



Cisco Crosswork Situation Manager 7.2.x Administrator Guide

Powered by Moogsoft AIOps 7.2

Table of Contents

Administrator Guide	3
Apply a Cisco Crosswork Situation Manager License	3
Reporting and Dashboards	3
Insights	3
Grafana Dashboards	4
Manage User Access.....	9
Manage Roles	10
Manage Users	14
Manage Teams	15
Automate Alert and Situation Workflow	16
Action States	16
Transitions	17
Auto Close	18
Workflow Engine	21
Cookbook.....	24
Configure a Cookbook	25
Configure a Cookbook Recipe.....	27
Situation Visualization	28
Troubleshooting and Diagnostic Tools.....	29
Implement Generic Server Tools	29
Implement Situation Server Tools.....	31
Implement Alert Server Tools	34
Implement Client Tools	36
Configure Hotkeys	41
Configure ChatOps Shortcuts.....	42
Additional System Configuration.....	42
Create Shared Alert and Situation Filters.....	43
Configure the Landing Page.....	43
Customize User Experience and Workflow	44
Create Link Definitions	46
Configure Alert and Situation Columns.....	48
Configure and Retrain Probable Root Cause	49
Configure Labs Features	50
Monitor Your Cisco Crosswork Situation Manager System.....	51
Self Monitoring.....	51
Audit Trail	58

Administrator Guide

The Administrator Guide contains topics about the various administrator functions you can perform in Cisco Crosswork Situation Manager.

Apply a Cisco Crosswork Situation Manager License

When you purchase Cisco Crosswork Situation Manager, Cisco provides you with a license key. After you install Cisco Crosswork Situation Manager, you can maintain your license key in the System Settings UI.

Navigate to Settings > System > Licensing to apply a new license or to view details of your current license. You can set up a system notification to alert you within 1 to 120 days of a pending license expiration.

To add a new license key, copy and paste the license text into the Add New License Key text box and click Update License. A green panel confirms "Your new license key has been applied" when you enter a valid license.

Reporting and Dashboards

You can take advantage of Cisco Crosswork Situation Manager [Insights](#) to analyze trends in operational performance. You can use the default dashboard or you can use Grafana to [create a custom dashboard](#).

Insights

Insights is built on the Stats API that exposes time-series data so you can report on:

- Active Situations, the teams they're assigned to, and the services they impact.
- Reoccurring Situations that could indicate deeper systemic issues.
- Key performance indicators like Mean Time To Resolution.

You can use the reporting tool of your choice to take advantage of the [Stats API](#). Otherwise, check out the Cisco Crosswork Situation Manager [app for Grafana](#) to view and modify the default dashboard. See [Grafana Dashboards](#) for more information.Stats API

Insights exposes a variety of statistics and metrics to help you understand your operations. For example, consider the valuable data in the default dashboard:



You can see how your teams are managing active Situations:

- View the number of open Situations system-wide and see how many open Situations are unassigned, unacknowledged or that have been reassigned.
- Identify if the number of open reoccurring Situations which can highlight areas of impact that need increased attention or resource allocation.

You can monitor the distribution of your Situations over time, to see which teams handle the most Situations and which services are most impacted by Situations. Key Performance Indicator metrics reveal how quickly Cisco Crosswork Situation Manager detects Situations and how quickly teams address open Situations over time:

- Mean Time To Detect: the mean time to detect a Situation from the first event time.
- Mean Time To Acknowledge: the mean time to acknowledge a Situation from the first event time.
- Mean Time To Resolution: the mean time to resolve a Situation from the first event time.

For details on all the available Insights, see the [Stats API](#).

Grafana Dashboards

You can view Cisco Crosswork Situation Manager statistics and reports in dashboards using [Grafana](#).

To set this up, you need to install Grafana, install the Moogsoft AIOps plugin and install the Grafana integration in Cisco Crosswork Situation Manager.

Before You Begin

Before you install the Moogsoft AIOps plugin, ensure you have met the following requirements:

- You have installed Grafana or you have a hosted instance of Grafana.

- Enable HTTPS if you are using an on-premises instance of Grafana. See the [Grafana docs](#) for how to edit the protocol, cert_file, and cert_key properties in the Grafana configuration .ini file. You can use the [Grafana Setup Tutorial](#) for an example of how to install Grafana on a host running Cisco Crosswork Situation Manager. [Configure Grafana Example](#)
- The port for Cisco Crosswork Situation Manager is open and accessible from Grafana.

Install the Moogsoft AIOps App

To install the Moogsoft AIOps [app](#) in Grafana, follow these steps:

- Install the app.
- Find it under Apps in your Grafana plugins and enter the following settings:

Field	Value
URL	<Your Cisco Crosswork Situation Manager URL>
User	Your Graze username
Password	Your Graze password

- Enable the app. A "Test Success" message appears if successful.

After you have set up the app, you can configure your dashboards.

Default Dashboards

You can configure the statistics that Cisco Crosswork Situation Manager collects depending on which dashboards you want to use. See [Configure Labs Features](#) for more details. You can also create a custom dashboard.

Global Situation Overview

The Global Situation Overview dashboard provides a broad overview of your Situation statistics, teams insights, and mean times to acknowledge, detect and resolve.

The dashboard's panels display the number of open Situations, unassigned Situations, reassigned Situations and recurring Situations. Other panels include the top 10 teams by open Situations, the top 10 services by open Situations, the number of Situations by status, the number of Situations by severity and a graph view of MTTA, MTTD and MTTR.



To edit the dashboard, click the header of any panel and edit the statistic endpoint or add a query. Alternatively, click Add Row at the bottom of the screen.

Team Situation Overview

The Team Situation Overview dashboard displays a broad overview of your team's Situation statistics, team insights and mean time to acknowledge and resolve.

The dashboard's panels display the number of reassigned Situations per team, the number of reoccurring Situations per team, number of Situations impacting each service per team, the number of Situations by status per team and the MTTA/MTTR for the team.



To edit the dashboard, click the header of any panel and edit the statistic endpoint or add a query. Alternatively, click Add Row at the bottom of the screen.

Team Workload Breakdown

The Team Workload dashboard provides an overview of how an individual team is performing in Cisco Crosswork Situation Manager.

The dashboard's panels pull statistical data about the MTTA/MTTR per team, the status of the team's Situations, and the number of comments made by the team.



To edit the dashboard, click the header of any panel and edit the statistic endpoint or add a query. Alternatively, click Add Row at the bottom of the screen.

Noise Reduction

The Noise Reduction dashboard displays an overview of the noise reduction performance of Cisco Crosswork Situation Manager.

This dashboard shows statistics including the number of accumulated events reduced into alerts and Situations over a period of time, the percentage reduction of events to alerts, the percentage reduction of alerts to Situations and the overall reduction.



To edit the dashboard, click the header of any panel and edit the statistic endpoint or add a query. Alternatively, click Add Row at the bottom of the screen.

Individual Stats Overview

The Individual Stats Overview dashboard allows you to view and compare statistics for multiple Cisco Crosswork Situation Manager users.

The dashboard includes Situation metrics, MTTA and MTTR, user activity, Situation stats by user, user performance overview and user activity overview.

By default, Cisco Crosswork Situation Manager collects statistical data for this dashboard for all users with the Operator role. You can add the 'collect_insights' permission to other roles if you want to include other users in the dashboard. See [Role Permissions](#) for more information.



Individual User Deep Dive

The Individual User Deep Dive dashboard provides an in-depth summary of different performance metrics for a single user.

The dashboard includes a user Situation metric overview, a user activity overview, a user performance overview, Situation stats by users, user activity overview and user performance overview. You can view a breakdown of specific statistics such as the number of Situations the user has acknowledged, assigned, closed, reassigned and how many they have open. You can also see which ChatOps tools the user has executed, the number of comments they have made, the number of invitations they have received, the number of alerts they have marked with PRC and the individual's MTTA and MTTR.

By default, Moogsoft AIOps collects statistical data for this dashboard for all users with the Operator role. You can add the 'collect_insights' permission to other roles if you want to include other users in the dashboard. See [Role Permissions](#) for more information.



Create a Custom Dashboard

You can add and configure custom dashboards to display different Cisco Crosswork Situation Manager statistics in Grafana. For more information see the [Grafana documentation](#). To create a dashboard, follow these steps:

- Log in to your Grafana instance.
- Click + and Dashboard.
- Configure the dashboard to meet your requirements. For more information on the available API endpoints and statistics see the [Stats API](#).

Once created, statistics from Cisco Crosswork Situation Manager appear in the dashboard.

Manage User Access

As an Administrator, you control user access to functions in the Cisco Crosswork Situation Manager UI. This ensures that authorized users can perform required functions and prevents unauthorized users from accessing the system and sensitive operations within it.

Functions you can restrict include the ability to assign alerts, assign Situation owners, mark alerts with Probable Root Cause (PRC) feedback, and access Integrations.

Follow these steps to manage user access:

- Create roles for specific job functions.
- Assign the permissions to perform operations to roles.
- Enable user authentication via SAML or LDAP, or manually create users.
- Specify a role for authenticating users, or manually assign roles to users.
- Set up teams (optional).

Manage Roles

Roles group the permissions that users need to perform a set of tasks within Cisco Crosswork Situation Manager. You can create roles for specific job functions and assign them the permissions to perform certain operations. For example, you could create a role named Situation Manager and assign it the permissions to perform certain operations, such as managing alerts and Situations.

You must assign at least one role to every user. You can do this manually when you create the user or you can map roles to users if you use SAML.

Cisco Crosswork Situation Manager contains a set of predefined roles with a predefined set of permissions. See [Role Permissions](#) for details.

Create, Edit and Delete Roles

To view a list of roles, navigate to Settings > Roles. You can use the search box on the left to filter the list.

Select a role to view and edit its configuration. You can edit the following:

- Selected permissions: See [Role Permissions](#) for a description of each permission.
- Session timeout: You can use the system timeout of 60 minutes or define a custom timeout period.
- Landing page: You can choose to inherit the landing page from the system configuration or select an alternative page.

You can also perform the following operations:

- Click + to create a new role.
- Click a role name and then - to delete a role.

You cannot delete a role that is assigned to users. Remove the role from all users first.

Role Permissions

Cisco Crosswork Situation Manager contains the following predefined roles: Super User, Administrator, Manager, Operator, Customer, and Grazer. The REST LAM Sender role is designed for use with REST LAM integrations. The role restricts UI functionality, so you should not assign it to UI users. The default permissions selected for these roles are as follows:

Permission	Description	Super User	Administrator	Manager	Operator	Customer	Grazer
add_media	Attach files to the collaborate tab in Situations and Team Room. Upload a photo to a user avatar.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
alert_assign	Assign alerts.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
alert_close	Close alerts.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

alert_modify	Manage alerts including changes to significance and severity.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
all_data	View all data. Users without this permission can only view Situation and alert data related to their teams.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
collab_read	View content, such as files and comments, added by other users, on the Collaborate tab within Team and Situation Rooms.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
collab_write	Add content, such as files and comments, on the Collaborate tab within Team and Situation Rooms.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
collect_insights	Collect statistics for users with this role for Insights dashboards.				<input checked="" type="checkbox"/>		
filters	Create and edit the user's own personal	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

	Situation and alert filters.						
graze_login	Log into the Graze API.						✓ <input type="checkbox"/>
manage_integrations	Access the Integrations tab.	✓ <input type="checkbox"/>					
manage_maint	Manage maintenance windows.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
mobile	Access the Cisco Crosswork Situation Manager application on a mobile device.						
moderator_assign	Assign a Situation owner.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
prc_feedback	Mark alerts with Probable Root Cause feedback.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
sig_close	Close Situations.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
sig_create	Create Situations manually and from alerts.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
sig_modify	Manage Situations including changes to descriptions , queues and alerts.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
sig_resolve	Resolve a Situation.	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>		✓ <input type="checkbox"/>
sig_visualize	Access information on what created a	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>				✓ <input type="checkbox"/>

	Situation.						
super_privileges	Super user privileges. Enables access to all system settings and the ability to manage dashboards, alert and Situation filters, templates, users, and roles.	✓ <input type="checkbox"/>					✓ <input type="checkbox"/>
thread_create	Deprecated permission	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>
view_summary	View the Summary screen. If you remove this permission, the user can no longer access the Summary screen that appears on the system's default landing page. If you remove this permission and the user's landing page is the Summary screen, Cisco Crosswork Situation Manager redirects the user to the Open Situations screen	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>	✓ <input type="checkbox"/>

	instead.						
--	----------	--	--	--	--	--	--

Manage Users

As with most software systems, you use user credentials to provide secure access to Cisco Crosswork Situation Manager for your personnel. You can use the System Settings UI to manage the various attributes that define users and the actions they are allowed to perform inside Cisco Crosswork Situation Manager.

As an alternative to managing users in the UI, you can configure the system to allow Single Sign-On (SSO) via the Security Assertion Markup Language (SAML) protocol. If you have a large number of users, enabling SSO saves you from setting them up individually. It also improves security by requiring users to remember a single complex password instead of multiple credentials for multiple systems.

Within the SAML configuration you can specify a role, primary group and team to assign to users when they authenticate for the first time. See [Configure Single Sign-On with SAML](#) for more information. You can also authenticate users with Lightweight Directory Access Protocol (LDAP). See [Configure Single Sign-On with LDAP](#) for more information. Configure Single Sign-On with SAML Configure Single Sign-On with LDAP

Manually Create and Edit Users

To view a list of users, navigate to Settings > Users. Use the search box on the left to filter the list. You can click the person icon to toggle the display of inactive users. Click + to create a new user or select a user to view and edit their attributes. You cannot delete users. The system retains a history of all user activity, including collaboration posts and ownership of alerts and Situations. You can set obsolete users to inactive in the Personal tab. Cisco Crosswork Situation Manager includes the following predefined users:

- Administrator: Super user role. For information on creating and editing roles, see [Manage Roles](#).
- Graze API user. Grazer role. This user is intended for system integration purposes, it is not a UI user.
- System Owner: Super user role.
- Moog. An anonymous system account used for unassigned alerts and Situations.

We recommend that you change the default password for each predefined user. Once you have set up your own users or enabled user authentication you may wish to deactivate the predefined users.

Edit User Details

Navigate to the Personal tab to view or edit the following user details:

- Username with 32 characters maximum. Mandatory.
- Full name.
- Password. If you do not enter a password the user is created as an LDAP user.
- Primary group. Mandatory.
- Department.
- Time zone if different to the system time zone.
- Active status. Inactive users cannot log into the UI. New users are active by default.
- Timeout. You can use the role timeout of 60 minutes or define a custom timeout period between 60 and 720 minutes (12 hours).

You can view or edit the user's email address or telephone number on the Contact tab.

Manage a User's Roles

Roles group the permissions users need to perform a set of tasks within Cisco Crosswork Situation Manager. See [Manage Roles](#) for information on creating and editing roles. You must assign at least one role to each user.

Assign a User Competencies

You can use competency rankings to indicate the user's level of expertise. Double-click the ranking and use the up and down arrows to adjust the number.

Assign a User to Teams

You can optionally group users into teams, to ensure that users working together view the Situations that are relevant to them. You can configure Cisco Crosswork Situation Manager to assign Situations to a particular team if they impact selected services or meet other criteria. See [Manage Teams](#) for further information.

Manage Teams

You can use the optional Teams feature in Cisco Crosswork Situation Manager to allow users working together to view the Situations that are relevant to them. You can configure the system to automatically create teams based on certain Situation data, or you can manually create teams.

Create and Edit Teams

To view a list of teams, navigate to Settings > Teams. Use the search box on the left to filter the list. You can click the people icon to toggle the display of inactive teams.

- Click + to create a new team.
- Click a team name and then the copy icon to duplicate a team.

You cannot delete teams. The system retains a history of all team activity. You can set obsolete teams to inactive in the General tab.

To create a team, you must assign the team a name with a maximum of 64 characters. You can optionally provide a description of the team.

By default, teams are active. Deselect the Active checkbox to deactivate a team. Inactive teams don't appear in team rooms and cannot have Situations assigned to them.

Navigate to the Users tab to select the users that belong to this team. You can define an alternative landing page for the team members on the Settings tab.

Create Automatic Teams

You can configure Cisco Crosswork Situation Manager to create teams based on current Situation data.

Note: Creating automatic teams sets all existing teams to inactive.

You can create teams based on any of the following Situation fields:

- Description
- Services Impacted
- Process Impacted
- Queue

After Cisco Crosswork Situation Manager creates a team, you can view and edit the team settings and membership.

Configure Team Permissions

You can filter data visible to team members according to services, Situations or alerts:

- Create a Service Filter in General to select services for which the team views affected Situations. Adding more than 200 services may affect system performance and stability.
- Create a Situation Filter in General to select the Situations that you can assign to members of the team. If you only want team members to be able to see these Situations, ensure they do not have the 'all_data' permission. See [Role Permissions](#) for details.
- Create an Alert Filter in Settings to select the alerts outside the team's Situation Filter that you want the team members to see.

Permissions are additive. Therefore, if you set several filters, Situations and alerts that meet any one of them are included. For example, you could set up a team's permissions so that the team views critical Situations affecting a database service, a messaging service, and a web service.

The **all_data** permission in a user role overrides the filters in team settings. Users with the 'all_data' permission can view all Situations and alerts.

If you want users to see only the alerts and Situations that are assigned to their team, configure roles and users as follows:

- Create a role without the **all_data** permission.
- Assign the role to the users.
- Add the users to the team.

See [Manage Roles](#) and [Manage Users](#) for more information.

Automate Alert and Situation Workflow

As an administrator, you can automate the alert and Situation workflow to maximize the efficiency of alert and Situation processing within Cisco Crosswork Situation Manager.

You need to define Action States and Transitions that will be used by the [Alert Rules Engine](#). The Alert Rules Engine processes alerts based on certain criteria and uses the Transitions to move these alerts to different Action States. Using the Alert Rules Engine to capture [link up-link down](#) conditions or as a [Heartbeat Monitor](#) ensures that alerts do not form Situations unnecessarily. Alert Rules Engine Link Up-Link Down Example Heartbeat Monitor

You can also use the Auto Close feature to define criteria for automatically closing alerts and Situations. This housekeeping feature ensures that alerts and Situations are closed in a timely manner.

Action States

Action States are the different states which alerts are placed into as they pass from the [Alert Builder](#) into the [Alert Rules Engine](#). See the [Alert Rules Engine](#) for a standard [link up-link down](#) example that uses Action States. Alert Builder Alert Rules Engine Alert Rules Engine Link Up-Link Down Example

The different states define how long the alerts are retained in a certain state and whether they are forwarded to any Moollets or Sigalisers. The default or base state is called 'Ground'. It is required for the system to function correctly and cannot be deleted. This is the state that alerts have when they enter the Alert Rules Engine.

Create an Action State

Click + to create a new Action State. The available fields are as follows:

Field	Input	Description
Name	String (Mandatory)	Name of the new Action State (up to a maximum of 64 characters).
Description	String	Description of the new Action State.
Remember Alerts For	Integer	Time in seconds that the system remembers the alerts in this state for. Any number less than 0 (<0) means do not remember it, so the state never retains a memory of the alert. 'Ground' has -1 because you do not want to accumulate a memory of every alert in the system. By default, you want the alert to pass to a Sigaliser. The purpose of the state engine is to spot specific alerts and do different things with them.
Cascade on Expiry	Boolean	Specifies what to do if you have set a time to remember alerts for. For example, the alert goes into the state and then after the set time of 30 seconds it is taken out of the state whether you dispose of it manually or return it back to its original state.
Forward Alerts	Boolean	If enabled, the alerts that enter this state are forwarded to the chain Moolet.
Close Filter	Filter	Defines which alerts are closed when they enter the state.
Entry Action	String	Moobot function that is called when an alert enters the state.
Exit Action	String	Moobot function that is called when an alert exits the state.

Click Save Changes to continue. Alternatively, click Revert Changes to undo any changes. The new Action State appears on the list to the left.

Delete an Action State

Select the Action State you want to delete from the list on the left.

Click - to delete the Action State. The pop-up confirmation window appears. Click Yes to confirm the deletion.

Transitions

Transitions are a user-configurable set of conditions that move an alert from one state to another within the [Alert Rules Engine](#) (ARE). Transitions result in the following:Alert Rules Engine

- Alerts move from one Moolet to the next Moolet in the chain.
- Alerts pass to a Sigaliser which clusters them into Situations.

To create and configure different transitions go to System Settings.

Create a New Transition

Click + to create a new transition and edit the fields to meet your requirements:

Field	Input	Description
Name	String	Name of the transition. This can be up to 64 characters. Mandatory.

Description	String	Description of the transition.
Priority	Integer	Determines the priority of the transition if there are multiple transitions. The higher the value, the higher the priority.
Active	Boolean	Sets the transition to active.
First Match Only	Boolean	Transition only occurs once if an alert meets the trigger conditions.
Trigger Filter	Filter	Filter that triggers the transition if an alert meets the defined trigger filter parameters. Mandatory.
Inclusion Filter	Filter	Filter that passes additional alerts to the end state if they arrive after the initial trigger and meet the defined inclusion filter parameters.
Start State	-	Determines the action state of the alerts in the inclusion filter. The start state and end state must be different. Mandatory.
End State	-	Determines the action state of the alerts if they match the inclusion or trigger filters. The start state and end state must be different. Mandatory.

When you have configured the transition, click Save to continue.

Delete a Transition

To delete a transition from the list of available transitions:

- Select the transition to delete.
- Click - to delete the transition.
- Click Yes to confirm the deletion.

Auto Close

The Auto Close feature lets you define criteria for automatically closing alerts and Situations. Auto Close enables you to use filtering rules to organize your data and keep it current so you can focus on the most important active alerts and Situations.

You also see performance improvements because automatically closing old alerts and Situations reduces the amount of data involved in statistic calculations.

Auto Close lets you define the conditions using filters and determine how often Cisco Crosswork Situation Manager checks which alerts and Situations to close. Any alerts and Situations older than a certain time and that meet the defined criteria are closed.

Configure Auto Close for Situations

The [Housekeeper Moolet](#) must be configured and running within Moogfarmd in order for Auto Close to work. Housekeeper Moolet

To configure which Situations should be auto closed, create a filter as follows:

- In the Auto Close > System Settings window, click Edit Filter to open the filter editor.
- Clear the filter using Empty Filter and Add Clause. Alternatively, you can manually type in your filter rules. You can set up as many auto close rules as you like. In a rule, you can either include or exclude Situations for auto closing but you cannot use both together. See [Filter Search Data](#) for reference. Filter Search Data

- Apply the changes to continue and click Done.
- After you add the filter, define the behavior for automatically closing Situations as follows:
- Close the Situation and all the alerts it contains.
- Close the Situation and all the unique alerts it contains. Unique alerts are any alerts that are not part of any other Situations.
- Close the Situation only.
- You can create tasks to configure:
 - The age when Situations are suitable for Auto Close.
 - The number of Situations to close in each Auto Close run.
 - Situations only close if all associated alerts are closed.

Edit the default task or click Add Task. The available settings are as follows:

Setting	Input	Options	Description
Situation Age	Integer	Minutes Hours Days	Defines how old a Situation must be for Cisco Crosswork Situation Manager to auto close it. To calculate age, the system looks at both the Situation's last_event_time and last_state_change. Must be a number greater than 1.
All Alerts closed	Boolean	-	If enabled, only Situations with no open alerts qualify for automatic closure.
Match filter	Filter	-	Defines the criteria a Situation must meet to qualify for automatic closure.
Batch size	Integer	-	Defines the maximum number of Situations to auto close in each Auto Close run. Defaults to 1000. Must be a number greater than 1.

Once saved, the Auto Close task runs after a set period of time. This time period is between five minutes and four hours depending on the age of the Situation.. The older the Situation age, the closer the frequency of the task gets to four hours (see the example below). There is no limit on the number of tasks, so you can add any as many as you need meet your requirements.

The example below demonstrates how you can configure an Auto Close task to close a maximum of 1000 Situations per run that meet the following criteria:

- Older than 23 hours.
- All associated alerts are closed.
- Have a clear severity.

Configure Auto Close for Alerts

To configure which alerts should be auto closed, on the System Settings > Auto Close window, select the Alerts tab and create a filter as follows:

- Click Edit Filter to open the filter editor.
- Clear the filter using Empty Filter and Add Clause. Alternatively, you can manually type in your filter rules. You can set up as many auto close rules as you like. In a rule, you can either include or exclude alerts for auto closing but you cannot use both together. See [Filter Search Data](#) for reference.
- Apply the changes to continue and click Done.
- You can create tasks to configure:
 - The age when alerts are suitable for Auto Close.
 - The number of alerts to close in each Auto Close run.

Edit the default task or click Add Task. The available settings are:

Setting	Input	Options	Description
Alert age	Integer	Minutes Hours Days	Defines how old the alert must be for Cisco Crosswork Situation Manager to auto close it. To calculate age, the system looks at the last time an event was received from a LAM for that alert. Must be a number greater than one.
Match filter	Filter	-	Defines which alerts to include in the batch being auto closed.
Batch size	Integer	-	Defines the maximum number of alerts to auto close in each Auto Close run. Must be a number greater than one. This is 1000 by default.

Once saved, the Auto Close task runs after a set period of time. This time period is between five minutes and four hours depending on the age of the alert. The older the alert age, the closer the frequency of the task gets to four hours.

There is no limit on the number of tasks, so you can add any as many as you need meet your requirements.

The example below demonstrates how you can configure a task to Auto Close a maximum of 1000 alerts per run that meet the following criteria:

- Older than 45 minutes.

- Have a clear severity or a minor severity.

Workflow Engine

Note: This feature is an Early Access Feature. An administrator can enable it at Settings > Labs > Configure > Early Access Features.

Implementers and administrators can use Workflow Engine to add custom logic for event, alert and Situation processing in Cisco Crosswork Situation Manager.

Workflow Engine includes a few default workflows to help you get started:

- "Closed Alerts Filter" prevents further processing of closed alerts.
- "Closed Situation Filter" prevents further processing of closed Situations.
- "Automated Ticketing" enables automatic ticketing using existing integrations with your incident management systems.

Other scenarios where you can implement the Workflow Engine include:

- Controlling stateful workloads. For example, holding a "link down" event until Cisco Crosswork Situation Manager receives a corresponding "link up" event within a time limit.
- Integrating with automation frameworks for automated remediation of alerts such as if a disk space alert being received.
- Extracting, transforming, and routing data for events, alerts, and Situations within Cisco Crosswork Situation Manager.
- Detecting the absence of events because of a missing keep alive event from a predictable source.

You can have multiple workflows running in for different types of engines. The three available types of Workflow Engine are:

- Event Workflow Engine
- Alert Workflow Engine
- Situation Workflow Engine.

Each Workflow Engine is a Moolet that you can configure in the the Cisco Crosswork Situation Manager UI. By default Cisco Crosswork Situation Manager has four workflow engines:

Name	Type	Position	Description
Event Workflows	Event	After the LAMs publish a message on the Message Bus.	Workflows for event messages use cases.
Enrichment Workflows	Alert	After Alert Builder but before Maintenance Window Manager.	Workflows for alert enrichment or prior to maintenance use cases.

Alert Workflows	Alert	After Maintenance Window Manager.	Workflows for after alert maintenance.
Situation Workflows	Situation	After Situation Manager.	Workflows for Situation use cases.

Manage Workflow Engines

Note: This feature is an Early Access Feature. An administrator can enable it at Settings > Labs > Configure > Early Access Features.

You can access the Workflow Engine at Settings > Automation in the Cisco Crosswork Situation Manager UI.

When you open the Workflow Engine, you see workflow tabs for Workflow Engine configuration types you can enable at startup.

Warning: There are breaking changes for Workflow Engine between v7.2.0 and v7.3.0. Upon upgrade, you may need to recreate your actions.

You can create and configure individual workflows or chains of workflows in the Cisco Crosswork Situation Manager UI.

Click +Add Workflow to create a workflow or double-click an existing workflow to open it.

Edit the Workflow Definition as follows to control which data the engine processes:

Workflow Property	Description
Workflow Name	Identifies the workflow.
Description	Describes the purpose of the workflow and what it should do.
Entry Filter	Identifies the criteria for events, alerts, or Situations to process with the current engine. Anything that doesn't meet the criteria skips to the next engine or Moolet in the chain. For example, you can set a filter on "severity > 3" to process only Major and Critical severity alerts. See /document/preview/35090#UIDf7925c4a2878b75931b6f34600f25045 for information on creating filters. Filter Search Data
Sweep Up Filter	Check the database for all objects that match the filter criteria and pass them to all workflow actions as a list parameter. The sweep up filter expedites entry of related objects into the workflow. For example if you receive a link-up alert, you can set a filter to retrieve all related link-down alerts from the database and have the sweep up filter close them.
First Match Only	Allow only the first occurrence of an object to pass through the workflow.

You can use the slider in the title bar to set the engine to Active or Inactive.

If you have multiple workflows, you can use the up and down arrows in Edit mode to reorder them. Alternatively, you can drag and drop the workflows into order.

After you create an engine, you can add [actions](#) to process data. When the engine is active, it process all objects that match the filtering criteria according to the actions.

Manage Workflow Engine Actions

Note: This feature is an Early Access Feature. An administrator can enable it at Settings > Labs > Configure > Early Access Features.

After you have defined the data you want to process using a Workflow Engine in Cisco Crosswork Situation Manager, you can set up actions to programmatically transform the data and control the data flow.

Warning: There are breaking changes for Workflow Engine between v7.2.0 and v7.3.0. Upon upgrade, you may need to recreate your actions.

When you edit an engine, you can click +Add Action to create a new action, or double-click an existing action to edit it.

Delay

By default, each workflow has a delay action. It is mandatory and you can not delete it. You can set the delay for up to 86,400 seconds (24 hours). If you set the Reset option

Actions

Define workflow actions as follows to add custom processing to events, alerts, or Situations depending on the type of engine:

Action Property	Description
Name	Identifier for the action. Must be unique within the workflow.
Function	<p>A Programmatic task based on JavaScript and Java functions. The available function list varies according to the object: event, action, or Situation.</p> <p>When you set the function, the UI displays its description and updates the Values to correspond to the function. For example, the contains action lets you check a field in your object for a matching values. See Workflow Engine Function Reference.</p>
Value	<p>Parameters for the function. The parameters vary from function to function. When you select a function, the UI updates the description of the parameters. For more information, see Workflow Engine Function Reference. and /document/preview/11736#UUID4fb1d287a35f949acb6fed44797e2f70.Alert and Event Field Reference</p>
Forwarding Behavior	Controls the data flow. For objects where the function returns true , you can choose to always forward to the next action or workflow, stop the current workflow, or stop all workflows for the object.

If you have multiple actions, you can drag and drop them to arrange them according to your requirements.

Workflow Engine Function Reference

Note: This feature is an Early Access Feature. An administrator can enable it at Settings > Labs > Configure > Early Access Features.

This is a function reference for Workflow Engine actions in Cisco Crosswork Situation Manager.

forward

Forwards objects to the destination Moolet.

moolet: String. The destination Moolet.

setClass

Sets the value of the **class** field to a constant for an object.

class: String. The value for the class.

containsAll

Checks for the existence of all the elements of an array in the value of a field in the object. A superset is valid as long as all values are present. For example, ['a', 'b','c'] satisfies the values ['a'] or ['a', 'c'].

field: String. The name of the object field.

values: Array. The required values for the field.

searchAndReplace

Matches a regular expression against a field and uses a map to replace the value of a destination field with the result. If you use multiple subgroups for the regular expression, you can match each one to a different object.

expression: String. The regular expression to apply to the field.

field: String. The source field of the object. For example **description**.

map: JSON. A map of the destination fields to the regular expression subgroup expressed as **\$extract.n** where n is the number of the subgroup. For example {"source": "\$extract.1", "custominfo.region": "\$extract.2"}.

setCustomInfoJSONValue

Sets the value for a new or existing key in **custom_info** to a JSON object. Keys can be complex.

value: JSON. The JSON you want to assign to the key in **custom_info**.

key: String. The destination key in **custom_info**.

setDescription

Sets the **description** field for the object to a static value.

description: String. The **description** value.

setType

Sets the **type** field for the object to a static value.

type: String. The **type** value.

Cookbook

Cookbook is a deterministic clustering algorithm in Cisco Crosswork Situation Manager that creates Situations defined by the relationships between alerts. You can configure Cookbook to cluster alerts

into Situations if they have specific characteristics such as temporal or topological proximity. Cookbook filters can include characteristics such as the following:

- Class or type
- Description
- Server priority
- Geographical location
- Environment classification

Each Cookbook is a collection of Recipes: sets of configurable filters, triggers, and other calculations, such as priority ordering and entropy threshold. A Cookbook can run multiple Recipes concurrently to process the incoming event stream and produce a variety of Situations. A Cisco Crosswork Situation Manager deployment may include multiple instances of Moogfarmd, each of which can run multiple Cookbooks.

You can configure a Cookbook and its recipes via the Cisco Crosswork Situation Manager UI. See [Configure a Cookbook](#) for details.

To use more advanced features, such as merging and Moobot-controlled Recipes in Moogfarmd, see [Configure a Cookbook Manually](#). Configure a Cookbook Manually

Cookbooks configured in the UI and in Moogfarmd can run concurrently.

Configure a Cookbook

Cookbook is a deterministic clustering algorithm in Cisco Crosswork Situation Manager that creates Situations defined by the relationships between alerts.

When you add a Cookbook via the UI, you can only configure the visible properties. Cookbook requires at least one active Recipe in order to function and cluster alerts into Situations. See [Configure a Cookbook Recipe](#) for more details.

If you want to implement a more complex Cookbook with advanced configuration and additional properties, see [Configure a Cookbook Manually](#). Refer to [Cookbook and Recipe Reference](#) to see all available properties. Cookbook and Recipe Reference

Before You Begin

Before you set up your Cookbook via the UI, ensure you have met the following requirements:

- You have set up the Recipes you want your Cookbook to use. See [Configure a Cookbook Recipe](#) for details.
- Your LAMs or integrations are running and Cisco Crosswork Situation Manager is receiving events.
- You have configured the Moolet that is the source of the alerts for the Cookbook. You select the source using the **process_output_of** property.

Create a Cookbook

To create a new Cookbook from the UI:

- Navigate to the Settings tab.
- Click Cookbooks in the Sigaliser section.

- Click the + icon to create a new Cookbook. See the [Cookbook and Recipe Reference](#) for a full description of all properties. You cannot configure some properties from the UI. Cookbook and Recipe Reference
- Fill in the properties to name and describe the Cookbook:
 - name: Name of the Cookbook (required).
 - description: Text description of the Cookbook.
- Configure the Cookbook's input and clustering behaviour:
 - process output of: Defines Moolet source of the alerts for the Cookbook (required).
 - cluster by: Determines the Cookbook's clustering behavior.
 - entropy threshold: Minimum entropy value an alert must have in order for Cookbook to cluster it into a Situation.
 - cook for: Period of time that Cookbook clusters alerts for before the recipe resets and determines when to start a new cluster.
 - scale by severity: Treat alerts with a high severity value like alerts with a higher entropy value.
 -
- Configure which recipes that Cookbook uses and when it uses them:
 - first recipe match only: Enables a priority order for recipes in the Cookbook.
 - selected recipes: Determines the Cookbook's clustering behavior.
- Click Save Changes to create the Cookbook.
- To enable the new Cookbook, return to System Settings and click Cookbook Selection.
- Move the new Cookbook to Active Cookbooks and click Save Changes.

Select a Cookbook

After completing the configuration, you can activate the new Cookbook to run alongside any existing active Cookbooks:

- Navigate to the Settings tab.
- Click Cookbook Selection in the Sigaliser section.
- Move the Cookbook under 'Active Cookbooks' using the arrow icons.
- Click the Merging tab and choose the merging option you want to use:
 - Resultant Situations from active Cookbooks are not to be merged together. Default.
 - Resultant Situations from active Cookbooks are eligible to be merged together if they share a degree of similarity. The similarity is set using the slider.
- Click the Advanced tab configure if you want Cisco Crosswork Situation Manager to purge closed and superseded Situations from moogfarmd. Define how often you want the purge to occur in hours and minutes.
- Save any changes.

Changes to the settings initiate a restart of Moogfarmd and all running Cookbooks.

Configure a Cookbook Recipe

A Cookbook Recipe is a set of configurable filters, triggers, and calculations that defines the type of alerts and the alert relationships that Cookbook detects and clusters into Situations.

Cookbook requires at least one active Recipe in order to function and cluster alerts into Situations. When you add Recipes via the UI, you can only configure the visible properties. Refer to [Cookbook and Recipe Reference](#) to see the available properties. You can only configure two recipe types from the UI: Cookbook and Recipe Reference

- CValueRecipeV2: Default Recipe that extracts and analyzes groups of consecutive characters to measure text similarity between alerts.
- CValueRecipe: First version of the CValue Recipe that uses a string comparison mechanism to determine text similarity between alerts.

See [Recipe Types](#) for more details on the different types of recipes available in Cookbook. If you want to implement a more complex Cookbook such as the CBotRecipe that allows you to call Moobot functions, see [Configure Recipe Manually](#) .Recipe TypesConfigure a Recipe Manually

Before you Begin

Before you set up your Recipe via the UI, ensure you have met the following requirements:

- Your LAMs or integrations are running and Cisco Crosswork Situation Manager is receiving events.
- If you want to use Vertex Entropy or hop limit in your Recipes, you have imported your network topology. See [Import a Topology](#) .Import a Topology

Create a Cookbook Recipe

To create a new Cookbook Recipe from the Cisco Crosswork Situation Manager UI:

- Navigate to the Settings tab.
- Click Cookbook Recipes in the Sigaliser section.
- Click the + icon to create a new Recipe. See the [Cookbook and Recipe Reference](#) for full descriptions of all properties. Some of these properties cannot be configured from the UI.Cookbook and Recipe Reference
- Fill in the properties to name and describe the Recipe:
 - Name: Name of the Recipe (required).
 - Description: Text description of the Recipe.
 - Situation description: Description that appears in Situations that the Recipe creates.
 - Recipe Type: Type of recipe. The only options are Value Recipe and Value Recipe 2.
 - Configure the Recipe behavior and filters that define the alert relationships:
 - Trigger Filter: Determines the alerts that Cookbook considers for Situation creation.
 - Exclusion Filter: Determines the alerts to exclude from Situation creation.
 - Seed Alert Filter: Determines whether to create a Situation from a seed alert.
 - Rate Filter: Determines the minimum event rate per minute required for Cookbook to create a Situation.

- Alert Threshold: Maximum number of alerts to cluster before Cookbook creates a Situation.
- Cook For: Time period that Cookbook clusters alerts for before the recipe resets. The Recipe cook_for value overwrites the Cookbook cook_for value.
- Configure the alert matching properties for the Recipe:
- Cluster By: Defines how Cookbook matches alerts to clusters.
- Hop Limit: Maximum number of hops between the alert source nodes in order for the alerts to qualify for clustering.
- Navigate to the Clustering tab.
- Click the + icon to add alerts fields you want Cookbook to factor in when clustering alerts.
- Use the slider to edit the similarity threshold for each field. The value determines the required percentage similarity for Cookbook to cluster a set of alerts.
- If you want to use custom info fields, configure the [Match List Items](#) option. See [Match List Item in Recipes](#) for details.
- If you are configuring a Value Recipe, check the **case_sensitive** property if you want the text similarity calculation to factor in case sensitivity.
- If you are configuring a Value Recipe 2, select whether you want Cookbook to calculate text similarity using shingles or words. If using shingles, select the **shingle_size** property. The default '3' is the optimal size.

When the configuration is complete, the changes are applied to any active Cookbooks that use the Recipe as soon as you save the changes. If the Recipe has not been added to an active Cookbook, go to Settings > Cookbook and move the Recipe under Selected Recipes for that Cookbook.

Situation Visualization

Caution

The Visualize tab is a "Labs Feature". Enable the Visualize feature in Labs to view it in the Situation Room. See [Configure Labs Feature](#) for details. Your role must have the "sig_visualize" permission to use this feature. See [Manage Roles](#) for details.

Currently, Cisco Crosswork Situation Manager does not handle fully alerts that a user has manually added to a Situation in this Early Access version of the Visualize feature. For example, manually added alerts do not display in a component diagram if their similarity to the reference alert is below the threshold but they will appear in another diagram if their similarity is above the threshold for that component.

The Visualize tab in Situation Rooms allows administrators and implementers to see which process created a Situation and the similarity of the alerts within the Situation. You can use this information to adjust your Cisco Crosswork Situation Manager configuration to improve the relevance of the Situations it creates.

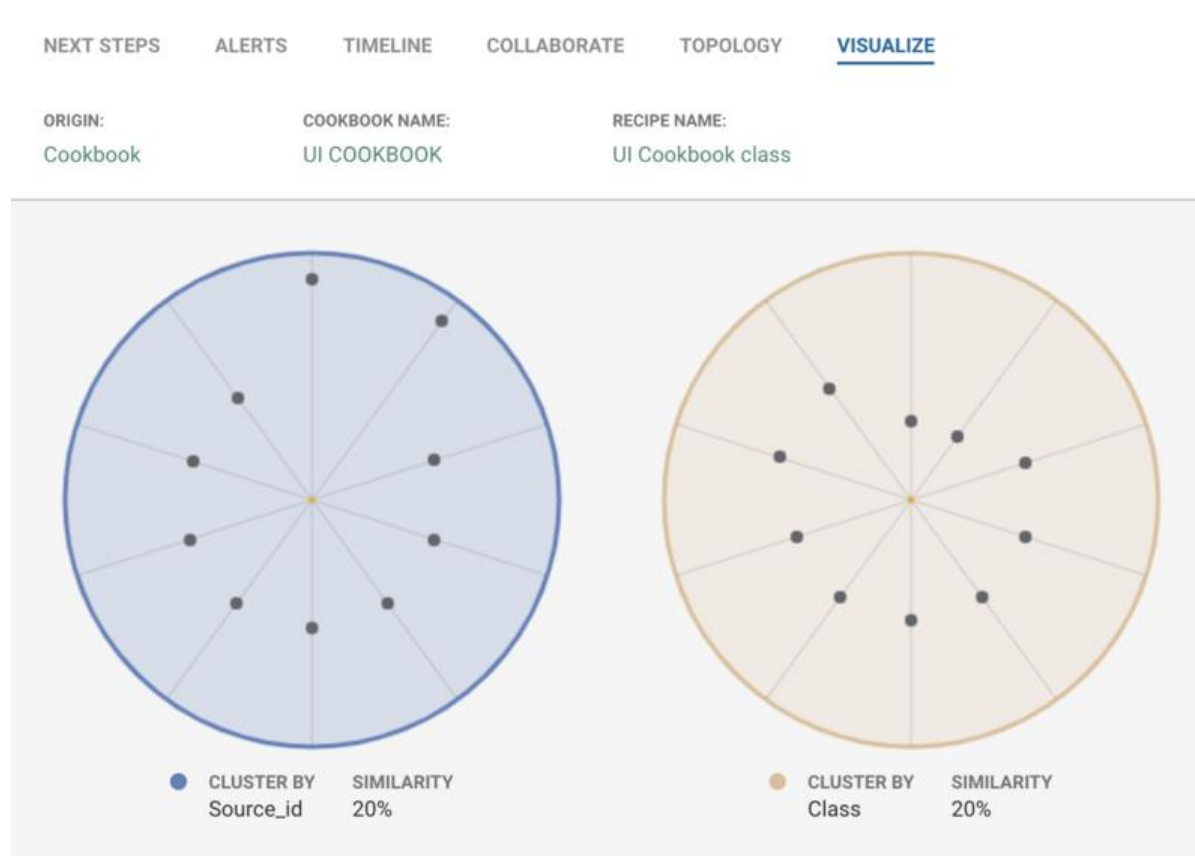
This tab displays the origin of the Situation and additional detail depending on the origin. For example:

- Cookbook Recipe: Cookbook and Recipe names.
- Manual Situation creation: User ID who manually created the Situation.
- Situations merged: UID of the user who merged the Situations and the merged Situation IDs.

To view the Visualize feature, go to a Situation Room and click the Visualize tab.

The Visualize tab shows diagrams of the alerts in the Situation according to how the Cookbook Recipe has clustered them. In the example below, this Situation has ten alerts which are clustered by two components: Source ID and Class. The Cookbook Recipe clusters alerts whose Source ID is at least 20% similar to the reference alert and whose Class is also at least 20% similar to the reference alert. The reference alert may be a seed alert or simply the first alert that the Cookbook Recipe added to the cluster.

Each diagram shows the similarity of the alert to the reference alert for one of the components. The reference alert has a similarity of 100% and is shown at the center of the circle. Alerts with a high similarity display closer to the center of the circle and alerts with a low similarity display nearer the edge of the circle. Alerts that are only 20% similar would display at the edge of the circle.



Troubleshooting and Diagnostic Tools

As an Administrator, you can set up tools that enable operators to troubleshoot and diagnose Situations. You can configure server tools to execute utilities on a remote host. These can be generic tools, or specific to Situations or alerts. You can also set up client tools, to retrieve or send information to a client, to help diagnose problems in Situations or alerts.

Cisco Crosswork Situation Manager provides a number of default hotkeys but you can set up additional hotkey shortcuts to make navigation easier for Cisco Crosswork Situation Manager users.

You can also set up ChatOps shortcuts to enable users to run tools from the Collaborate tab in the Situation Room. This gives Cisco Crosswork Situation Manager users quick access to the available tools.

Implement Generic Server Tools

Generic Server Tools in Cisco Crosswork Situation Manager are tools that allow a user to execute a utility on a remote host.

These tools specify a command that is run using the [Tool Runner](#) servlet, which is configured to connect to the remote host. The command can be anything you can run on the host in a Linux terminal command line, such as an inbuilt part of the OS (for example ping, cat) or your own script. Tool Runner

In Cisco Crosswork Situation Manager, the Generic Server Tools managed here are only available from Situation Room ChatOps feature. See [Take Additional Actions](#) in the Operator Guide for details. Take Additional Actions

The steps below describe how to create a Generic Server Tool and its command. Any arguments required are defined by the user when the tool is run.

Manage Generic Server Tools

Go to System Settings > Tools and then Generic Server Tools to open the configuration window:

- Click + to create a new tool.
- Fill in the available fields to define the tool. These are listed in the table below:

Field	Input	Description
Name	String (Mandatory)	The name for the Generic Server Tool (up to 100 characters). This appears in ChatOps when accessing the tool.
Description	String(Optional)	The text description of the tool..
Command	String	This is the file path of the command. Note: This command must be an accessible path on the host system. The host system and access information is defined in the Tool Runner servlet. Tool Runner
Run For	Boolean +String	Select a duration in with the spin box (minimum of 5 seconds). This sets how long to allow the tool to run for before it is stopped. If no time is set, the tool runs until it completes (or indefinitely).

- Click Save Changes to create the tool which then appears in the list on the left.
- Alternatively, click Revert Changes to discard your changes and confirm when prompted.

Edit a Generic Server Tool

- To edit a Generic Server Tool, click the required tool you want from the list on the left. Alternatively, type in the search box in the top left corner to search for the tool you want to edit.
- Edit the fields as described above.

- **Note**
- You cannot edit the tool name. If you need to do this, create a duplicate with the name you want. You can then delete the original.

- Click Save Changes.
- If you want to discard your changes, click Revert Changes.

Example

A Generic Server Tool with the following command runs the script myTests.sh which is located on the remote host at the path **/home/moog/bin**, using remote host access information defined in the Tool Runner servlet:

```
/home/moog/bin/myTests.sh
```

Implement Situation Server Tools

Situation Server Tools in Cisco Crosswork Situation Manager are tools that enable a user to execute a utility on a remote host. These tools specify a command and arguments that are run using the [Tool Runner](#) servlet, which is configured to connect to the remote host.

- The command can be anything you can run on the host in a Linux terminal command line, such as an inbuilt part of the OS (for example, ping) or your own script.
- The arguments are extracted from Situation attributes by prefixing the attribute name with '\$', such as \$description for the Situation description.

In Cisco Crosswork Situation Manager, the Situation Server Tools managed here are only available from ChatOps in the Situation Room. See [Take Additional Actions](#) in the Operator Guide for more information.

The steps below describe how to create a Situation Server Tool, its availability filter, command and arguments. You can also create Situation Server Tools via a command prompt.

Manage Situation Server Tools

Go to System Settings > Tools > Situation Server Tools to open the configuration window:

- Click the + to create a new tool
- Fill in the available fields to define the tool. These are listed in the table below:

Field	Input	Description
Name	String (Mandatory)	The name for the Situation Server Tool (up to 100 characters). This appears in ChatOps when accessing the tool.
Description	String(Optional)	The text description of the tool.
Context Filter	Filter(Optional)	Click the pencil icon to create a filter for specific criteria which Situations must match for this tool to be available.
Command	String(Mandatory)	This is the file path of the command. Please note: This command must be an accessible path on the host system. The host system and access information is defined in the Tool Runner servlet.
Arguments	String	This is the specific input for the command, which can use Situation attributes. To use Situation attributes, type '\$' as a prefix and enter the attribute you want from the drop down list.
Run For	Boolean +Integer	If enabled, you can define the number of seconds the tool runs for. The minimum value for this field is 5 seconds.

To prevent substitution with potentially malicious commands, arguments are escaped using a backslash.

For example:

Command: echo

Argument: \$args (where \$args is echo_something; rm file.txt)

This results in the following command being executed:

```
echo echo_something\; rm file.txt
```

The semi-colon is escaped to prevent the rm command from being run.

- Click Save Changes to create the new tool. This appears in the list to the left of the screen.
- To discard any changes, click Revert Changes and confirm when prompted.

Note: You can also create Situation Server Tools via a command prompt.

Example

The screenshot below shows a Situation Server Tool called 'LogSitnDetails' with the Command:
/home/moog/bin/logger.sh.

← System Settings / Situation Server Tools

NAME:	LogSitnDetails
DESCRIPTION:	Log Situation Details to a file on the remote host (using logger.sh script) Only available for closed Situations.
CONTEXT FILTER:	'Category' = 'Closed'
COMMAND:	/home/moog/bin/logger.sh
ARGUMENTS:	\$sig_id \$created_at \$description \$total_alerts
RUN FOR:	<input checked="" type="checkbox"/> 42 SECONDS

This tool runs the script logger.sh on the remote host which logs Situation details to a file. The details logged are the Situation ID, created time, description and total number of alerts, which are defined with the Arguments: ig_id \$created_at \$description \$total_alerts.

Each Situation attribute name is prefixed with \$. The Context Filter makes this tool available only for Closed Situations.

Create a Tool with a Command Prompt

You can create Situation Server Tools via a command prompt. This is useful for efficient creation of multiple tools using a scripted process, for example:

- Open a new Terminal window on the Cisco Crosswork Situation Manager system and type the following:
- **moog_add_sitn_server_tool**
- Type any flags and arguments for the tool settings. See the examples below.

- **Note**
- Cisco Crosswork Situation Manager command line tools are located here:
- **\$MOOGSOFT_HOME/utils**
- To display the help information for this tool, type:

- **moog_add_sitn_server_tool** and press **Enter**.

Use a double-dash prefix "--" to define all following text as arguments. This ensures arguments are not misinterpreted as flags.

For example, "-- -c" to define the argument "-c", which would otherwise be interpreted as the command flag.

- When you have defined the tool, press Enter. If successful, "Tool was added" appears.

- **Note**
- If there is a mistype, the help information appears.
- If the tool name already exists, the message "Error: A tool named: [toolname] already exists." appears.
- If a Run for time of less than 5 seconds is typed, the message "Error: The run_for value is too small. Please provide a value no smaller than 5 seconds." appears.

Once the UI is refreshed, newly created tools appear in the Situation Server Tools configuration window.

Examples

```
moog_add_sitn_server_tool --name "Sitn ID" --desc "Get the Situation ID" --cmd  
echo --args "Situation ID = \${sig_id}" --run_for 42
```

- Name: Sitn ID (--name "Sitn ID"). Quotes are required because there is a space in the name.
- Description: Get the Situation ID (--desc "Get the Situation ID")
- Context Filter: none
- Command: echo (--cmd echo)
- Arguments: display 'Situation ID = ID'
- (--args "Situation ID = \\${sig_id}"). The backslash is required to escape the '\$' because it is an environment variable.
- Run for: 42 seconds (--run_for 42)

```
moog_add_sitn_server_tool -d "five pings" -m "sig_id<10" -c ping -a -- -c 5
```

This creates a tool with the following settings:

- Description: five pings (-d "five pings")
- Context Filter: ID < 10 (-m "sig_id<10")
- Command: ping (-c ping)
- Arguments: ping five times (-- -c 5). The argument starts with -c which is itself a tool flag. Therefore the "--" double-dash prefix is used to interpret -c 5 as an argument, and not a flag.
- Run for: no time set (no -r flag and argument)
- Name: ping. The name is not defined here (no -n flag and argument) so the Command is used as the name by default.

Available Situation Arguments

The available Situation arguments are as follows:

affected_entities
category
Created_at
delta_entities
delta_priority
description
first_event_time
internal_priority
last_event_time
last_state_change
moderator_id
participants
process_list
queue
rating.rating
service_list
sig_id
status
story_id
teams
total_alerts
user
user_comments
username

Implement Alert Server Tools

Alert Server Tools are tools that allow a user to execute a utility. The tools available are relevant to the alert selected. Each tool executes on a remote host, which is defined when it is running.

The arguments passed to the utilities are extracted from the alert attributes. For example, testing the reachability (ping) of hardware using the source attribute of the alert.

The configuration steps described below define the Alert Server Tool (its command and argument).

Manage Alert Server Tools

Go to System Settings > Tools > Alert Server Tools to open the configuration window.

To create a new Alert Server Tool:

- Click the + icon. This opens a clear configuration window.
- Fill the available fields to define the tool:

Field	Input	Description
Name	String (Mandatory)	The name for the Alert Server Tool (up to 100 characters).
Description	String	The text description of the Alert Server Tool.
Alert Type filter	String	The Alert Types for which the Alert Server Tool is available. Note: Enter .* to make it available for all alert types.
Filter using Regex	Boolean	If enabled, the Alert Type filter uses regular expression.
Command	String (Mandatory)	This is the command to carry out using alert information Note: This command must be an accessible path on the host system. This is defined when you run the tool.
Arguments	String	This is the specific input for the command.
Run for	Boolean +Integer	If enabled, you can define the number of seconds the tool runs for. The minimum value for this field is 5 seconds.

Example

The screenshot below shows an Alert Server Tool that tests the reachability of the source the alert and returns the results.

The Command `ping` is used with Arguments `$source` and `-c5` which specify the source, from the alert attribute, and the number of times to ping (five).

← System Settings / Alert Server Tools

NAME: Ping

DESCRIPTION: Ping the alert source

ALERT TYPE FILTER: *

FILTER USING REGEX: ☒

COMMAND: ping

ARGUMENTS: -c 5 \$source

RUN FOR: ☐ 5 SECONDS

The Alert Type Filter uses a regular expression '.*' to make the tool available for all Alerts.

Implement Client Tools

You can create Client Tools in Cisco Crosswork Situation Manager to use Situation and alert data to execute actions through a specified URL.

Client Tools can be set to return response data; providing a more detailed response in the UI that includes response status and data, which can yield useful and important information. Another example is for the tools to link to an external trouble ticket system (via its URL) which then opens a new ticket using data from the selected Situation.

There are two different types of Client Tools which can be run: Alert Client Tools and Situation Client Tools.

Configure Client Tools

Go to System Settings > Tools and then either Alert Clients Tools or Situation Client Tools to open the configuration window. This is the same for both alert and Situation Client Tools.

- Click the + icon to create a new Client Tool.
- Fill the available fields to define the tool. These are listed in the table below:

Field	Input	Description
Name	String (Mandatory)	The name for the Client Tool (up to 100 characters)
Description	String	The text description of the tool
Context	Filter (Optional)	Click the pencil icon to create a filter for specific criteria which the Alerts or Situations must match for this tool to be available

- Next select one of the radio button options to choose one of the following options:
- URL Tool: If you want to create a tool that uses a URL.
- Merge Custom Info: If you want to create a tool that uses custom info fields.

URL Tool

The different fields used to configure a URL Tool are described below:

Field	Input	Description
Show All Response Data	Boolean	If enabled, the tool returns a more detailed response in the UI, including the response status and data.
HTTP Method	GET POST	Select GET if the tool needs to retrieve information or select POST if the tool needs to send information. Note: Choose the method appropriate for the URL service you are interacting with.
Open Window	Boolean	If enabled, this opens a new browser window when using the GET HTTP Method. Note: This disables the Show All Response Data.
URL	String	This is the URL of the Client Tool.
URL Encoded Content	String	This is the payload data that is to be posted when the tool is run when using the POST HTTP Method. Note: The payload data must be URL encoded and can include Situation

		and alert attributes and prompt variables.
--	--	--------------------------------------------

Merge Custom Info

Select Merge Custom Info and in the Custom Info box, enter valid JSON for the custom_info you want the tool to add.

The example JSON blob below adds a set of custom info called "TPS data" that contains a string "From MOOG", the Situation ID and the timestamp for when the Situation was created:

```
{"TPS data": ["From MOOG", "$sig_id", "$created_at"]}
```

The JSON in the box can include Situation and alert attributes and prompt variables.

When creating a client tool, entries in the URL, URL Encoded Content or Custom Info boxes can contain Situation or alert attributes, for example, \$description for the contents of the Situation or alert description field, and prompt variables.

Prompt Variables

Prompt variables open a message box when the tool is run, prompting the user to type text, a number, or select from a list.

In the URL, URL Encoded Content or Custom Info boxes, enter prompt variables in the following format:

\$<prompt_name>

The prompt name cannot be any of the existing Situation or alert attribute names.

To add a new prompt:

- When entering text in the URL, URL Encoded Content or Custom Info box, type a prompt variable as described above. The prompt name appears in the Prompts table.
- To edit the prompt, double-click on it or select it and then click Edit Prompt.
- Enter a Display Name. This is what appears in the prompt message.

Next choose from one of the three prompt options: Text, Number and List.

- Text - this prompts users for string text. The optional text settings are:

Setting	Input	Description
Default Value	String	The default prompt text.
Minimum Length	String	The minimum length of text which users can enter into the prompt.
Maximum Length	String	The maximum length of text which users can enter into the prompt.

- Number - this prompts users for a number. The optional number settings are:

Setting	Input	Description
Default Value	String	The default number value.
Minimum Value	String	The minimum number which users can enter into the prompt.
Maximum Value	String	The maximum number which users can enter into the prompt.

Note: Numbers can be integers or floating point; in which case they are truncated to two decimal places.

- List - this prompts users to select from a list. The list settings are:

Setting	Input	Description
Available Options	String	The other available options.
Default Value	String	The default list value.

Click Add Option to add new options to the Available Options list. In the 'Display' column enter what you want to appear for selection. In the 'Value' column, type what data you want to be added to the custom_info when the option is selected from the list. Click Update to add the option to the list.

LIST

DEFAULT VALUE: ☒ LEVEL 1

AVAILABLE OPTIONS:

+ ADD OPTION - REMOVE OPTION	
DISPLAY	VALUE
LEVEL 1	1
LEVEL 2	2
LEVEL 3	3

CANCEL OK

Finally click OK when you have finished. The new prompt is added to the Prompts table.

When you have finished, click Save Changes. The new tool appears in the list on the left.

Edit a Client Tool

- Select the client tool you want to edit. Alternatively, type into the search bar to find the tool.
- Edit fields as described above.

Note: You cannot edit the tool Name. If you need to do this, create a duplicate with the name you want. You can then delete the original.

- Click Save Changes.
- If you want to discard your changes, click Revert Changes.

Running Client Tools

The Client Tools can be accessed from the following areas:

Alert Client Tools: On the Alert Tools Menu, see [Alerts Overview](#) (Right-Click menu). Or via "Situation Alerts" in a [Situation Room](#). Alerts Overview Situation Rooms

Situation Client Tools: The Situation Tools Menu, from Tools menu on the Situation Room or via ChatOps in the Collaborate tab.



If you want to run Client Tools using Safari, go to Safari > Preferences > Security and uncheck 'Block pop-up windows' as this is checked by default.

Examples

Client tools can also be configured to alter custom info fields. For example, running a tool to raise a ticket on a third party system can be configured to prompt for entries of pre-defined (custom info) values to provide more information in the ticket raised in the third party system.

Client Custom Info Tool with a Prompt Variable

To create a Client custom info tool with a prompt variable, select the Merge Custom Info option:

System Settings / Alert Client Tools

NAME: TPSLEVEL

DESCRIPTION: Set Level data for TPS

CONTEXT FILTER: To edit the filter press the pencil button or click here.

☐ URL TOOL

SHOW ALL RESPONSE ☐

DATA:

HTTP METHOD: POST

OPEN WINDOW: ☐

URL:

URL FORMATTED CONTENT:

☒ MERGE CUSTOM INFO

CUSTOM INFO: {"LEVEL": \$prompt1}

PROMPTS:

EDIT PROMPT

NAME	DISPLAY NAME	VALIDATORS
prompt1	prompt1	Default: LEVEL 1; One Of: LEVEL 1, LEVEL 2, LEVEL 3; Type...

REVERT CHANGES SAVE CHANGES

In this example, the custom info entered is:

```
{"LEVEL": $prompt1}
```

The screenshot below shows how the prompt variable settings can be configured:

Edit prompt1

NAME:

prompt1

DISPLAY NAME:

Select a TPS LEVEL...

☒ TEXT

DEFAULT VALUE:

☐

MINIMUM LENGTH:

☐

MAXIMUM LENGTH:

☐

☐ NUMBER

DEFAULT VALUE:

☐

MINIMUM VALUE:

☐

MAXIMUM VALUE:

☐

☒ LIST

DEFAULT VALUE:

☒

LEVEL 1

AVAILABLE OPTIONS:

+ ADD OPTION

- REMOVE OPTION

DISPLAY	VALUE
LEVEL 1	1
LEVEL 2	2
LEVEL 3	3

CANCEL

OK

Run the Tool

To run the tool:

- Go to an alert, right-click or click Tools > Tools > Set LEVEL data for TPS.
- The prompt shown below appears:



- Click OK to continue.

Configure Hotkeys

Hotkeys are keyboard shortcuts you can use on the Alert View, Situation View and Situation Room screens in Cisco Crosswork Situation Manager. The default hotkeys are as follows:

Key	Action
A	Assign
D	Show Details
I	Invite User
M	Own
T	Open Server Tools

You can add more custom hotkeys for additional actions to make navigation easier for you and your team.

Add a Hotkey

Click + Create Hotkey in the top left corner of the window to add a new hotkey shortcut.

Under 'Key', select a number between 0-9 or a letter between A-Z then select an action for it to represent. The new hotkey is highlighted with orange markers.

Click Save Changes to continue.

Delete a Hotkey

Select any unwanted hotkey from the list, default hotkeys included, and click - Remove Hotkey. The selected hotkey disappears from the list.

Click Save Changes to continue or click Revert Changes to undo the action.

Configure ChatOps Shortcuts

The ChatOps feature enables Cisco Crosswork Situation Manager users to run tools from the Collaborate tab in the Situation Room. For more information, see [Take Additional Actions](#) in the Operator Guide.


The ChatOps shortcuts can be set up to give your users quick access to the available tools. To do this, go to System Settings > ChatOps Shortcuts:

Any existing shortcuts are listed under the Tools panel to the right of the window.

Create a ChatOps Shortcut

Click the + Create Shortcut button to get started.

Next enter a name for your new ChatOps shortcut in the Shortcut text box. This is what users enter to run the ChatOps tool.

 You can use 0-9, lowercase a-z, dash (-), underscore (_) and period(.) If the name already exists, the name highlights in red in the list on the left and you cannot save until the name is edited to be unique.

Select the checkbox for the tool you want. To search for a tool, type text to the right of the search icon. Default alert and Situation workflow tools, such as ping, nslookup, are available.

Repeat the steps above to create as many shortcuts as required.

Click Save Changes when you are finished.

Remove a ChatOps Shortcut

Select the ChatOps shortcut you want to delete, from the list on the left.

Click the - Remove Shortcut button to remove the shortcut from the list.

If you accidentally remove the wrong shortcut, you can click Revert Changes to undo this. This discards all changes since the last save.

Additional System Configuration

As an administrator, you can perform additional system configuration to create an effective Cisco Crosswork Situation Manager working environment for your organization. For example, you can configure which columns display on Situation and Alert Views and the order in which they appear, and the landing page that displays when users open Cisco Crosswork Situation Manager.

You can create global filters for all users, and team filters for selected teams, to restrict the alerts and Situations that Cisco Crosswork Situation Manager users can access. Individual users can create personal filters for alerts and Situations for their own use.

You can customize the user experience and workflow within Cisco Crosswork Situation Manager. For example, you can set the default tab that displays when a user enters a Situation Room, define the effect on alerts when actions are performed on the Situations they are in, set the period of inactivity before a user is logged out, and configure a number of system settings such as date format and time zone.

You can also enable Probable Root Cause and define which users can access it. This feature allows users to identify which alerts are the probable root cause of a Situation.

You can configure Labs Features that users can use, including statistics for Insights, and Early Access features. Early Access features are for evaluation only and should not be used in production environments.

Create Shared Alert and Situation Filters

You can use filters to configure which alerts and Situations you want to access and display from the Cisco Crosswork Situation Manager Workbench. As an Administrator, you can create, edit and delete global filters for all users, and team filters for selected teams. If you share a filter with a specific team, only the users in the team can access the filter in the filter list.

Individual users can create personal filters for alerts or Situations. Only the creator can see personal filters.

Navigate to System Settings > Filters and either Alert Filters or Situation Filters to open the configuration window.

Create a Filter

- Click the + icon to create a new filter.
- Fill in the available fields to configure the filter:

Field	Input	Description
Name	String (Mandatory)	The name of the new filter (up to a maximum of 100 characters).
Description	String	The text description of the filter.
Show in	Navigation Dashboards	Select whether the filter is shown in Navigation and/or Dashboards.

- Click Add Clause to start building the filter.
- Click the drop-down menu arrow and select a parameter.
- Click the drop-down menu below this and select an operator.
- Depending on the parameter selected, enter or select a value in the final box and then click Apply.
- To add more clauses, click the clause and then click AND, OR or NOT and fill in the boxes as before.
- Click Save Changes to create the filter.

See [Filter Search Data](#) for filter examples.

Configure the Landing Page

You can configure the landing page users land on when they open Cisco Crosswork Situation Manager. You can set the landing page for each user's role, for each team and for the system. The default system landing page is the Summary screen. The landing page a user adopts follows the priority order: role > team > system.

Set a Role's Landing Page

To configure the landing page for a role:

- Go to System Settings > Roles.
- Select the Role you want to edit.
- Set the 'Landing Page' and save your changes.

See [Manage Roles](#) for more details.

Configure other Landing Pages

You can also configure landing pages for teams and the Cisco Crosswork Situation Manager system in the System Settings. To add landing page for a team see [Manage Teams](#). To add a landing page for your system see [Customize User Experience and Workflow](#).

Customize User Experience and Workflow

You can configure the functionality and default tabs of Cisco Crosswork Situation Manager for Situation Rooms, Workflow, System Settings and Interface Settings. To access these options, click Customization in the System section of the Settings tab.

Situation Room

Use the Situation Room tab to select the default tab that displays when any user opens the Situation Room and the columns that appear in the Situation Room header.

Default Tab

You can choose between Next Steps, Alerts, Collaborate, Topology, and Visualize as the default tab that displays. By default, the tab is Next Steps. To change the default tab:

- Select the default tab that you want from the drop-down list.
- Click Save Changes to continue.

Situation Header Columns

You can select up to eight columns to display in the Situation Room header. To change the columns that you want to display in the Situation Room header:

- To add a new column, click Add Field and select a column from the drop-down list.
- To delete an existing column, click x next to the column name.
- To move a column, click on a column and drag it to the place where you want it to display.

Workflow

The Workflow tab allows you to alter the standard workflow of all Situations.

Propagate Situation Actions to Alerts

When enabled, this mirrors any actions to the Situation down to its alerts. Click Enable to continue and then define the scope:

Setting	Description
Any unassigned Alerts	Action applies to any currently unassigned alerts in the Situation.
Any unassigned Alerts and any assigned but not acknowledged Alerts	Action applies to any unassigned alerts and any assigned but not acknowledged alerts.
All Alerts	Action applies to all of the alerts in the Situation.

Close Situations

These settings determine the behavior when closing Situations:

Setting	Description
---------	-------------

Close Situation and Open Alerts	This closes the Situation and all open alerts within it.
Close Situation and Unique Open Alerts	This closes the Situation and all unique open alerts.
Close Situation Only (Not recommended for normal operation)	This only closes the Situation but not its alerts.

Click Save Changes to continue.

System Settings

The System Settings tab is where you can set when Cisco Crosswork Situation Manager times out, either with the system default or a custom timeout:

Setting	Description
Use System defined timeout	The system default timeout of one hour (60 minutes).
Custom timeout	Any custom-defined timeout (any time between 60 and 480 minutes).

Click Save Changes to continue.

Interface Settings

The Interface Settings section is where you configure the default time format, landing page and theme for the Cisco Crosswork Situation Manager interface.

Setting	Input	Description
Default time format	US (hh:mm:ss MM/DD/YYYY) International (hh:mm:ss DD/MM/YYYY)* Sortable (YYYY-MM-DD hh:mm:ss)	The default time format that applies throughout Cisco Crosswork Situation Manager.
Landing page	Summary* Management Dashboard Cisco Crosswork Situation Manager Dashboard My Situations Open Situations Open Situations with Impacted Services	The default landing page that opens when you launch Cisco Crosswork Situation Manager or click the Cisco logo in the top left corner.
Default theme	Light* Dark	The color scheme of Cisco Crosswork Situation Manager (dark or light).
Allow users to select theme	Boolean	Allows users to select their own color scheme. Enabled by default.

Default time zone	Use Client Time Zone*	Defines the default time zone for new users logging in to Cisco Crosswork Situation Manager. The default 'User Client Time Zone' means Cisco Crosswork Situation Manager adopts the local time zone.
Allow users to select time zone	Boolean	Allows users to set their own time zone under the My Account settings. Enabled by default.
Select Custom Logo	-	Upload an image such as a logo so display on the login page and on the top bar of the workbench.

Note: These are the default settings for Cisco Crosswork Situation Manager.

Click Save Changes to continue.

Upload a Logo

You can upload a custom image such as a company or brand logo to appear on the login page and on the top bar of the workbench:

- Click Upload and select the desired image file from your computer. Currently PNG, JPG and GIF files up to 5MB in size are supported.
- Click Save Changes for the changes to be applied.
- Click the image to go to the default or configured landing page.

Create Link Definitions

Link Definitions allow you to format alert and Situation view custom info values as links to external tools for individual alerts or Situations.

You can add Link Definitions to columns in alert and Situation views. You can configure links using Situation and alert data and custom info fields. You can use them to perform queries and to link directly to corresponding tickets in third-party ticketing systems.

Create a Link Definition

To create a new Link Definition:

- Go to Settings > Link Definitions and click + to create a new definition. Complete the details for the Link Definition as follows:
 - Name. Name of the Link Definition.
 - Link. Link format, including query syntax if required. It can include a \$reference to one or more alert or Situation fields.
 - Display. Link text to appear in Situation and alert views. It can include the \$value of a referenced field.
- To display the Link Definition in a Situation or alert view column, go to Settings > Situation Columns and Settings - Alert Columns. See [Configure Alerts and Situation Columns](#) for more information.

The following screenshot displays two example Link Definitions, ServiceNow Ticket and Google Link.

<input type="checkbox"/>	SEVERITY	ID ↓	CREATED AT	OWNED BY	SERVICENOW TICKET	GOOGLE LINK	DESCRIPTION
<input type="checkbox"/>	Clear	#26	Today 12:58	A Administrator	ServiceNow REQ7877442	Google Description	Service Pack Update SP21
<input type="checkbox"/>	Major	#25	Today 12:37	A Administrator	ServiceNow INC1190341	Google Description	Network outage
<input type="checkbox"/>	Critical	#24	Today 12:37	AO Amanda Operator	ServiceNow INC0868823	Google Description	License expiry
<input type="checkbox"/>	Critical	#23	Today 12:37	AO Amanda Operator	ServiceNow INC6628443	Google Description	Memory leak
<input type="checkbox"/>	Critical	#22	Today 12:37	MO Melissa Operator	ServiceNow REQ9983372	Google Description	Database timeout
<input type="checkbox"/>	Critical	#21	Today 12:37	SA Susan Administrator	ServiceNow INC1044290	Google Description	High CPU on EC2 servers

Third Party Ticketing Example

The Link Definition for ServiceNow Ticket is configured to take the value of the custom info servicenow field, and also displays this value as part of the link itself:

- Name: ServiceNow
- Link: [https://instance.service-now.com/nav_to.do?uri=incident.do?number=\\$value](https://instance.service-now.com/nav_to.do?uri=incident.do?number=$value)
- Display: ServiceNow \$value

The Situation column is configured to display data from the custom_info servicenow field and links to the ServiceNow link definition:

- Field: custom_info.servicenow
- Header: ServiceNow Ticket
- Type: Text
- Link Definition: ServiceNow

Situation #25 has the following custom_info:

- Name: servicenow
- Value: INC1190341

In the screenshot example, the ServiceNow INC1190341 link for Situation #25 contains the following URL: https://instance.service-now.com/nav_to.do?uri=incident.do?number=INC1190341

Query Example

The Link Definition for Google Link is configured to perform a google query for the text strings in the \$description Situation field and the custom info impact field:

- Name: Google Description
- Link: [https://www.google.com/search?q=\\$description&q=\\$custom_info.impact](https://www.google.com/search?q=$description&q=$custom_info.impact)
- Display: Google Description

The Situation column is configured to link to the Google Description link definition. In this example, the Field setting is ignored, but you must still enter a custom info field here:

- Field: custom_info.impact
- Header: Google Link
- Type: Text
- Link Definition: Google Description

Situation #26 has the following custom_info:

- Name: impact
- Value: documentation



In the screenshot example, the Google Description link for Situation #26 contains the following URL:
<https://www.google.com/search?q=Service%20Pack%20Update%20SP21&q=documentation>

Configure Alert and Situation Columns

You can change the columns to display on Situation and Alert Views and add new columns based on custom_info fields. Optionally add link definitions to custom_info columns, for example, to link the custom_info data to a third-party system. See [Link Definitions](#).

Navigation

Click the Columns drop-down menu in the top right corner to display which columns are displayed by default. Check or uncheck columns to add or remove them from the default column layout.

Icon	Description
	Click the border of any column and drag left or right to make the column narrower or wider. Double-click to auto-resize the column to the current content.
	Click and drag any column to another position to change the order the columns appear in.

Click any column and edit the text next to 'Header' to change the column header.

Create a New Column

Click Columns > Add Column to add a new custom column to the default layout. Edit the available fields to configure the column:

Field	Input	Description
Field	String	Enter the custom_info field you want to use or show in the column. Note: This entry must start with custom_info. (added when creating a new column). For example, to use a Custom_info field 'TPS_ID' enter: custom_info.TPS_ID
Header	String	This is the header name of the column.
Type	Number OR Text	Select 'Number' if the column content is numeric or 'Text' if the column content is a text string.
Link Definition	Selection	Select the Link Definition from the list (if required).
Indexed	Boolean	If enabled, the column data is indexed in the database. When new columns are added they are filterable and sortable by default. This improves performance of filtering and sorting, but may affect the performance of additions. If you are planning to use this custom_info field in alert or Situation filters or you are planning to sort using this column, we recommend you enable the indexed option to aid filter loading performance. Too many indexed columns may impact performance.

Adjust the column width as required and change the order by dragging and dropping the new column where you would like it to be. Click Save Changes to continue and confirm when prompted. Alternatively, click Revert Changes to discard your changes.

Example

This example walks you through setting up an Alert Column with Custom_info Data from Prompt. The custom_info field 'TPSLEVEL' is added to Alerts using a client tool with a prompt variable: 'Set TPS Level'. See [Client Tools](#) for information on how to set up the TPS Level client tool.

1. Right-click and select Tools > Set TPS Level tool or Tools > Tools > Set TPS Level to run the tool on an alert.
2. Select the TPS level on the prompt window.
3. Right-click on the alert, select Show Details... and Custom Info...
4. Navigate to System Settings > Columns > Alert Columns to create the custom_info column.
5. Click Columns > Add Column and then configure the column.
6. Click Save Changes to continue.

The Alert Views window displays the TPS Level column display custom_info data in the second column.

Configure and Retrain Probable Root Cause

Probable root cause (PRC) for Cisco Crosswork Situation Manager is enabled by default. This means that you can mark Situation alerts as having a root cause or not and Cisco Crosswork Situation Manager shows a root cause estimate in Next Steps in the Situation Room.

Navigate to System Settings > Configure & Retrain to enable or disable PRC.

To configure which users can mark alerts for PRC, go to Security > Roles. Select the role you want to edit and under Permissions, move 'prc_feedback' to 'Selected' using the direction arrows. This permission is enabled for Administrator and Super User roles by default.

Root Cause

The PRC Model gives each alert within a Situation a probable root cause estimate. Retrain recalculates the estimates with the current data. You can choose which features your model uses when predicting the probable root cause of an alert. The default PRC configuration uses two types of Severity. The other features are listed below:

Feature	Description
Agent	The agent of the alert represented as an enumeration. Each value of 'agent' is considered to be independent from all other values.
Alert Arrival Order	Represents the arrival order of the alert in a Situation.
Alert Time	Represents the alert time as the components of the 'time of day', for example, hours of day, minutes of hour.
Class	The class of the alert, represented in a way that identifies naming conventions in the class name.
Description	Tokenizes the description into words and uses those words to identify key words and phrases that may indicate root cause.
Host	The host of the alert, represented in a way that identifies naming conventions in the class name.
Manager	The manager of the alert represented as an enumeration. Each value of 'manager' is considered to be independent from all other values.

Severity & Arrival Order (default)	The severity of the alert represented as independent values and when the alert arrived for each value of severity. For best results use in conjunction with 'Severity Raw'.
Severity Enum	The severity of the alert represented as independent values. For best results use in conjunction with 'Severity Raw'.
Severity Raw (default)	The severity of the alert represented as a continuous value such that 'Warning' < 'Major' < 'Critical'. For best results use in conjunction with 'Severity Enum' or 'Severity & Arrival Order'.
Situation Alert Time	Represents the alert time as the components of time, for example, hours of day, minutes of hour, relative to the first alert in the Situation.
Type	The type of the alert, represented in a way that identifies naming conventions.

Reset all Feedback

To clear all feedback from your Cisco Crosswork Situation Manager instance click the Reset button.

Configure Labs Features

Cisco Crosswork Situation Manager Labs offers a preview of unreleased features. Navigate to Settings > Labs > Configure to view available labs features for the current release.

Statistics Collection

You can disable and enable the collection of different statistics for Insights. See [Grafana Dashboards](#) for more details. Available collections that populate the default Grafana dashboards include:

- Team Room Overview
- Ops Insights
- Noise Reduction Insights
- Team Ops Insights
- Team Performance Insights
- Individual Performance Insights
- UI Dashboards

All collections are active by default. Uncheck a collection if you do not want to use that particular dashboard. You might want to disable collections and their related processes if you are only interested in retrieving a specific set of statistics or you want to keep the load on your system to a minimum.

Early Access Features

You can disable and enable different early access features. Do not use these features in production environments. Available early access features include:

- Visualize: Allows administrators and implementers to view the Visualize tab in a Situation Room that shows which process created the Situation and the similarity of the alerts within the Situation. See Situation Visualization for details.
- Workflow Engine: Allows you to define custom workflows for events, alerts and Situations.
- New Grid: Allows operators to see Situation and alert lists using the new grid. This has improved performance, better scrolling, and is easier to use compared with the old grid. Some

actions, such as drag and select rows, and copy and paste, behave slightly differently in the new grid.

Monitor Your Cisco Crosswork Situation Manager System

As an Administrator, you can monitor your Cisco Crosswork Situation Manager system. You can use Self Monitoring to view the status, health, and processing metrics of the Moogsoft AIOps processes. You can use the audit trail feature to review actions that have been performed on Situations or alerts.

Self Monitoring

Administrators can use Self Monitoring to view the status, health, and processing metrics of the Cisco Crosswork Situation Manager processes. The different tabs show the state of Processing Metrics, Event Processing, Web Services, Event Ingestion and Message Bus.

Heartbeats are one of the key concepts in Self Monitoring. A heartbeat is an internal message sent by a process every 10 seconds to inform Self Monitoring that it is still running.

All data displayed in this screen is live and updates continually.

Package States

The table below describes the possible states for a package:

Icon	Description
Green circle with a white check.	The process is running (reserved or unreserved*).
Yellow circle with a white exclamation mark.	The reserved process has missed some heartbeats. This could indicate a potential problem and should be investigated.
Red circle with a white cross.	The reserved process is either not running or has missed its last heartbeat. This could indicate the process has failed, has not started or that Cisco Crosswork Situation Manager is not working properly.
Gray circle with a white backslash.	The unreserved process is not running.
White circle with a green check.	The process is in passive mode. <i>This is for High Availability deployments only. See /document/preview/77155#UIDbea404d9dd1afee65fa1471105d1b3c6 for more information.</i> High Availability Overview

You can set processes as reserved or unreserved in the system.conf file

(\$MOOGSOFT_HOME/config/system.conf. If a package's 'reserved' setting is 'true', the self monitoring reports a warning if the package is not running. Stopped unreserved processes do not generate warnings.

Controls

There are a number of controls in Self Monitoring that can be used to stop, start and restart Moogfarmd and the LAM services:

Button	Description
Refresh symbol.	Restart.

Stop symbol.	Stop - only works if Moogfarmd is running as a process rather than a service.
Play symbol.	Start.

These can be configured by users with Super User permissions.

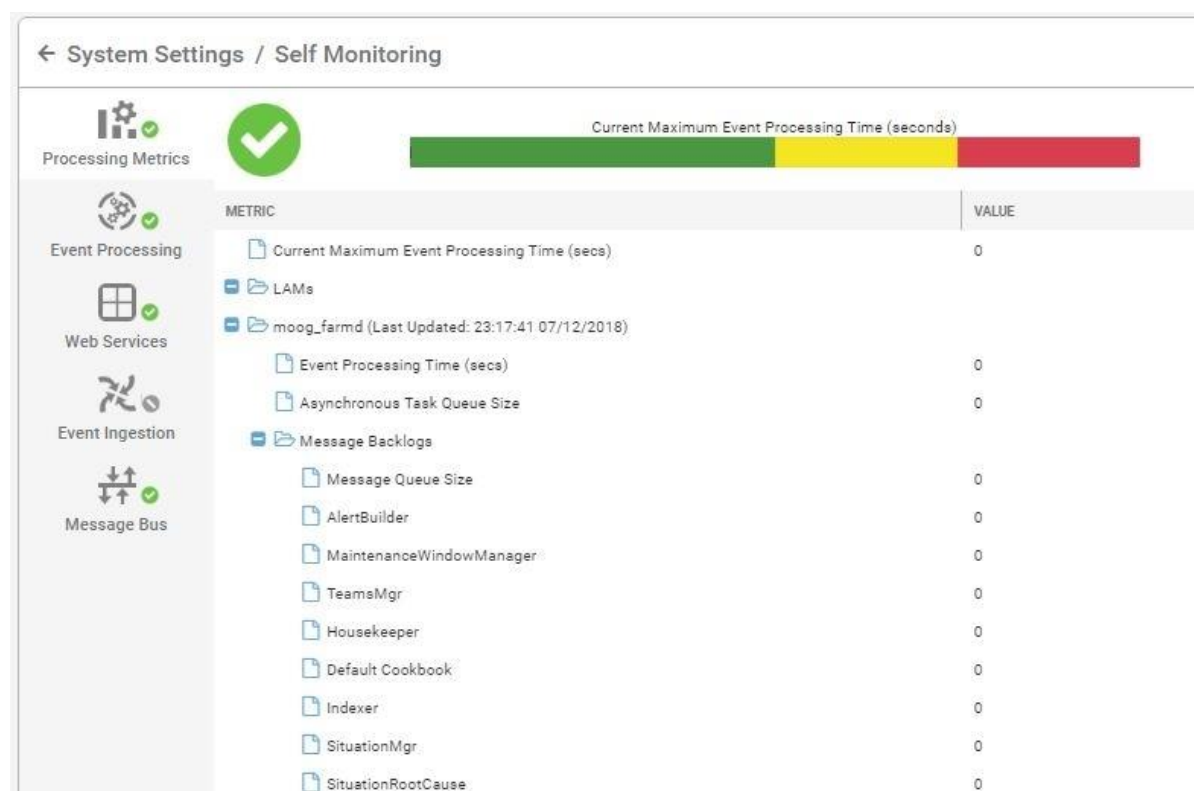
Self Monitoring Tabs

The Self Monitoring screen is divided into a number of tabs. Each section displays the states of the various processes, indicating which are running or which have issues:

- Processing Metrics
- Event Processing
- Web Services
- Event Ingestion
- Message Bus

Processing Metrics

This tab, which is open by default when Self Monitoring is launched, displays event processing times and other metrics.



The icon in the top left corner indicates the overall state of event processing. This is determined by the Current Maximum Event Processing Time in seconds. This time is indicated by the position of the gray bar on the colored bullet graph shown below. The Current Maximum Event Processing Time is 1.917s in this example:



The default bullet chart color values are as follows:

- GREEN (0 - 10 seconds) Good performance
- YELLOW (10 - 15 seconds) Marginal performance
- RED (15 - 20 seconds) Poor performance

The time values are configurable in the web.conf file.

Using Processing Metrics

To use the Processing Metrics tab, open the LAMs and moog_farmd folders and look for deviations from normal values.

METRIC	VALUE
Current Maximum Event Processing Time (secs)	0
LAMs	
moog_farmd (Last Updated: 23:19:01 07/12/2018)	
Event Processing Time (secs)	0
Asynchronous Task Queue Size	0
Message Backlogs	
Message Queue Size	0
AlertBuilder	0
MaintenanceWindowManager	0
TeamsMgr	0
Housekeeper	0
Default Cookbook	0
Indexer	0
SituationMgr	0

The numeric value itself may not be an absolute measurement of health, so as a general rule, look for unusual or sudden changes in the values or behavior. See the examples below:

- If a particular LAM becomes a data flow bottleneck, expect to see substantial increases in the values for the Message Queue Size and/or Socket Backlog metrics for that LAM. This leads to an increasing Event Processing Time for the appropriate Moogfarmd (which is expecting data from the LAM).
- If an AlertRulesEngine in a Moogfarmd instance becomes a data flow bottleneck, expect to see a substantial increase in the Message Backlog and possibly the Messages Processed decreasing for that AlertRulesEngine. This also leads to an increasing Event Processing Time for the Moogfarmd.

Both of these result in the bullet chart (at the top) showing increasing Current Maximum Event Processing Time, from green to yellow to red.

Event Processing

This tab contains a process group including Moogfarmd (the core Cisco Crosswork Situation Manager application) and the Moolets, such as AlertBuilder, Alert Rules Engine, Sigalisers.

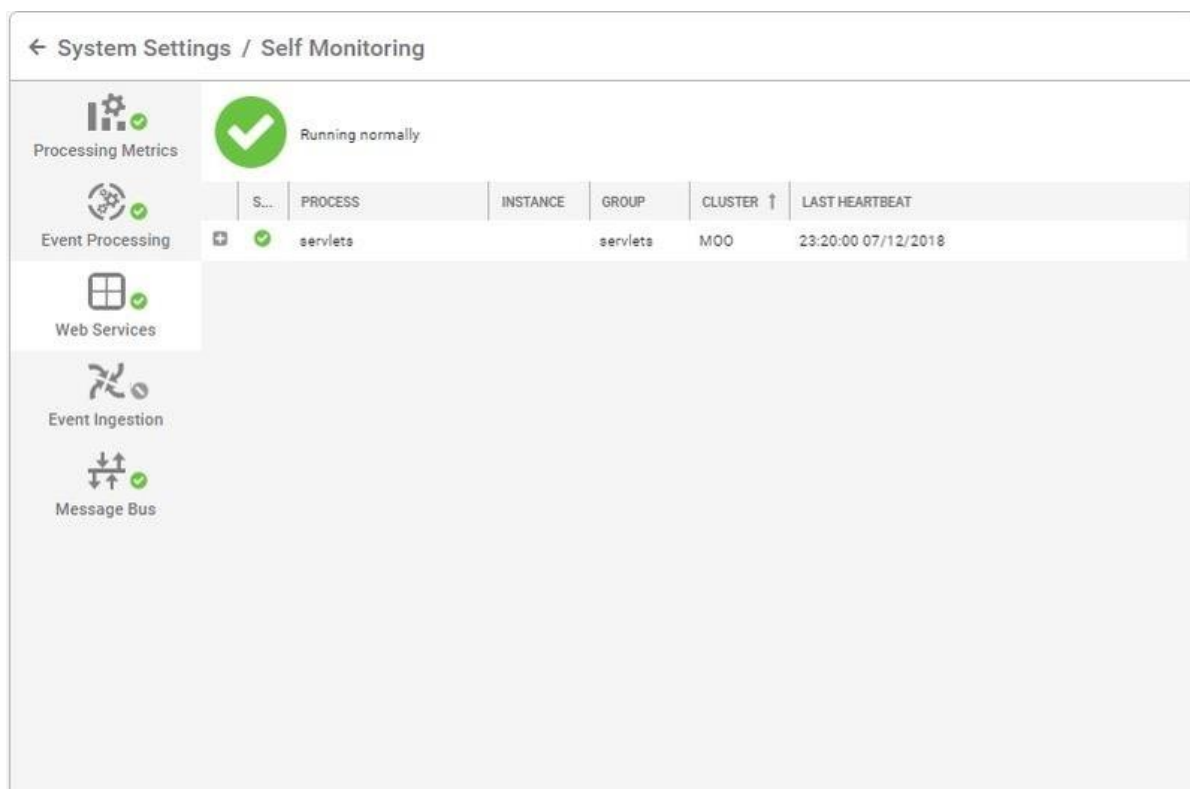
The screenshot shows the 'System Settings / Self Monitoring' interface. On the left is a sidebar with icons for Processing Metrics, Event Processing (selected), Web Services, Event Ingestion, and Message Bus. The main area displays the 'moog_farmd' group status as 'Running normally' with a green checkmark icon. Below this, it shows 'Last Heartbeat: 23:19:21 07/12/2018' and 'Group: moog_farmd, Cluster: MOO'. A table lists the Moolet processes:

✓	AlertBuilder	
✓	Default Cookbook	
✓	Housekeeper	
✓	Indexer	
✓	MaintenanceWindowManager	
✓	SituationMgr	
✓	SituationRootCause	
✓	TeamsMgr	
✗	AlertRootCause	None
✗	AlertRulesEngine	None
✗	Cookbook	None
✗	Enricher	None
✗	Feedback	None

The icon in the top left corner indicates the overall state (running normally in the example above). The group and cluster names are displayed in the top right corner. The time and date of the last heartbeat is displayed above the list of Moolet processes.

Web Services

This tab contains all processes related to Tomcat web applications: moogsvr, moogpoller, toolrunner and Graze.



Each row displays the following information:

Column	Description
+	Click this button to expand or collapse the row for further information. For example 'No reported problems'.
State	This shows an indicator icon showing whether or not the process is running as normal.
Process	The name of the Cisco Crosswork Situation Manager component.
*Instance	The name of the instance (in High Availability there are multiple instances of Cisco Crosswork Situation Manager).
*Group	The name of the Process Group the component belongs to.
*Cluster	The name of the Cluster the component's Process Group belongs to.
Last Heartbeat	The time of the last received heartbeat. A heartbeat indicates a health component.

Note: These only apply to High Availability deployments where there are more than one instance of Cisco Crosswork Situation Manager and its component processes.

Event Ingestion

This tab displays information about the state of all processes relating to the LAMs and the individual processes which process raw data and create events:

← System Settings / Self Monitoring

Processing Metrics

Event Processing

Web Services

Event Ingestion

Message Bus

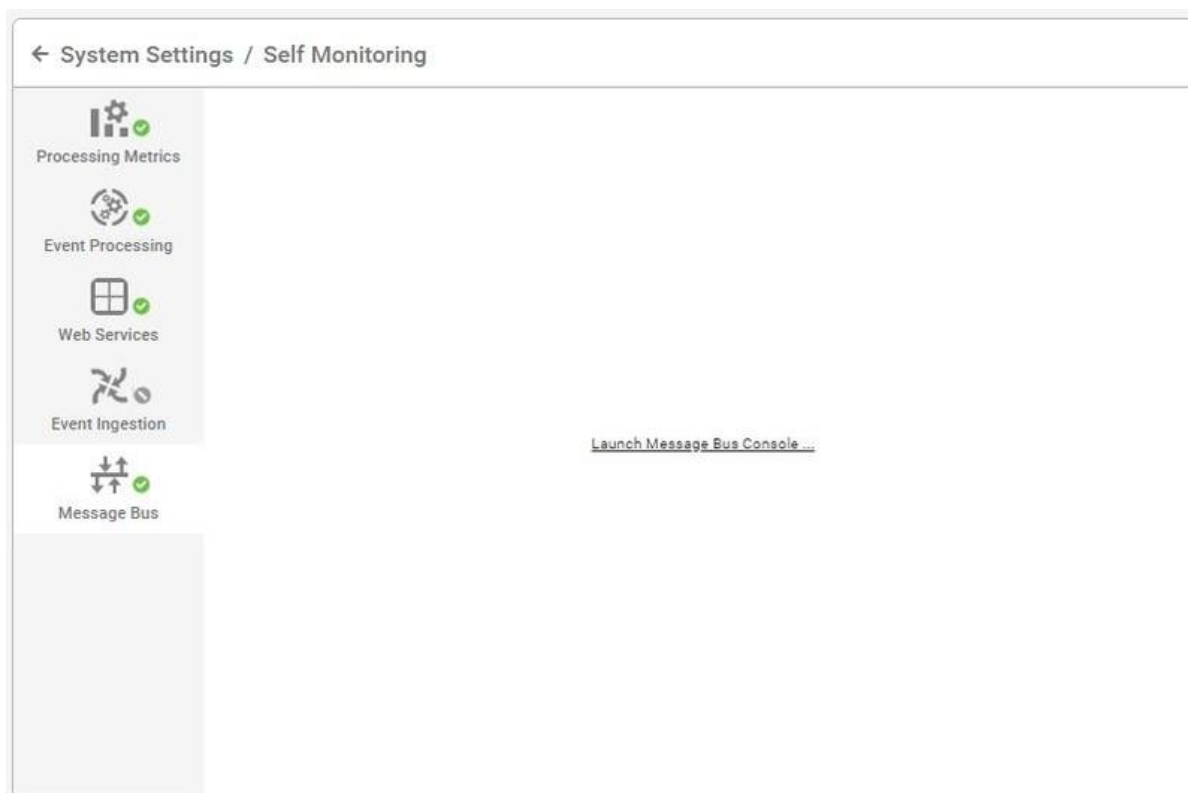
Not running

S...	PROCESS	INSTANCE	GROUP	CLUSTER ↑	LAST HEARTBEAT	CONTROL
+	newrelic_lam		newrelic_...	M00	None	▶
+	nagios_lam		nagios_la...	M00	None	▶
+	trapd_lam		trapd_lam	M00	None	▶
+	appdynamics_lam		appdyna...	M00	None	▶
+	netcool_lam		netcool_L...	M00	None	▶
+	logfile_lam		logfile_lam	M00	None	▶
+	rest_lam		rest_lam	M00	None	▶
+	socket_lam		socket_la...	M00	None	▶
+	solarwinds_lam		solarwin...	M00	None	▶
+	rest_client_lam		rest_clie...	M00	None	▶

The controls in the far right column can be used to stop and restart active LAM processes or to start inactive LAMs.

Message Bus

The final tab provides a link to the Message Bus Console, also known as the MooMs (Moogsoft Messaging System). This is hosted by message-queueing software RabbitMQ.



Click the link to proceed to the RabbitMQ management console.

The username and password to log in are specified and can be configured in **\$MOOGSOFT_HOME/config/system.conf** (under mooms.username and mooms.password in the JSON) and correspondingly in RabbitMQ. See [Configure the Message Bus](#) for more information. Configure the Message Bus

Once logged in, RabbitMQ displays information about message rates, connections, channels, queued messages, etc.



Configuration

The 'Restart/Stop/Start' feature uses the moogfarmd/LAM service scripts under **/etc/init.d**, for example, **/etc/init.d/moogfarmd** and **/etc/init.d/logfilelamd**, in combination with the Apache Tomcat 'toolrunner'.

You need Super User role permissions to configure this feature. Create a user in the 'moogsoft' group. This user must be used by the toolrunner and the services in order to start/stop services via the UI. For example:

- **/etc/init.d/moogfarmd** - PROCESS_OWNER set to 'controluser'
- **\$APPSERVER_HOME/webapps/toolrunner/WEB-INF/web.xml** - toolrunneruser set to 'controluser' (toolrunnerpassword needs to be the password for that user)

Cisco recommends that you do not use the default 'moogsoft' user because that is a system user and does not allow you to log in using a password. Update the **/etc/init.d/** service scripts to have the correct:

- SERVICE_NAME (to make the services unique)
- PROCESS_OWNER (must be the same user as the toolrunner user)

- INSTANCE/CLUSTER/GROUP (unless already configured via relevant the LAM/Moogfarmd/system.conf configuration file). These need to be provided to the 'daemon' lines as command line parameters. For example **--instance MY_INSTANCE --group MY_GROUP --cluster MY_CLUSTER**.

Add the name of the service script into the 'service_name' field in **\$MOOGSOFT_HOME/config/system.conf** for that Cisco Crosswork Situation Manager process. To ensure the service appears in the right Self Monitoring tab, the process_type field must be set. See the default **system.conf** file for examples.

If a Moogfarmd service or LAM service is run that does not match a configuration block in system.conf/'processes', then it still appears within the UI 'Self Monitoring' dialog, but it is not possible to start/stop/restart the service.

The 'toolrunner' is used to control the services (requires configuring **\$APPSERVER_HOME/webapps/toolrunner/WEB-INF/web.xml**):

- The 'toolrunneruser' must match the PROCESS_OWNER specified within the relevant service script. This is because only root can run services as a different user.
- The 'toolrunnerpassword' must be the password of the 'toolrunneruser'.
- The 'toolrunnerhost' value must match the host of the machine which contains the moogfarmd/LAM services and the PROCESS_OWNER user.

It is more likely that an existing LAM/Moogfarmd service will have been run already in upgrade scenarios. If the service is one which needs to be controlled via the UI, then the service log file and PID (if present) need to be 'chowned' to the new service script PROCESS_OWNER/toolrunner user before it will work. For example:

```
chown toolrunneruser /var/log/moogsoft/moogfarmd.log
```

See the example of a **\$MOOGSOFT_HOME/config/system.conf** file below:

```
{
  "group"      : "moog_farmd",
  "instance"   : "",
  "service_name" : "moogfarmd",
  "process_type" : "moog_farmd",
  "reserved"   : true,
  "subcomponents" :
    [
      "AlertBuilder",
      "Sigaliser",
      "Default Cookbook",
      "Journaller",
      "TeamsMgr",
      #"AlertRulesEngine",
      #"SituationMgr",
      #"Notifier"
    ]
},
```

Audit Trail

Administrators can use the audit trail feature to review actions that have been performed on Situations or alerts. For example, you might want to view Situations that were resolved and closed within the last two weeks. You can use the Graze API endpoints **getAlertActions** and **getSituationActions** to achieve this. See [Graze API](#) for details.Graze API

When a user performs an action on a Situation or an alert, Cisco Crosswork Situation Manager records the user that performed this action and the time that it occurred. When a user resolves a Situation, Cisco Crosswork Situation Manager does not mark the alerts within it as resolved and no audit information is recorded for the individual alerts. When a user closes a Situation, the effect on the alerts within it depends on the setting in the Systems > Configure > Workflow tab. Cisco Crosswork Situation Manager records audit information for any alerts that are closed when the Situation is closed.

If a user manually resolves or closes individual alerts, Cisco Crosswork Situation Manager records the user that performed the action and time that it occurred.

You can use the Cisco Crosswork Situation Manager UI, Graze API, or MoogDb V2 to resolve or close Situations and alerts. See [Graze API](#) and [MoogDb V2](#) for details of the **resolveSituation**, **closeSituation**, **resolveAlerts**, and **closeAlert** endpoints/methods. Graze API MoogDb V2