Tech Support

Tech Support and System Logs

Multi-Site Orchestrator system logging is automatically enabled when you first deploy the Orchestrator cluster and captures the events and faults that occur in the environment.

You can choose to download the logs at any time or stream them to an external log analyzer, such as Splunk, if you want to use additional tools to quickly parse, view, and respond to important events without a delay.

Starting with Release 3.3(1), the tech support logs are split into two parts:

- Original database backup files containing the same information as in prior releases
- JSON-based database backup for ease of readability

Within each backup archive, you will find the following contents:

- `x.x.x.x`—one or more files in *x.x.x.x* format for container logs available at the time of the backup.
- `msc-backup-<date>_temp`—Original database backup containing the same information as previous releases.
- `msc-db-json-<date>_temp`—Backup contents in JSON format.

  For example:

  ```
  msc_anpEpgRels.json
  msc_anpExtEpgRels.json
  msc_asyncExecutionStatus.json
  msc_audit.json
  msc_backup-versions.json
  msc_backupRecords.json
  msc_ca-cert.json
  msc_cloudSecStatus.json
  msc_consistency.json
  ...
  ```

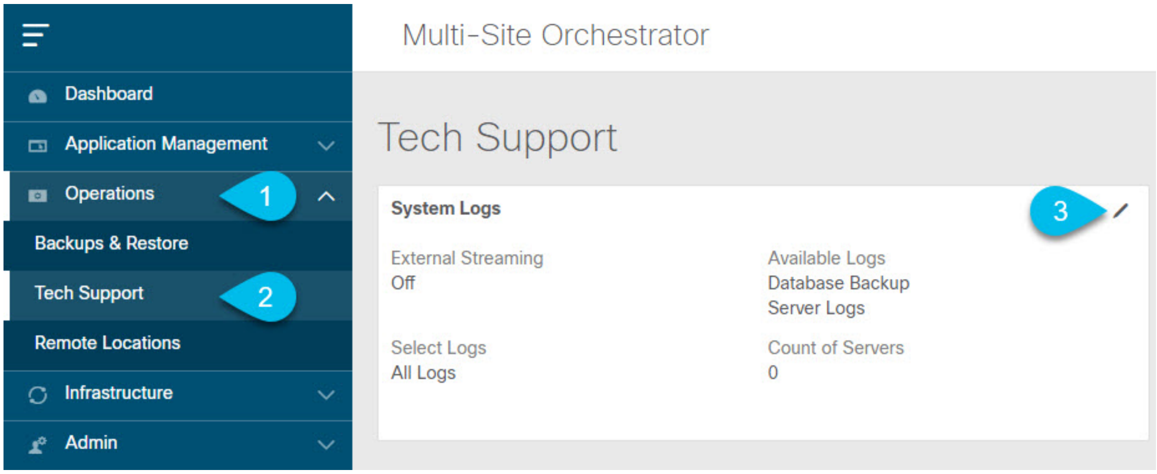
Downloading System Logs

This section describes how to generate a troubleshooting report and infrastructure logs file for all the schemas, sites, tenants, and users that are managed by Multi-Site Orchestrator.

Procedure

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 Open the **System Logs** screen.



System Logs

External Streaming
Off

Available Logs
Database Backup
Server Logs

Select Logs
All Logs

Count of Servers
0

a) In the main menu, select **Operations** > **Tech Support**.
b) In the top right corner of the **System Logs** frame, click the edit button.

Step 3 Click **Download** download the logs.

An archive will be downloaded to your system. Containing all the information as described in the first section of this chapter.

Streaming System Logs to External Analyzer

Multi-Site Orchestrator allows you to send the Orchestrator logs to an external log analyzer tool in real time. By streaming any events as they are generated, you can use the additional tools to quickly parse, view, and respond to important events without a delay.

This section describes how to enable Multi-Site Orchestrator to stream its logs to an external analyzer tool, such as Splunk or syslog.

Before you begin

- This release supports only Splunk and `syslog` as external log analyzer.
- This release supports `syslog` only for Multi-Site Orchestrator in Application Services Engine deployments.

- This release supports up to 5 external servers.
- If using Splunk, set up and configure the log analyzer service provider.

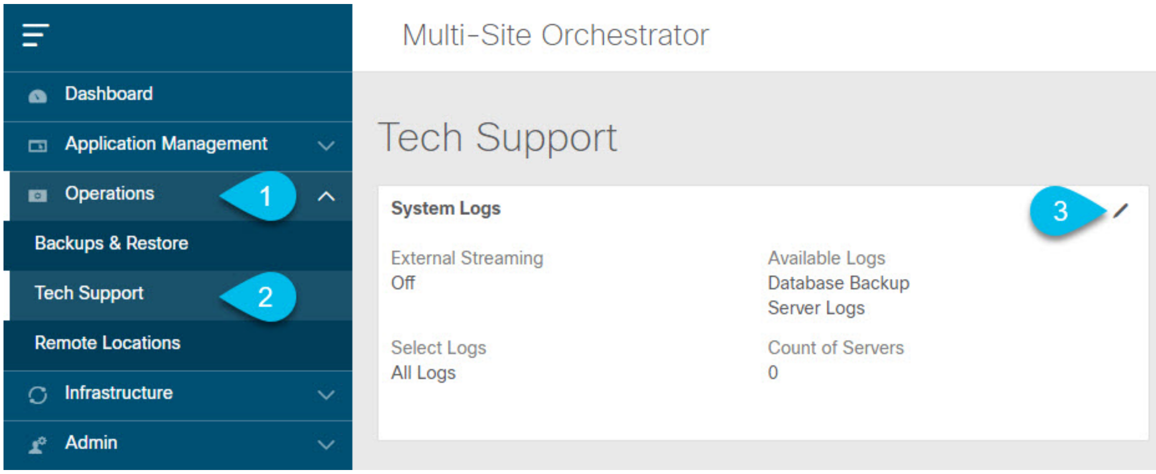
  For detailed instructions on how to configure an external log analyzer, consult its documentation.
- If using Splunk, obtain an authentication token for the service provider.

  Obtaining an authentication token for Splunk service is detailed in the Splunk documentation, but in short, you can get the authentication token by logging into the Splunk server, selecting **Settings** > **Data Inputs** > **HTTP Event Collector**, and clicking **New Token**.

Procedure

Step 1 Log in to your Multi-Site Orchestrator GUI.

Step 2 Open the **System Logs** screen.



External Streaming
Off

Available Logs
Database Backup
Server Logs

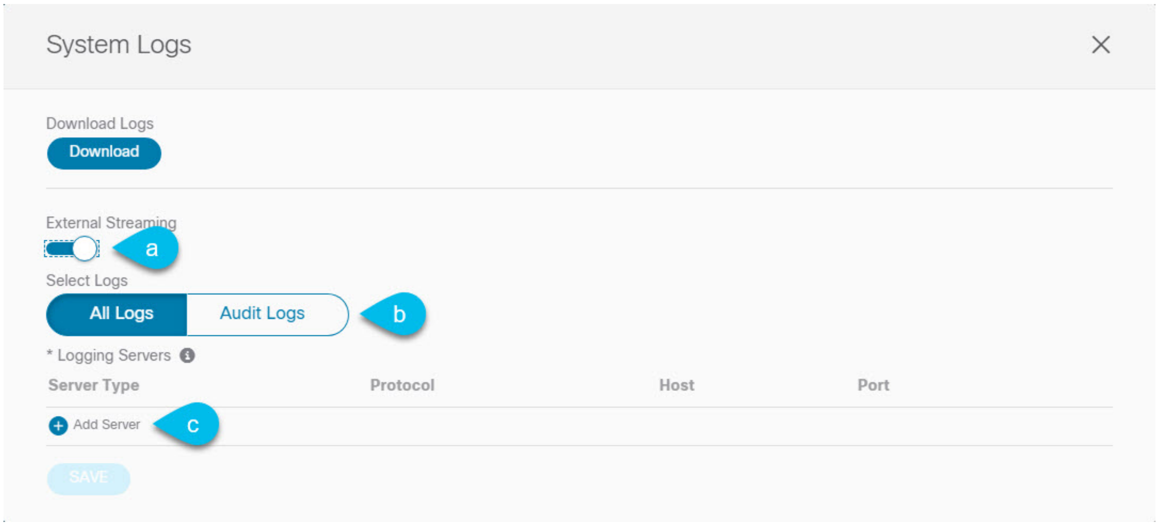
Select Logs
All Logs

Count of Servers
0

a) In the main menu, select **Operations** > **Tech Support**.

b) In the top right corner of the **System Logs** frame, click the edit button.

Step 3 In the **System Logs** window, enable external streaming and add a server.



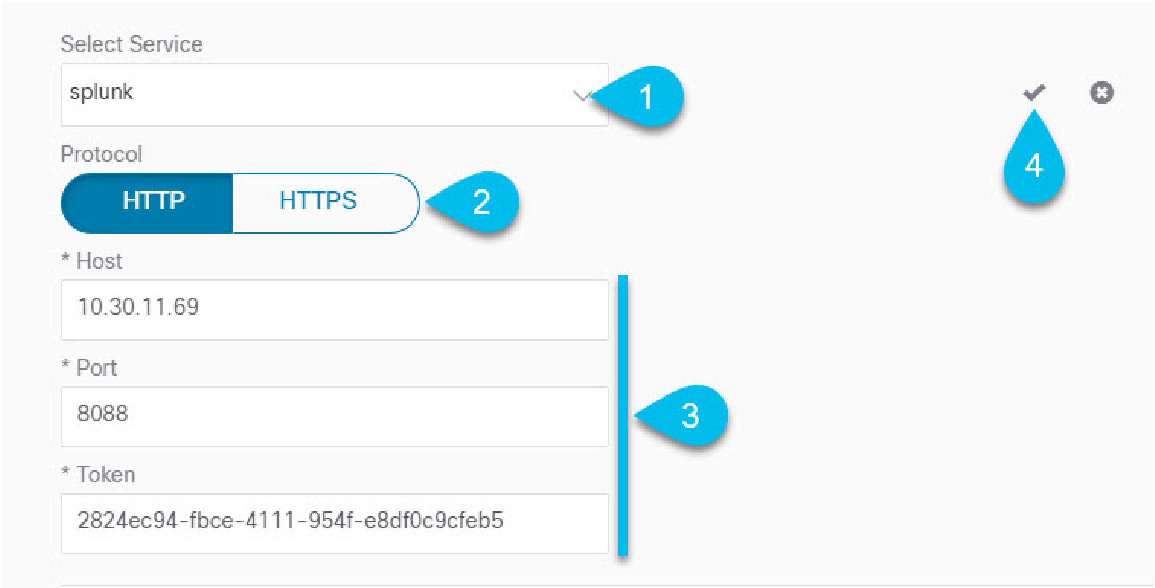
a) Enable the **External Streaming** knob.

b) Choose whether you want to stream **All Logs** or just the **Audit Logs**.

c) Click **Add Server** to add an external log analyzer server.

Step 4 Add a Splunk server.

If you do not plan to use Splunk service, skip this step.


Select Service: splunk

Protocol: HTTP | HTTPS

* Host: 10.30.11.69

* Port: 8088

* Token: 2824ec94-fbce-4111-954f-e8df0c9cfeb5

a) Choose `splunk` for the server type.

b) Choose the protocol.

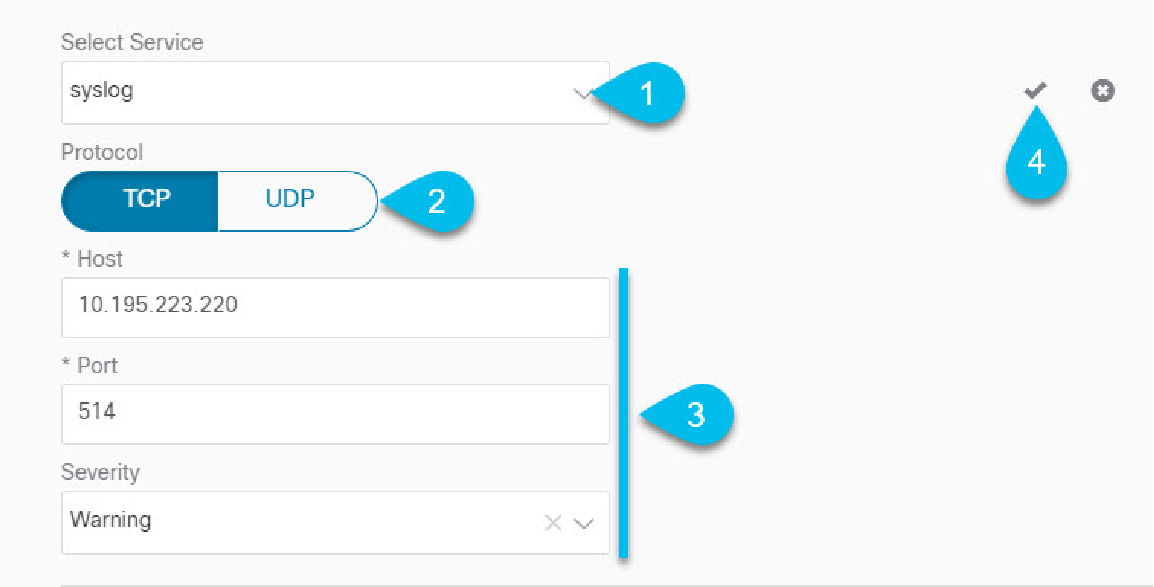
c) Provide the server name or IP address, port, and the authentication token you obtained from the Splunk service.

Obtaining an authentication token for Splunk service is detailed in the Splunk documentation, but in short, you can get the authentication token by logging into the Splunk server, selecting **Settings** > **Data Inputs** > **HTTP Event Collector**, and clicking **New Token**.

d) Click the checkmark icon to finish adding the server.

Step 5 Add a `syslog` server.

If you do not plan to use `syslog`, skip this step.



Select Service: syslog

Protocol: TCP | UDP

* Host: 10.195.223.220

* Port: 514

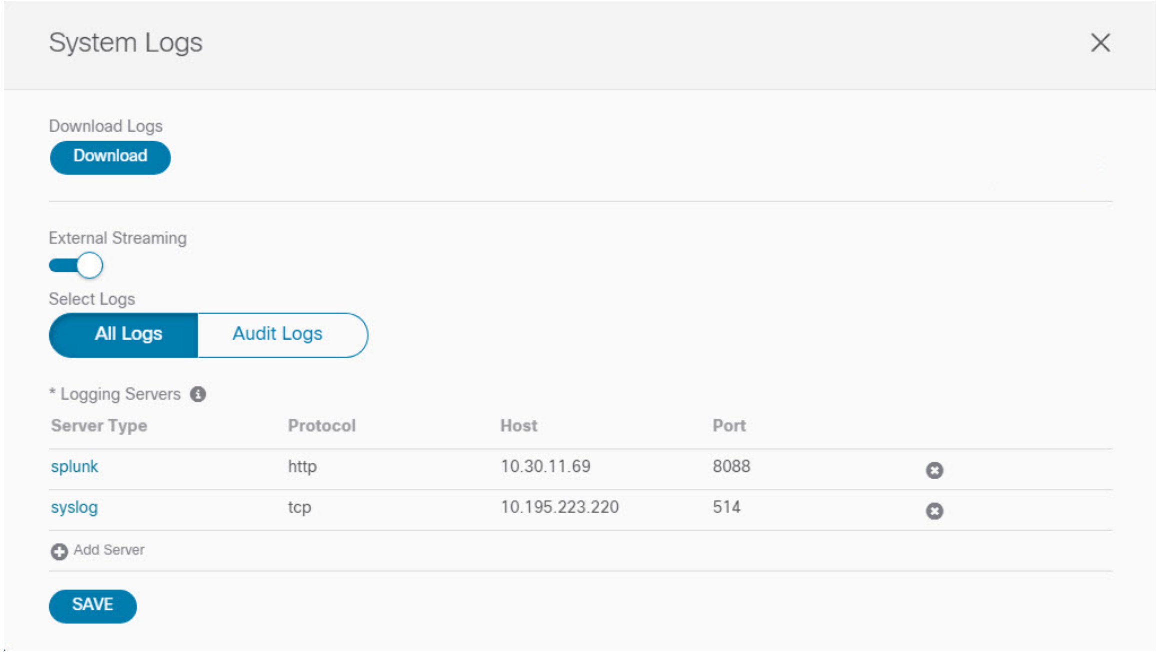
Severity: Warning

a) Choose `syslog` for the server type.
b) Choose the protocol.
c) Provide the server name or IP address, port number, and the severity level of the log messages to stream.
d) Click the checkmark icon to finish adding the server.

Step 6 Repeat the steps if you want to add multiple servers.

This release supports up to 5 external servers.

Step 7 Click **Save** to save the changes.



System Logs

Download Logs

External Streaming

Select Logs

* Logging Servers

Server Type	Protocol	Host	Port
splunk	http	10.30.11.69	8088
syslog	tcp	10.195.223.220	514