LOGZILLA DOCUMENTATION

Avaya Communications Manager

Forward Avaya Communication Manager system, security, kernel, and CM IP logs to LogZilla via syslog using the System Management Interface

Receiving Data in LogZilla · Generated April 27, 2026 · logzilla.ai/docs/receiving-data/avaya-communications-manager

Configure Avaya Communication Manager Syslog

Avaya Communication Manager (CM) can forward system logs to LogZilla via syslog over TCP or UDP. The configuration is performed through the System Management Interface (SMI) web interface.

Prerequisites

- Administrative access to Avaya Communication Manager System Management Interface
- Confirm syslog listener ports in LogZilla (see Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings))
- Network connectivity between Communication Manager and LogZilla on the selected syslog port

Configure syslog server

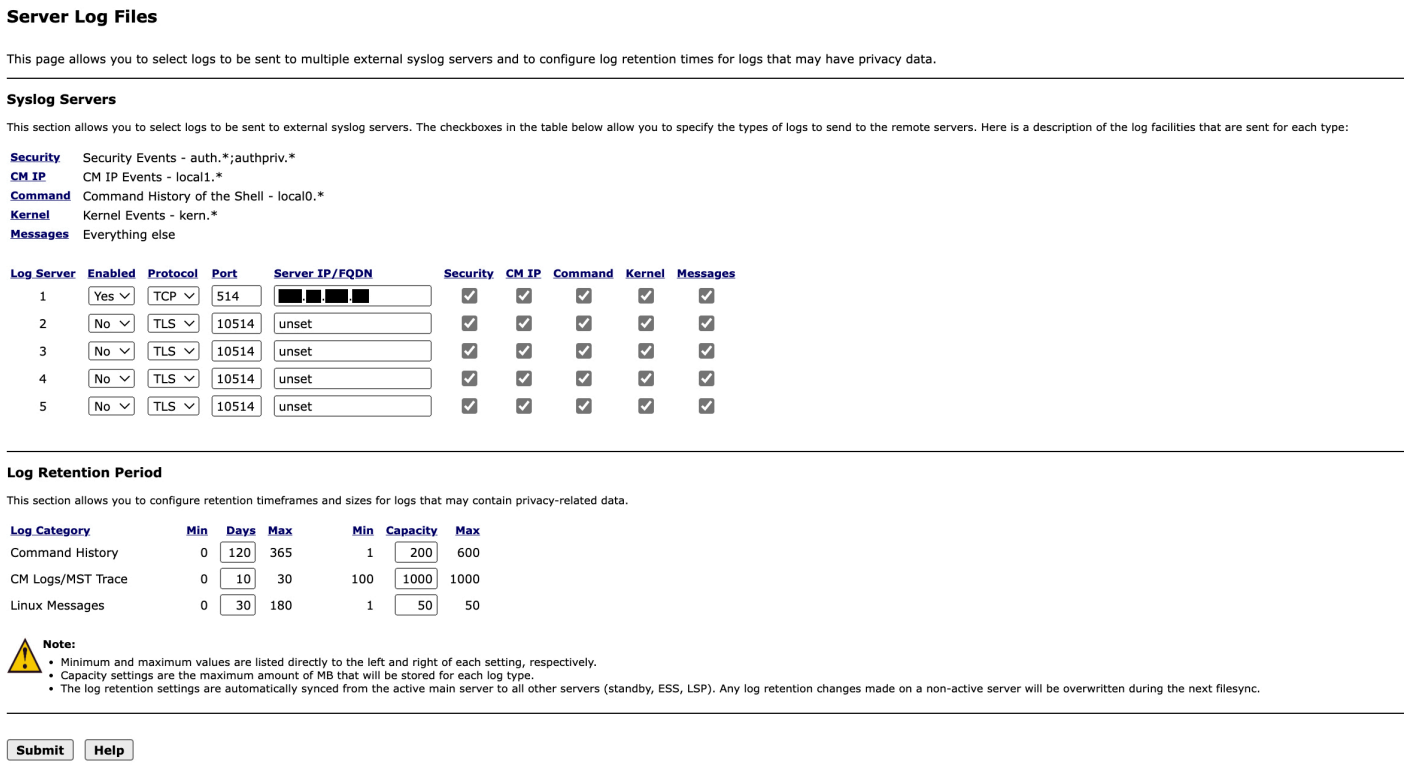
Access the System Management Interface and navigate to the Administration menu.
Select `Server (Maintenance)` from the menu options.
In the left navigation pane under `Security`, select `Server Log Files`.
Locate an available log server entry in the table where `Enabled` is set to `No` (typically the first row unless other syslog servers are already configured).
Configure the following settings:

- Enabled: `Yes`
- Protocol: `TCP` (recommended) or `UDP`
- Port: `514` (or the configured LogZilla syslog port)
- Server IP/FQDN: LogZilla server hostname or IP address

Select the log types to forward by checking the appropriate columns:

- Security: System security events
- CM IP: Communication Manager IP-related events
- Command: Administrative commands
- Kernel: Operating system kernel messages
- Messages: General system messages

Apply the configuration by clicking `Submit`.



Server Log Files

This page allows you to select logs to be sent to multiple external syslog servers and to configure log retention times for logs that may have privacy data.

Syslog Servers

This section allows you to select logs to be sent to external syslog servers. The checkboxes in the table below allow you to specify the types of logs to send to the remote servers. Here is a description of the log facilities that are sent for each type:

Security	Security Events - auth.*;authpriv.*
CM IP	CM IP Events - local1.*
Command	Command History of the Shell - local0.*
Kernel	Kernel Events - kern.*
Messages	Everything else

Log Server	Enabled	Protocol	Port	Server IP/FQDN	Security	CM IP	Command	Kernel	Messages
1	Yes	TCP	514	[redacted]	☑	☑	☑	☑	☑
2	No	TLS	10514	unset	☑	☑	☑	☑	☑
3	No	TLS	10514	unset	☑	☑	☑	☑	☑
4	No	TLS	10514	unset	☑	☑	☑	☑	☑
5	No	TLS	10514	unset	☑	☑	☑	☑	☑

Log Retention Period

This section allows you to configure retention timeframes and sizes for logs that may contain privacy-related data.

Log Category	Min	Days	Max	Min	Capacity	Max
Command History	0	120	365	1	200	600
CM Logs/MST Trace	0	10	30	100	1000	1000
Linux Messages	0	30	180	1	50	50

Note:
- Minimum and maximum values are listed directly to the left and right of each setting, respectively.
- Capacity settings are the maximum amount of MB that will be stored for each log type.
- The log retention settings are automatically synced from the active main server to all other servers (standby, ESS, LSP). Any log retention changes made on a non-active server will be overwritten during the next filesync.

Submit Help

Verify in LogZilla

- Confirm reception by searching for events from the Communication Manager host in LogZilla.
- For network-level troubleshooting, see Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting).

Related topics

- Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings)
- Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting)