

TSI Server Configuration Mode Commands

Command Modes

Exec > Global Configuration > Security Configuration > TSI Server Configuration

configure > security > server talos-intelligence *server-name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-server-tsi)#`

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- do show, on page 1
- end, on page 2
- exit, on page 2
- ip, on page 2
- logging, on page 3
- sftp, on page 4
- update-time, on page 5

do show

Executes all **show** commands while in Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

ip

Configures the IP address and port number used to communicate with the Talos Security Intelligence (TSI) database server (Mediator).

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Security Configuration > TSI Server Configuration

configure > security > server talos-intelligence *server-name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

Syntax Description

ip address *ip_address* **port** *port_number*
no ip

no ip

Removes the configured TSI server.

address *ip_address*

Specifies the IP address of the TSI database server (Mediator) from which security updates are received.

ip_address must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number*

Specifies the port number used to communicate with the TSI server (Mediator).

port_number must specified as **5341** for successful communication with the TSI database server..

Usage Guidelines

Use this command to configure the IP address and port number for the system to connect to the TSI database server.

Example

The following command configures the system to connect to a TSI server with the IP address of 10.1.10.10 on port number 5341:

```
ip address 10.1.10.10 port 5341
```

logging

Configures the logging level for connection events to the TSI database server events and transactions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Security Configuration > TSI Server Configuration

configure > security > server talos-intelligence *server-name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

Syntax Description

logging level { error | warning | unusual | info | debug }
no logging

no logging

Removes the configured event logging level and returns the system to the default logging level of **error**.

level { error | warning | unusual | info | debug }

Specifies the level of information to be logged for TSI database server connectivity events. The following severities are supported:

- **error** – log error events and all events with a higher severity level
- **warning** – log warning events and all events with a higher severity level
- **unusual** – log unusual events and all events with a higher severity level
- **info** – log info events and all events with a higher severity level
- **debug** – log all events.

The default logging level severity is **error**.

Usage Guidelines Use this command to set the logging level for events and transactions with the TSI database server.

sftp

Configures the SFTP port number used to pull database updates from the Talos Security Intelligence (TSI) database server (Mediator).

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Security Configuration > TSI Server Configuration

configure > security > server talos-intelligence *server-name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-server-tsi)#`

Syntax Description **`[ no ] port`** *`port_number`*

no

Removes the configured port number.

port_number

Specifies the SFTP port number used to retrieve updates from the TSI database server (Mediator).

port_number must specified as **2222** for successful communication with the TSI database server.

Usage Guidelines Use this command to configure the SFTP port number for the system to retrieve update files from the TSI database server.

Update files are stored locally in /hd-raid/tsi/update.

update-time

Configures the time of day when the system shall contact the Talos Security Intelligence (TSI) database server (Mediator) for security updates.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Security Configuration > TSI Server Configuration

configure > security > server talos-intelligence *server-name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-server-tsi)#`

Syntax Description

`update-time hour` *`value`* **`minute`** *`value`*
`no update-time`

no update-time

Removes the configured time of day when the system retrieves security updates.

hour *value*

Specifies the hour of the day when the system retrieves security updates.

value must be an integer from 0 through 23.

The default is a value of zero for both hour and minute which results in a UTC of midnight.

minute *value*

Specifies the hour of the day when the system retrieves security updates.

value must be an integer from 0 through 59.

The default is a value of zero for both hour and minute which results in a UTC of midnight.

Usage Guidelines

Use this command to configure time of day when the system shall connect to the TSI database server to retrieve security updates. The security databases are updated once a day.

Example

The following command configures the system to connect to a TSI server at 11:00 PM:

```
update-time hour 23 minute 0
```