TACACS+ Configuration Mode Commands

Important TACACS Configuration Mode is available in releases 11.0 and later.

Command Modes

This chapter describes all commands available in the TACACS+ Configuration Mode. TACACS+ (Terminal Access Controller Access-Control System Plus) is a secure, encrypted protocol. By remotely accessing TACACS+ servers that are provisioned with the administrative user account database, the ASR 5500 support TACACS+ accounting and authentication services for system administrative users.

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

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

- accounting, on page 2
- authorization, on page 3
- do show, on page 4
- end, on page 4
- exit, on page 4
- idle-session threshold, on page 5
- max-sessions, on page 6
- on-authen-fail, on page 6
- on-network-error, on page 7
- on-unknown-user, on page 8
- priv-lvl, on page 9
- rem_addr client-ip, on page 10
- server, on page 11
- user-id, on page 14

accounting

Enables the recording of the start and the stop time each command issued during a TACACS+-authenticated CLI session.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

```
[ no ] accounting { command | start-stop }
```

no

Disables a speicifed TACACS+ accounting setting.

command

Enables accounting on a command-by-command basis. The TACACS+ server is contacted prior to the execution of the command and the command which is about to be executed is recorded. Only commands which are valid for the user privilege and context (mode) in which they are about to be executed will be recorded. StarOS does not record whether the command itself succeeded or failed. For security reasons, some secure or restricted commands are not recorded. In such cases, the accounting record will record the command as three asterisks ("***").

start-stop

Records the time at which the session starts (the time at which the user passes authentication) and the time at which the user exits. If a user exits before passing authentication, only a stop time is recorded.

Usage Guidelines

Use this command to configure the accounting method for TACACS+-based CLI sessions.

Important *For releases after 15.0 MR4,* TACACS+ accounting (CLI event logging) will not be generated for Lawful Intercept users with privilege level set to 15 and 13.

Example

The following command enables TACACS+ accounting for commands:

```
accounting command
```

authorization

Enables the authorization of TACACS+ CLI users on a command-by-command, command + command argument, or command prompt basis. If the user is not authorized to execute the command, the command will fail.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

`[local]host_name(config-tacacs)#`

Syntax Description

`[ no ] authorization { arguments | command | prompt }`

no

Disables a specified TACACS+ authorization type.

arguments

Enables per-command and command + argument authorization. The TACACS+ server authorizes each command and its arguments for the user. If the user is not authorized to execute the command and the corresponding arguments, the command fails. If the command does not contain any arguments, then the command only is passed to the authorization server.

command

Enables per-command authorization. The TACACS+ server is contacted for each command and each command is authorized for the user. If the user is not authorized to execute the command, then the command fails. If the user is authorized for the command, the command is executed.

prompt

Enables per-command authorization, as described for the **command** option above. However, since commands may be duplicated in different CLI modes, this version of the command authorization also passes the command prompt string to the server. The TACACS+ server is contacted for each prompt and command and must have a matching string for the prompt/command combination. Enabling **prompt** authorization supersedes **command** authorization, since the prompt and command must be authorized together.

Usage Guidelines

Use this command to configure the authorization method for TACACS+-based CLI sessions.

Example

The following command requires per-command TACACS+ authorization:

`authorization command`

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.

idle-session threshold

Configures the idle session threshold available for TACACS+ sessions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

idle-session threshold *number* **user-id** *tacacs_userid*
default idle-session threshold user-id *tacacs_userid*

threshold *number*

Configures the idle sessions threshold value in minutes. If a session is idle, the CLI flags it as being in an idle state when it has been inactive for a specific amount of time. *number* specifies the idle-session threshold number in minutes. This setting must be an alphanumeric integer from 0 to 10 minutes. The default value is 5 minutes. 0 indicates that there is no idle session threshold for the user. When a CLI session has reached the threshold, then the session is in the idle state but it will not be in the idle state indefinitely.

user-id *tacacs_userid*

Identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

default *tacacs_userid*

Configures the default number for idle sessions to 5 minutes.

Usage Guidelines

Use this command to configure the idle session threshold in minutes for a specific TACACS+ user.

The default value of 5 minutes is used if the idle-session threshold is not configured for a user.

After upgrading to 21.2.0, the default maximum sessions number is assigned to all users. After downgrading to a previous release, the maximum sessions configuration is lost.

While using the **user-id** *TACACS+ Configuration Mode* command without the **idle session threshold** command, the system will keep the existing configured value or the default value if nothing is configured.

Example

The following command configures the threshold for this user to be 5 minutes:

```
idle-session threshold 5 user-id admin
```

max-sessions

Configures the maximum number of sessions available for a TACACS+ user.

Product

All products

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

max-sessions *number* **user-id** *tacacs_userid*
default max-sessions user-id *tacacs_userid*

number

Specifics the maximum number of simultaneous CLI sessions. It must be alphanumeric integer from 0 to 100. The default number is 100.

user-id *tacacs_userid*

Identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

default

Configures the default number of simultaneous CLI sessions to 100.

Usage Guidelines

Use this command to configure the maximum number of sessions available for a TACACS+ user.

After upgrading to 21.2.0, the default maximum sessions number is assigned to all users. After downgrading to a previous release, the maximum sessions configuration is lost.

Example

The following command configures 50 CLI sessions for a specific TACACS user:

```
max-sessions 50 user-id admin
```

The following command configures 100 CLI sessions for a specific TACACS user:

```
default max-sessions user-id admin
```

on-authen-fail

Defines system behavior when an administrative login fails due to a TACACS+ authentication failure. This command also can be used to configure system behavior separately for TACACS+ authentication failures for administrative users accessing the system via the StarOS Console port.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description **`on-authen-fail { continue | stop } [ tty console ]`**

continue

After a TACACS+ authentication failure, the system will continue with authentication using non-TACACS+ authentication services.

stop

After a TACACS+ authentication failure, the system forces the failed TACACS+ user to exit.

tty console

Release 12 and later systems only: Used after the **stop** or **continue** parameters to specify system behavior for users being authenticated via the StarOS Console port:

- **stop tty console**: Forces the failed TACACS+ user to exit.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

Usage Guidelines Use this command to configure system behavior for users that fail TACACS+ authentication.

Example

The following command instructs the system to stop upon TACACS+ authentication failure:

```
on-authen-fail stop
```

on-network-error

Configures StarOS behavior when a TACACS+ login fails due to a network error. This command also can be used to configure system behavior separately for TACACS+ network error login failures for administrative users accessing the system via the Console port.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

```
on-network-error { continue | stop } [ tty console ]
```

continue

The system will continue with authentication using non-TACACS+ authentication services.

stop

The system forces the failed TACACS+ user to exit.

tty console

Release 12 and later systems only: Can be used after the **continue** or **stop** options to specify system behavior for TACACS+ CLI users being authenticated via the StarOS Console port:

- **stop tty console**: Forces the failed user to exit when authentication fails.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

Usage Guidelines

Use this command to configure system behavior for users who fail TACACS+ authentication due to a network error.

Example

The following command conifgures the system to stop when a TACACS+ login fails due to a network error:

```
on-network-error stop
```

on-unknown-user

Configures StarOS behavior when a TACACS+ server cannot authenticate a given user name. This command also can be used to configure system behavior separately for TACACS+ unknown user login failures for administrative users accessing the system via the StarOS console port.

Important Some TACACS+ server implementations will not send a Reply message indicating that the user name is invalid. Instead, these types of implementations will accept the username, whether valid or not, and then examine the username and password in combination before sending a Reply message indicating a failed TACACS+ login. In these cases, specifying **on-unknown-user** will continue the login process. To avoid this scenario, determine the method the configured TACACS+ servers will use to validate user names before deciding whether specifying the **on-unknown-user** command will provide the desired result.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

```
on-unknown-user { continue | stop } [ tty console ]
```

continue

The system will continue with authentication using non-TACACS+ authentication services.

stop

The system forces the failed TACACS+ user to exit.

tty console

Release 12 and later systems only: Can be used after the **continue** or **stop** options to specify the behavior of the system for TACACS+ CLI users being authenticated via the StarOS console port.

- **stop tty console**: The system forces the failed user to exit when authentication fails.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

Usage Guidelines

Use this command to configure StarOS behavior for users who fail TACACS+ user name authentication.

TACACS+ authentication is also performed on non-local VPN context logins, if TACACS+ is configured and enabled. If TACACS+ is enabled with the **on-unknown-user stop** option, the VPN context name into which the user is attempting a login must match the VPN name specified in the username string. If the context name does not match, the login fails and exits out.

Example

The following command forces users who fail TACACS+ user name authentication to exit StarOS:

```
on-unknown-user stop
```

priv-lvl

Configures authorized StarOS privileges for a specified TACACS+ privilege level.

Product

All products

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

```
priv-lvl lvl_number authorization-level { administrator | inspector |
operator | security-admin } [ cli | ecs | ftp | li-administration | nocli
 | noecs | noftp | nocli-administration ]
```

lvl_number

Specifies the TACACS+ privilege level with which StarOS authorizations will be associated. as an integer from 1 through 15.

authorization-level { administrator | inspector | operator | security-admin }

Specifies the StarOS administrative authorization level for this privilege level.

- **administrator** – Allows user to execute Administrator level configuration commands.
- **inspector** – Allows user to execute Inspector commands.
- **operator** – Allows user to execute Operator commands.
- **security-admin** – Allows user to execute Security Administrator commands

For detailed information about StarOS administration levels, refer to the *System Settings* chapter of the *System Administration Guide*.

[cli | ecs | ftp | li-administration | nocli | noecs | noftp | nocli-administration]

Specifies a set of access privileges or restrictions for this TACACS+ privilege level. Multiple options may be specified.

- **cli** – Permits access to the StarOS command line interface.
- **ecs** – Permits access to Enhanced Charging Services (ECS) commands.
- **ftp** – Permits of File Transfer Protocol (FTP).
- **li-administration** – Permits access to Lawful Intercept (LI) administrative commands.
- **nocli** – Denies access to the StarOS CLI.
- **noecs** – Denies access to ECS commands
- **noftp** – Denies use of FTP.
- **nocli-administration** – Denies access to StarOS Administrator and Security Administrator commands.

Usage Guidelines

Use this command to customize StarOS access authorization for users at various TACACS+ privilege levels.

Example

The following command sequence authorizes a TACACS+ priv-level 13 user to execute StarOS Administrator commands but denies access to LI administrative commands and FTP.

```
priv-lvl 13 authorization-level administrator cli noftp
```

rem_addr client-ip

Sends a remote client IPv4 address field in the TACACS+ protocol for use by a Cisco Secure ACS server.

Product

All products

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

[default | no] rem_addr client-ip

default

Disables the sending of a remote client IP address field to a Cisco Secure ACS server for a TACACS+ login request.

no

Disables the sending of a remote client IP address field to a Cisco Secure ACS server for a TACACS+ login request.

Usage Guidelines

A Cisco Secure ACS server can be configured to explicitly check the NAS source address for TACACS+ connections. StarOS may not properly set the rem_addr field in the TACACS+ protocol packet when initiating a connection with the Cisco Secure ACS server. This may cause the Cisco Secure ACS server to reject the TACACS+ login request.

Important The default behavior is to not fill in the rem_addr field.

This CLI command enables the setting and sending of the remote address to the IPv4 address associated with the local context management interface for customers who require this field to be verified via the Cisco Secure ACS server.

When enabled the rem_addr field contains the ssh client IP address in ASCII form. If the IP address cannot be retrieved, the length is set to zero.

Example

The following command enables the sending of the rem_addr field to a Cisco Secure ACS server for a TACACS+ login request:

rem_addr client-ip arg1

server

Configures TACACS+ AAA service-related parameters for use in authenticating StarOS administrative users via a TACACS+ server.

Important Once a TACACS+ server is configured with the **server** command, TACACS+ AAA services for StarOS must be enabled using the **aaa tacacs+** command in Global Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

server priority *priority_number* **ip-address** *ip_address* **[{ encrypted password** *shared_secret* **] [key** *text_password* **] [nas-source-address** *ip_address* **] [password** *text_password* **] [port** *port_number* **] [retries** *num_retries* **] [service { accounting |authentication | authorization }]] [timeout** *seconds* **]**
no server priority *priority_number*

no

Removes a specified server (by priority number) from the TACACS+ server list.

priority *priority_number*

Specifies the order in which TACACS+ servers are to be tried. The priority number corresponds to a configured TACACS+ server.

For releases prior to 18.2, *priority_number* can be an integer from 1 (highest priority) to 3 (lowest priority).

For releases 18.2+, *priority_number* can be an integer from 1 (highest priority) to 4 (lowest priority).

If no server with priority 1 is specified, the next highest priority is used. If the specified priority matches that of a TACACS+ server already configured, any previously defined server configuration parameter(s) for that priority are returned to the default setting(s).

ip-address

Specifies the IP address of the TACACS+ server in IPv4 or IPv6 dotted-decimal notation. Only one IP address can be defined for a given **server priority**

encrypted password *shared_secret*

Specifies the encrypted value of the shared secret key. The server-side configuration must match the decrypted value for the protocol to work correctly. If **encrypted password** is specified, specifying **password** is invalid. No encryption is used if this value is null (""). The encrypted password can be an alphanumeric string of 1 through 100 characters. If neither an **encrypted password** or **password** is specified, StarOS will not use encryption

key *text_password*

Release 11.0 systems only. Instead of using an encrypted password value, the user can specify a plain-text key value for the password. If the **key** keyword is specified, then specifying **encrypted password** is invalid. A null string represents no encryption. The password can be from 1 to 32 alphanumeric characters in length. If neither an **encrypted password** or **key** is specified, then StarOS will not use encryption.

nas-source-address *ip_address*

Release 12 and later systems only: Sets the IPv4 or IPv6 address to be specified in the Source Address of the IP header in the TACACS+ protocol packet sent from the NAS to the TACACS+ server. *ip_address* is entered using IPv4 dotted-decimal notation and must be valid for the interface.

password *text_password*

Release 12.0 and later systems. Instead of using an encrypted password value, the user can specify a plain-text value for the password. If the **password** keyword is specified, specifying **encrypted password** is invalid. A null string ("") represents no encryption. The password can be an alphanumeric string of 1 through 32 characters. If neither an **encrypted password** or **password** is specified, then StarOS will not use encryption.

port *port_number*

Specifies the TCP port number to use for communication with the TACACS+ server. *port_number* can be an integer from 1 through 65535. If a port is not specified, StarOS will use port 49.

retries *number*

Release 12 and later systems only: Specifies the number of retry attempts at establishing a connection to the TACACS+ server if the initial attempt fails. **retries** *number* can be an integer from 0 through 100. The default is 3. Specifying 0 (zero) retries results in StarOS trying only once to establish a connection. No further retries will be attempted.

service { accounting | authentication | authorization }

Release 12 and later systems only: Specifies one or more of the AAA services that the specified TACACS+ server will provide. Use of the **service** keyword requires that at lease one of the available services be specified. If the **service** keyword is not used, StarOS will use the TACACS+ server for all AAA service types. The default is to use authentication, authorization and accounting. Available service types are:

- **accounting**: The specified TACACS+ server should be used for accounting. If TACACS+ authentication is not used, TACACS+ accounting will not be used. If no accounting server is specified and the user is authenticated, no accounting will be performed for the user.
- **authentication**: The specified TACACS+ server should be used for authentication. If a TACACS+ authentication server is not available, TACACS+ will not be used for authorization or accounting.
- **authorization**: The specified TACACS+ server should be used for authorization. If TACACS+ authentication is not used, TACACS+ authorization will not be used. If no authorization server is specified and the user is authenticated, the user will remain logged in with minimum privileges (Inspector level).

timeout *seconds*

Specifies the number of seconds to wait for a connection timeout from the TACACS+ server. *seconds* can be an integer from 1 through 1000. If no timeout is specified, StarOS0 will use the default value of 10 seconds.

Usage Guidelines Use this command to specify TACACS+ service parameters for a specified TACACS+ server.

Example

The following command configures a priority 2, TACACS+ authetication server at IP address 192.156.1.1:

```
server priority 2 ip-address 192.156.1.1 authentication
```

user-id

Configures additional profile attributes for a specific TACACS+ user identifier.

Product All products

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

Syntax Description

user-id *tacacs_userid* **[li-admin | noli-admin]**

[default] user-id *tacacs_userid*

user-id *tacacs_userid*

Identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

[li-admin | noli-admin]

Grants or denies access to Lawful Intercept (LI) configuration commands.

default

Configures default profile attributes for a specific TACACS+ user identifier.

Usage Guidelines Use this command to grant LI access to a specified TACACS+ user identifier.

After upgrading to 21.2.0, the default maximum sessions number is assigned to all users. After downgrading to a previous release, the maximum sessions configuration is lost.

Example

The following command sequence grants TACACS+ user *victor134* access to LI administration commands:

```
user-id victor134 li-admin
```