log file configuration.

Syntax

`display logfile summary`

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the log file configuration.

```
<Sysname> display logfile summary
  Log file: Enabled.
  Log file size quota: 10 MB
  Log file directory: flash:/logfile
  Writing frequency: 24 hour 0 min 10 sec
```

Table 5 Command output

Field	Description
Log file	Log file status: • **Enabled**—Logs can be output to the log file. • **Disabled**—Logs cannot be output to the log file.
Log file size quota	Maximum log file size, in MB.
Log file directory	Log file directory.

Field	Description
Writing frequency	Log file writing frequency.

display security-logfile summary

Use **display security-logfile summary** to display the summary of the security log file.

Syntax

display security-logfile summary

Views

Any view

Predefined user roles

security-audit

Usage guidelines

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference*.

Examples

Display the summary of the security log file.

```
<Sysname> display security-logfile summary
  Security log file: Enabled
  Security log file size quota: 10 MB
  Security log file directory: flash:/seclog
  Alarm threshold: 80%
  Current usage: 30%
  Writing frequency: 24 hour 0 min 0 sec
```

Table 6 Command output

Field	Description
Security log file	Status of the security log file: • **Enabled**—Security logs can be output to the security log file. • **Disabled**—Security logs cannot be output to the security log file.
Security log file size quota	Maximum storage space reserved for the security log file.
Security log file directory	Security log file directory.
Alarm-threshold	Alarm threshold of the security log file usage.
Current usage	Current usage of the security log file.
Writing frequency	Security log file writing frequency.

Related commands

authorization-attribute (*Security Command Reference*)

enable log updown

Use **enable log updown** to enable an interface to generate link up or link down logs when the interface state changes.

Use **undo enable log updown** to disable an interface from generating link up or link down logs when the interface state changes.

Syntax

enable log updown

undo enable log updown

Default

All interfaces are allowed to generate link up and link down logs.

Views

Interface view

Predefined user roles

network-admin

Examples

Disable GigabitEthernet 1/0/1 from generating link up or link down logs.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo enable log updown
```

info-center diagnostic-logfile directory

Use **info-center diagnostic-logfile directory** to configure the directory to save the diagnostic log file.

Syntax

info-center diagnostic-logfile directory *dir-name*

Default

The diagnostic log file directory is **flash:/diagfile**.

Views

System view

Predefined user roles

network-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified directory must have been created.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the diagnostic log file directory to **flash:/test**.

```
<Sysname> mkdir test
```

```
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center diagnostic-logfile directory flash:/test
```

info-center diagnostic-logfile enable

Use **info-center diagnostic-logfile enable** to enable saving diagnostic logs to the diagnostic log file.

Use **undo info-center diagnostic-logfile enable** to disable saving diagnostic logs to the diagnostic log file.

Syntax

info-center diagnostic-logfile enable

undo info-center diagnostic-logfile enable

Default

Saving diagnostic logs to the diagnostic log file is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables saving diagnostic logs to the diagnostic log file for centralized management. Users can view the diagnostic logs to monitor device activities and to troubleshoot problems.

Examples

Enable saving diagnostic logs to the diagnostic log file.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile enable
```

info-center diagnostic-logfile frequency

Use **info-center diagnostic-logfile frequency** to configure the interval at which the system saves diagnostic logs from the diagnostic log file buffer to the diagnostic log file.

Use **undo info-center diagnostic-logfile frequency** to restore the default.

Syntax

info-center diagnostic-logfile frequency *freq-sec*

undo info-center diagnostic-logfile frequency

Default

The diagnostic log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the diagnostic log file saving interval in seconds. The value range is 10 to 86400.

Usage guidelines

The system outputs diagnostic logs to the diagnostic log file buffer, and then saves the buffered logs to the diagnostic log file at the specified interval.

Examples

Set the diagnostic log file saving interval to 600 seconds.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile frequency 600
```

Related commands

info-center diagnostic-logfile enable

info-center diagnostic-logfile quota

Use **info-center diagnostic-logfile quota** to set the maximum diagnostic log file size.

Use **undo info-center diagnostic-logfile quota** to restore the default.

Syntax

info-center diagnostic-logfile quota *size*

undo info-center diagnostic-logfile quota

Default

The maximum diagnostic log file size is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum size for the diagnostic log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the diagnostic log file.

```
<Sysname> system-view
[Sysname] info-center diagnostic-logfile quota 6
```

info-center enable

Use **info-center enable** to enable the information center.

Use **undo info-center enable** to disable the information center.

Syntax

info-center enable

undo info-center enable

Default

The information center is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
Information center is enabled.
```

info-center format

Use **info-center format** to set the format for logs sent to log hosts.

Use **undo info-center format** to restore the default.

Syntax

info-center format { **cmcc** | **unicom** }

undo info-center format

Default

Logs are sent to log hosts in standard format.

Views

System view

Predefined user roles

network-admin

Parameters

cmcc: Specifies the China Mobile Communications Corporation (**cmcc**) format.

unicom: Specifies the China Unicom (**unicom**) format.

Usage guidelines

Logs can be sent to log hosts in standard, **unicom**, or **cmcc** format. For more information about log formats, see *Network Management and Monitoring Configuration Guide*.

Examples

Set the log format to **unicom** for logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center format unicom
```

info-center logbuffer

Use **info-center logbuffer** to enable log output to the log buffer.

Use **undo info-center logbuffer** to disable log output to the log buffer.

Syntax

info-center logbuffer

undo info-center logbuffer

Default

Log output to the log buffer is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable log output to the log buffer.

```
<Sysname> system-view
[Sysname] info-center logbuffer
```

Related commands

display logbuffer

info-center enable

info-center logbuffer size

Use **info-center logbuffer size** to set the maximum number of logs that can be stored in the log buffer.

Use **undo info-center logbuffer size** to restore the default.

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

Default

The log buffer can store a maximum of 512 logs.

Views

System view

Predefined user roles

network-admin

Parameters

buffersize: Specifies the maximum number of logs that can be stored in the log buffer. The value range is 0 to 1024, and the default is 512.

Examples

Set the maximum log buffer size to 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

Restore the default maximum log buffer size.

```
<Sysname> system-view
[Sysname] undo info-center logbuffer size
```

Related commands

display logbuffer

info-center enable

info-center logfile directory

Use **info-center logfile directory** to specify the directory to save the log file.

Syntax

info-center logfile directory *dir-name*

Default

The log file directory is **flash:/logfile**.

Views

System view

Predefined user roles

network-admin

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified log file directory must have been created.

The log file uses the .log extension.

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center logfile directory flash:/test
```

Related commands

info-center logfile enable

info-center logfile enable

Use **info-center logfile enable** to enable the log file feature.

Use **undo info-center logfile enable** to disable the log file feature.

Syntax

info-center logfile enable

undo info-center logfile enable

Default

The log file feature is enabled.

Views

System view

Predefined user roles

network-admin

Examples

Enable log output to the log file.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

info-center logfile frequency

Use **info-center logfile frequency** to configure the interval at which the system saves logs from the log file buffer to the log file.

Use **undo info-center logfile frequency** to restore the default.

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

Default

The log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the log file saving interval in seconds. The value range is 1 to 86400.

Usage guidelines

This command enables the system to automatically save logs in the log file buffer to the log file at the specified interval.

Examples

Set the log file saving interval to 60000 seconds.

```
<Sysname> system-view
[Sysname] info-center logfile frequency 60000
```

Related commands

info-center logfile enable

info-center logfile overwrite-protection

Use **info-center logfile overwrite-protection** to enable log file overwrite-protection.

Use **undo info-center logfile overwrite-protection** to disable log file overwrite-protection.

Syntax

info-center logfile overwrite-protection [**all-port-powerdown**]

undo info-center logfile overwrite-protection

Default

Log file overwrite-protection is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

all-port-powerdown: Shuts down all the service ports on the device when no log file space or storage device space is available. If you do not specify this keyword, the device does not shut down service ports when no log file space or storage device space is available.

Usage guidelines

This command is available only in FIPS mode.

Log file overwrite protection enables the system to stop saving new logs when no log file space or storage device space is available.

Examples

Enable log file overwrite-protection.

```
<Sysname> system-view
[Sysname] info-center logfile overwrite-protection
```

info-center logfile size-quota

Use **info-center logfile size-quota** to set the maximum log file size.

Use **undo info-center logfile size-quota** to restore the default.

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

Default

The maximum log file size is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Specifies the maximum log file size, in MB. The value range is 1 to 10.

Examples

Set the maximum log file size to 6 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 6
```

Related commands

info-center logfile enable

info-center logging suppress duplicates

Use **info-center logging suppress duplicates** to enable duplicate log suppression.

Use **undo info-center logging suppress duplicate** to disable duplicate log suppression.

Syntax

info-center logging suppress duplicates

undo info-center logging suppress duplicates

Default

Duplicate log suppression is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Outputting consecutive duplicate logs wastes system and network resources and increases device maintenance costs. You can enable this feature to suppress output of consecutive duplicate logs.

Examples

Enable duplicate log suppression on device A.

```
<Sysname> system-view
[Sysname] info-center logging suppress duplicates
```

info-center logging suppress module

Use **info-center logging suppress module** to configure a log suppression rule for a module.

Use **undo info-center logging suppress module** to delete a log suppression rule.

Syntax

info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

undo info-center logging suppress module *module-name* **mnemonic** { **all** | *mnemonic-value* }

Default

The device does not suppress output of any logs from any modules.

Views

System view

Predefined user roles

network-admin

Parameters

module-name: Specifies a log source module by its name, a case-insensitive string of 1 to 8 characters. To view the list of available log source modules, use the **info-center logging suppress module ?** command.

mnemonic { **all** | *mnemonic-value* }: Configures a mnemonic filter for log suppression.

- **all**: Suppresses output of all logs of the module.
- *mnemonic-value*: Suppresses output of logs with the specified mnemonic value. The *mnemonic-value* argument is a case-insensitive string of 1 to 32 characters, which must be the complete value contained in the mnemonic field of the log message. Log suppression will fail if a partial mnemonic value is specified.

Usage guidelines

You can configure log suppression rules to filter out the logs that you are not concerned with. A log suppression rule suppresses output of all logs or only logs with a specific mnemonic value for a module.

Examples

Configure a log suppression rule to suppress output of logs with the **shell_login** mnemonic value for the shell module.

```
<Sysname> system-view
[Sysname] info-center logging suppress module shell mnemonic shell_login
```

Related commands

info-center source

info-center loghost

Use **info-center loghost** to specify a log host and to configure output parameters.

Use **undo info-center loghost** to remove a log host.

Syntax

info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**facility** *local-number*]

undo info-center loghost [**vpn-instance** *vpn-instance-name*] { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* }

Default

No log hosts are specified.

Views

System view

Predefined user roles

network-admin

Parameters

vpn-instance *vpn-instance-name*: Specifies an MPLS L3VPN instance by its name, a case-sensitive string of 1 to 31 characters. If the log host is on the public network, do not specify this option.

hostname: Specifies a log host by its name, a case-insensitive string of 1 to 253 characters. The host name can contain letters, digits, and special characters including hyphen (-), underscore (_), and dot (.).

ipv4-address: Specifies a log host by its IPv4 address.

ipv6 *ipv6-address*: Specifies a log host by its IPv6 address.

port *port-number*: Specifies the port number of the log host, in the range of 1 to 65535. The default is 514. It must be the same as the value configured on the log host. Otherwise, logs cannot be sent to the log host.

dscp *dscp-value*: Specifies the DSCP value in log packets sent to the log host. The value range for the *dscp-value* argument is 0 to 63, and the default is 0. The DSCP value of a packet defines the priority of the packet and affects the transmission priority of the packet. A greater DSCP value represents a higher priority.

facility *local-number*: Specifies a logging facility from local0 to local7 for the log host. The default value is local7. Logging facilities are used to mark different logging sources, and query and filer logs.

Usage guidelines

The **info-center loghost** command takes effect only after the information center is enabled by using **info-center enable** command.

Examples

Output logs to the log host at 1.1.1.1.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

info-center loghost source

Use **info-center loghost source** to specify a source IP address for logs sent to log hosts.

Use **undo info-center loghost source** to restore the default.

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Default

The source IP address of logs sent to log hosts is the primary IP address of the outgoing interface.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

The system uses the primary IP address of the specified interface as the source IP address of the logs sent to log hosts.

The **info-center loghost source** command takes effect only after the information center is enabled by using **info-center enable** command.

Examples

Use the IP address of interface Loopback 0 as the source IP address of the logs sent to log hosts.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 2.2.2.2 32
```

```
[Sysname-LoopBack0] quit
[Sysname] info-center loghost source loopback 0
```

info-center security-logfile alarm-threshold

Use **info-center security-logfile alarm-threshold** to set the alarm threshold for security log file usage.

Use **undo info-center security-logfile alarm-threshold** to restore the default.

Syntax

info-center security-logfile alarm-threshold *usage*

undo info-center security-logfile alarm-threshold

Default

The alarm threshold for security log file usage is 80. When the usage of the security log file reaches 80%, the system outputs a message to inform the administrator.

Views

System view

Predefined user roles

network-admin

Parameters

usage: Specifies an alarm threshold. The value must be an integer in the range of 1 to 100.

Usage guidelines

When the security log file is full, the system deletes the oldest logs and then writes new logs to the security log file. This feature helps avoid security log loss by setting an alarm threshold for the security log file usage. When the threshold is reached, the system outputs log information to inform the administrator. The administrator can log in to the device with the security-audit user role and back up the security log file.

Examples

Set the alarm threshold for security log file usage to 90.

```
<Sysname> system-view
[Sysname] info-center security-logfile alarm-threshold 90
```

Related commands

info-center security-logfile size-quota

info-center security-logfile directory

Use **info-center security-logfile directory** to specify the security log file directory.

Syntax

info-center security-logfile directory *dir-name*

Default

The security log file is saved in the **flash:/seclog** directory.

Views

System view

Predefined user roles

security-audit

Parameters

dir-name: Specifies a directory by its name, a string of 1 to 64 characters.

Usage guidelines

The specified directory must have been created.

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference.*

This command cannot survive an IRF reboot or a master/subordinate switchover.

Examples

Set the security log file directory to **flash:/test**.

```
<Sysname> mkdir test
Creating directory flash:/test... Done.
<Sysname> system-view
[Sysname] info-center security-logfile directory flash:/test
```

info-center security-logfile enable

Use **info-center security-logfile enable** to enable saving of security logs to the security log file.

Use **undo info-center security-logfile enable** to restore the default.

Syntax

info-center security-logfile enable

undo info-center security-logfile enable

Default

The saving of security logs to the security log file is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the system to output security logs to the security log file buffer, and then saves the buffered logs to the security log file regularly.

Examples

Enable saving security logs to the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile enable
```

info-center security-logfile frequency

Use **info-center security-logfile frequency** to configure the interval for saving security logs to the security log file.

Use **undo info-center security-logfile frequency** to restore the default.

Syntax

info-center security-logfile frequency *freq-sec*

undo info-center security-logfile frequency

Default

The security log file saving interval is 86400 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

freq-sec: Specifies the security log file saving interval in seconds. The value range is 10 to 86400 seconds.

Usage guidelines

The system outputs security logs to the security log file buffer, and then saves the buffered logs to the security log file at the specified interval.

Examples

Set the security log file saving interval to 600 seconds.

```
<Sysname> system-view
[Sysname] info-center security-logfile frequency 600
```

Related commands

info-center security-logfile enable

info-center security-logfile size-quota

Use **info-center security-logfile size-quota** to set the maximum size for the security log file.

Use **undo info-center security-logfile size-quota** to restore the default.

Syntax

info-center security-logfile size-quota *size*

undo info-center security-logfile size-quota

Default

The maximum size for the security log file is 10 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Sets the maximum size for the security log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the security log file.

```
<Sysname> system-view
[Sysname] info-center security-logfile size-quota 6
```

Related commands

info-center security-logfile alarm-threshold

info-center source

Use **info-center source** to configure a log output rule for a module.

Use **undo info-center source** to restore the default.

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** }

Default

Table 7 lists the default log output rules.

Table 7 Default output rules

Destination	Source modules	Common log	Security log	Diagnostic log	Hidden log
Console	All supported modules	debugging	Disabled	Disabled	Disabled
Monitor terminal	All supported modules	debugging	Disabled	Disabled	Disabled
Log host	All supported modules	informational	Disabled	Disabled	informational
Log buffer	All supported modules	informational	Disabled	Disabled	informational
Log file	All supported modules	informational	Disabled	Disabled	informational
Security log file	All supported modules, cannot be filtered	Disabled	Debugging, which cannot be filtered	Disabled	Disabled
Diagnostic log file	All supported modules, cannot be filtered	Disabled	Disabled	Debugging, which cannot be filtered	Disabled

Views

System view

Predefined user roles

network-admin

Parameters

module-name: Specifies a module by its name. You can use the **info-center source ?** command to view the modules supported by the device.

default: Specifies all supported modules.

console: Outputs logs to the console.

logbuffer: Outputs logs to the log buffer.

logfile: Outputs logs to the log file.

loghost: Outputs logs to the log host.

monitor: Outputs logs to the monitor terminal.

deny: Disables log output.

level *severity*: Specifies a severity level in the range of 0 to 7. The smaller the severity value, the higher the severity level. See Table 2 for more information. Logs at the specified severity level and higher levels are allowed or denied to be output.

Usage guidelines

If you do not set an output rule for a module, the module uses the output rule set by using the **default** keyword. If no rule is set by using the **default** keyword, the module uses the default output rule.

To modify or remove an output rule set for a module, you must use the *module-name* argument. A new output rule configured by using the **default** keyword does not take effect on the module.

If you execute this command for a module multiple times, the most recent configuration takes effect.

If you execute this command for the **default** modules multiple times, the most recent configuration takes effect.

Examples

Output only VLAN module's information with the emergency level to the console.

```
<Sysname> system-view
[Sysname] info-center source default console deny
[Sysname] info-center source vlan console level emergency
```

Based on the previous configuration, disable output of VLAN module's information to the console so no system information is output to the console.

```
<Sysname> system-view
[Sysname] undo info-center source vlan console
```

info-center synchronous

Use **info-center synchronous** to enable synchronous information output.

Use **undo info-center synchronous** to disable synchronous information output.

Syntax

info-center synchronous

undo info-center synchronous

Default

Synchronous information output is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

System log output interrupts ongoing configuration operations, including obscuring previously entered commands. Synchronous information output shows the obscured commands. It also provides a command prompt in command editing mode, or a [Y/N] string in interaction mode so you can continue your operation from where you were stopped.

Examples

Enable synchronous information output, and then execute the **display current-configuration** command to view the current configuration of the device.

```
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] display current-
```

At this time, the system receives log information. It displays the log information first, and then displays your previous input, which is **display current-** in this example.

```
%May 21 14:33:19:425 2007 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Sysname] display current-
```

Enter **configuration** to complete the **display current-configuration** command, and press the **Enter** key to execute the command.

Enable synchronous information output, and then save the current configuration (enter interactive information).

```
<Sysname> system-view
[Sysname] info-center synchronous
Info-center synchronous output is on
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:
```

At this time, the system receives the log information. It displays the log information first and then displays [Y/N].

```
%May 21 14:33:19:425 2007 Sysname SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

Enter **Y** or **N** to complete your input.

info-center syslog min-age

Use **info-center syslog min-age** to set the minimum storage period for logs in the log buffer and log file.

Use **undo info-center syslog min-age** to restore the default.

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

Default

The log minimum storage period is not set.

Views

System view

Predefined user roles

network-admin

Parameters

min-age: Sets the minimum storage period in hours. The value range is 1 to 8760.

Examples

Set the log minimum storage period to 168 hours.

```
<Sysname> system-view
[Sysname] info-center syslog min-age 168
```

info-center syslog trap buffersize

Use **info-center syslog trap buffersize** to set the maximum number of log traps that can be stored in the log trap buffer.

Use **undo info-center syslog trap buffersize** to restore the default.

Syntax

info-center syslog trap buffersize *buffersize*

undo info-center syslog trap buffersize

Default

The log trap buffer can store a maximum of 1024 traps.

Views

System view

Predefined user roles

network-admin

Parameters

buffersize: Specifies the maximum number of log traps that can be stored in the log trap buffer. The value range is 0 to 65535. Value 0 indicates that the device does not buffer log traps.

Usage guidelines

Log traps are SNMP notifications stored in the log trap buffer. After the **snmp-agent trap enable syslog** command is configured, the device sends log messages in SNMP notifications to the log trap buffer. You can view the log traps by accessing the MIB corresponding to the trap buffer.

The default buffer size is usually used. You can adjust the buffer size according to your network condition. New traps overwrite the oldest traps when the log trap buffer is full.

Examples

Set the log trap buffer size to 2048.

```
<Sysname> system-view
[Sysname] info-center syslog trap buffersize 2048
```

Related commands

snmp-agent trap enable syslog

info-center timestamp

Use **info-center timestamp** to set the timestamp format for logs sent to the console, monitor terminal, log buffer, and log file.

Use **undo info-center timestamp** to restore the default.

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

Default

The timestamp format for logs sent to the console, monitor terminal, log buffer, and log file is **date**.

Views

System view

Predefined user roles

network-admin

Parameters

boot: Sets the timestamp format to xxx.yyy, where xxx is the most significant 32 bits (in milliseconds) and yyy is the least significant 32 bits. For example, 0.21990989 equals Jun 25 14:09:26:881 2007. The **boot** time shows the time since system startup.

date: Sets the timestamp format to MMM DD hh:mm:ss:xxx YYYY, such as Dec 8 10:12:21:708 2007. The **date** time shows the current system time.

- MMM: Abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- DD: Date, starting with a space if it is less than 10, for example " 7".
- hh:mm:ss:xxx: Local time, with hh in the range of 00 to 23, mm and ss in the range of 00 to 59, and xxx in the range of 0 to 999.
- YYYY: Year.

none: Indicates no time information is provided.

Examples

Set the timestamp format to **boot** for logs sent to the console, monitor terminal, log buffer, and log file.

```
<Sysname> system-view
[Sysname] info-center timestamp boot
```

Related commands

info-center timestamp loghost

info-center timestamp loghost

Use **info-center timestamp loghost** to set the timestamp format for logs sent to log hosts.

Use **undo info-center timestamp loghost** to restore the default.

Syntax

info-center timestamp loghost { **date** | **iso** [**with-timezone**] | **no-year-date** | **none** }

undo info-center timestamp loghost

Default

The timestamp format for logs sent to log hosts is **date**.

Views

System view

Predefined user roles

network-admin

Parameters

date: Sets the timestamp format to mmm dd hh:mm:ss yyyy, such as Dec 8 10:12:21 2007. The **date** time shows the current system time.

iso: Sets the ISO 8601 timestamp format, for example, 2009-09-21T15:32:55.

with-timezone: Includes the time zone information in the ISO format timestamp. For example, 2009-09-21T15:32:55+01:00. By default, the ISO format timestamp does not contain the time zone information.

no-year-date: Sets the timestamp format to the current system date and time without year.

none: Indicates that no timestamp information is provided.

Examples

Set the timestamp format to **no-year-date** for logs sent to log hosts.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

Related commands

info-center timestamp

info-center trace-logfile quota

Use **info-center trace-logfile quota** to set the maximum size for the trace log file.

Use **undo info-center trace-logfile quota** to restore the default.

Syntax

info-center trace-logfile quota *size*

undo info-center trace-logfile quota

Default

The maximum size for the trace log file is 1 MB.

Views

System view

Predefined user roles

network-admin

Parameters

size: Sets the maximum size for the trace log file, in MB. The value range is 1 to 10.

Examples

Set the maximum size to 6 MB for the trace log file.

```
<Sysname> system-view
[Sysname] info-center trace-logfile quota 6
```

logfile save

Use **logfile save** to manually save logs in the log file buffer to the log file.

Syntax

logfile save

Views

Any view

Predefined user roles

network-admin

Usage guidelines

You can specify the directory to save the log file by using the **info-center logfile directory** command.

The system clears the log file buffer after saving the buffered logs to the log file automatically or manually.

If the log file buffer is empty, this command displays a success message even though no logs are saved to the log file.

Examples

Manually save logs from the log file buffer to the log file.

```
<Sysname> logfile save
The contents in the log file buffer have been saved to the file flash:/logfile/logfile.log.
```

Related commands

info-center logfile enable

info-center logfile directory

reset logbuffer

Use **reset logbuffer** to clear the log buffer.

Syntax

reset logbuffer

Views

User view

Predefined user roles

network-admin

Examples

Clear the log buffer.

```
<Sysname> reset logbuffer
```

Related commands

display logbuffer

security-logfile save

Use **security-logfile save** to manually save security logs from the security log file buffer to the security log file.

Syntax

security-logfile save

Views

Any view

Predefined user roles

security-audit

Usage guidelines

The system clears the security log file buffer after saving the buffered security logs to the security log file automatically or manually.

If the security log file buffer is empty, this command displays a success message even though no security logs are saved to the security log file.

To use this command, a local user must have the security-audit user role. For information about configuring the security-audit user role, see AAA commands in *Security Command Reference*.

Examples

Manually save the security logs in the security log file buffer to the security log file.

```
<Sysname> security-logfile save
The contents in the security log file buffer have been saved to the file
flash:/seclog/seclog.log.
```

Related commands

info-center security-logfile directory

authorization-attribute (*Security Command Reference*)

snmp-agent trap enable syslog

Use **snmp-agent trap enable syslog** to enable SNMP notifications for log messages.

Use **undo snmp-agent trap enable syslog** to disable SNMP notifications for log messages.

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

Default

The device does not send SNMP notifications for log messages.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to send an SNMP notification for each log message it outputs. The device encapsulates logs in SNMP notifications and then sends them to the SNMP module and the log trap buffer.

For the SNMP module to send the received SNMP notifications correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

To view the traps in the log trap buffer, access the MIB corresponding to the log trap buffer. The log trap buffer size can be set by using the **info-center syslog trap buffersize** command.

Examples

Enable the device to send SNMP notifications for log messages.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable syslog
```

Related commands

info-center syslog trap buffersize

terminal debugging

Use **terminal debugging** to enable display of debug information on the current terminal.

Use **undo terminal debugging** to disable display of debug information on the current terminal.

Syntax

terminal debugging

undo terminal debugging

Default

Display of debug information is disabled on the current terminal.

Views

User view

Predefined user roles

network-admin

Usage guidelines

To enable display of debug information on the console, perform the following tasks:

1. Execute the **terminal debugging** command.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

To enable display of debug information on the current terminal, perform the following tasks:

1. Execute the **terminal monitor** and **terminal debugging** commands.
2. Enable the information center. The information center is enabled by default.
3. Use a debugging command to enable the related debugging.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

You can also enable display of debug information on the current terminal by executing the **terminal logging level 7** command. This command has the following differences from the **terminal debugging** command:

- The **terminal logging level 7** command enables log display for all levels (levels **0** through **7**) on the current terminal.
- The **terminal debugging** command only enables display of logs with the following severity levels:
  - Debug level (level **7**).
  - Severity level higher than or equal to the level specified in the **terminal logging level** command.

Examples

Enable display of debug information on the current terminal.

```
<Sysname> terminal debugging
The current terminal is enabled to display debugging information.
```

Related commands

terminal logging level

terminal monitor

terminal logging level

Use **terminal logging level** to set the lowest level of logs that can be output to the current terminal.

Use **undo terminal logging level** to restore the default.

Syntax

terminal logging level *severity*

undo terminal logging level

Default

The lowest level of logs that can be output to the current terminal is 6 (Informational).

Views

User view

Predefined user roles

network-admin

Parameters

severity: Specifies a log severity level. Valid values are alert, critical, debugging, emergency, error, informational, notification, warning, and digits from 0 to 7.

Usage guidelines

This command enables the device to output logs with a severity level higher than or equal to the specified level to the current terminal. For example, if you set the *severity* argument to 6, logs with a severity value from 0 to 6 are output to the current terminal.

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Configure the device to output logs with the debugging level and higher levels to the current terminal.

```
<Sysname> terminal logging level 7
```

terminal monitor

Use **terminal monitor** to enable monitoring of logs on the current terminal.

Use **undo terminal monitor** to disable monitoring of logs on the current terminal.

Syntax

terminal monitor

undo terminal monitor

Default

Monitoring of logs is enabled on the console and disabled on the monitor terminal.

Views

User view

Predefined user roles

network-admin

Usage guidelines

This command takes effect only for the current connection between the terminal and the device. If a new connection is established, the default is restored.

Examples

Enable monitoring of logs on the current terminal.

```
<Sysname> terminal monitor
The current terminal is enabled to display logs.
```