CYTOMIC

ServiceNow integration guide_

Legal notice.

Registered trademarks.

Contact information.

Corporate Headquarters:
Cytomic (Business Unit of Panda Security S.L.)
Calle Santiago de Compostela 12
Bilbao (Bizkaia) 48003 Spain.
https://www.pandasecurity.com/uk/about/contact/

Version: 2.4.10

Author: Cytomic

Date: 20/03/2020

About the Cytomic Orion Snow plugin User Guide

- For the most recent version of this guide, refer to this web address:

https://info.cytomicmodel.com/resources/guides/Orion/en/ORION-snowguide-EN.pdf

Cytomic Orion User Guide

- For questions about a specific topic, access the product's online help at this web address:

https://info.cytomicmodel.com/resources/guides/Orion/en/ORION-guide-EN.pdf

- For questions about the specific features of Threat Hunting API, access online help at this web address:

https://info.cytomicmodel.com/resources/help/Orion/en/threathuntingAPI/index.htm

Contents

Chapter 1: Preface - 7

Intended Audience 7

Product Version 7

Document History.. 8

Icons 8

Chapter 2: Overview - 9

Overview of Cytomic Orion Snow plugin 9

Chapter 3: Importing the Cytomic Orion Snow plugin - 11

Prerequisites 12

Activating the Configuration Management for Scoped Apps plugin 12

Importing the Cytomic Orion SNOW.. 13

Requesting Cytomic Orion SNOW from the SNOW store 13

Installing the plugin using the xml file 14

Modifying the instance scope 15

Assigning Role to a User 15

Chapter 4: User Roles Supported by Cytomic Orion SNOW Plugin - - - - - - - - - - - - - - - 17

Supported roles 17

Plugin Admin Role 18

Plugin End User Role.. 18

Chapter 5: Using the Cytomic Orion Snow plugin - 19

Configuring the Cytomic Orion SNOW Account.. 19

Managing Indicators 21

Viewing indicators 21

Viewing Incidents 21

Deleting Indicators 22

Scheduling a Job 22

System Properties in Plugin 24

Viewing the logs 24

Changing log level... 25

Support 25

Chapter 1

Preface

This document describes how to import and use the Cytomic Orion ServiceNow (SNOW) plugin, where you can fetch alerts and create incidents.

CHAPTER CONTENT

Intended Audience - 7
Product Version - 7
Document History - 8
Icons - 8

Intended Audience

The reader of the Cytomic Orion ServiceNow (SNOW) plugin guide must be familiar with the following:

- Administrator knowledge of ServiceNow Client.

Product Version

This document applies to Cytomic Orion Snow plugin v1.0 release.

Document History

Date	Revision	Details
December 2019	0.2	Working draft
January 2020	0.3	Incorporate technical review comments
January 2020	0.4	Added delete indicators, system properties, and install plugin from SNOW store

Icons

In this guide, the following icons are used:

ⓘ	*Explanations and additional information, such as an alternative method for completing a certain task.*
⚠	*Suggestions and recommendations.*
💡	*Important tip regarding the correct use of Cytomic Orion Snow Plugin's options.*
🔍	*See other chapter or point in the handbook.*

Chapter 2

Overview

CHAPTER CONTENT

Overview of Cytomic Orion Snow plugin - 9

Overview of Cytomic Orion Snow plugin

The SNOW plugin integrates with Cytomic Orion and allows you to use SNOW for its ITSM requirements. The plugin provides indicators of attack and incident management for specified Cytomic Orion Indicators of Attack. The Indicators of Attack from Cytomic Orion are imported in ServiceNow. As a part of the Incident Management module, the plugin raises an incident for any serviceability event from Cytomic Orion in SNOW.

The Cytomic Orion Snow plugin integrates with the Cytomic Orion Platform. The plugin lets you use the SNOW platform for the ITSM requirements. It also provides indicators sync and incident management.

The Cytomic Orion plugin supports following features:

- Configure the Cytomic Orion account
- Raise incidents for indicators

Chapter 3

Importing the Cytomic Orion Snow plugin

This chapter describes the details to import the Cytomic Orion Snow plugin. It also provides steps to configure various parameters that are used by Cytomic Orion Snow plugin.

Perform the following settings and configurations in the mentioned sequence before you use the Cytomic Orion Snow plugin:

- Activate the Configuration Management for Scoped Apps plugin
- Import the Cytomic OrionCytomic Orion Snow plugin
- Assign role to a user

CHAPTER CONTENT

Prerequisites -12
Activating the Configuration Management for Scoped Apps plugin - - - - - - - - - - - - - -12
Prerequisites 12
Procedure 12
What to do next 13
Importing the Cytomic Orion SNOW -13
Requesting Cytomic Orion SNOW from the SNOW store 13
Prerequisites 13
Procedure 13
What to do next 14
Installing the plugin using the xml file 14
Prerequisites 14
Procedure 14
What to do next 15
Modifying the instance scope 15
Prerequisites 15
Procedure 15
What to do next 15
Assigning Role to a User 15
Prerequisites 15
Procedure 16
What to do next 16

Prerequisites

The plugin is installed in the SNOW instance. Before you begin installation of the Cytomic Orion Snow plugin, ensure that you have the following:

- Cytomic Orion Snow plugin version: v1.0
- Supported SNOW release: New York.

Activating the Configuration Management for Scoped Apps plugin

You must install the `Configuration Management for Scoped Apps (com.snc.cmdb.scoped)` plugin within a specified instance. After the plugin is installed successfully, the application is available to the users within SNOW.

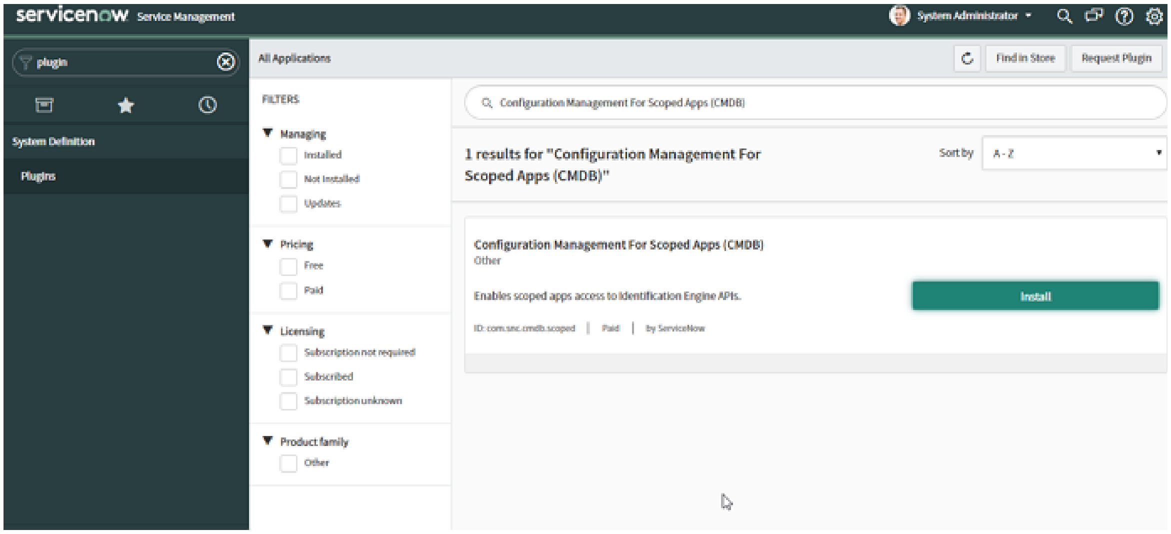
Prerequisites

User role: System Administrator

Procedure

To activate the Configuration Management for Scoped Apps plugin:

- Navigate to the ServiceNow Instance.
- Choose System Definition > Plugins.
- On the right pane, search for the **Configuration Management for scoped apps (com.snc.cmdb.scoped)** option, and click **Install**. The **Activate Plugin** dialog box is displayed.



1 results for "Configuration Management For Scoped Apps (CMDB)"

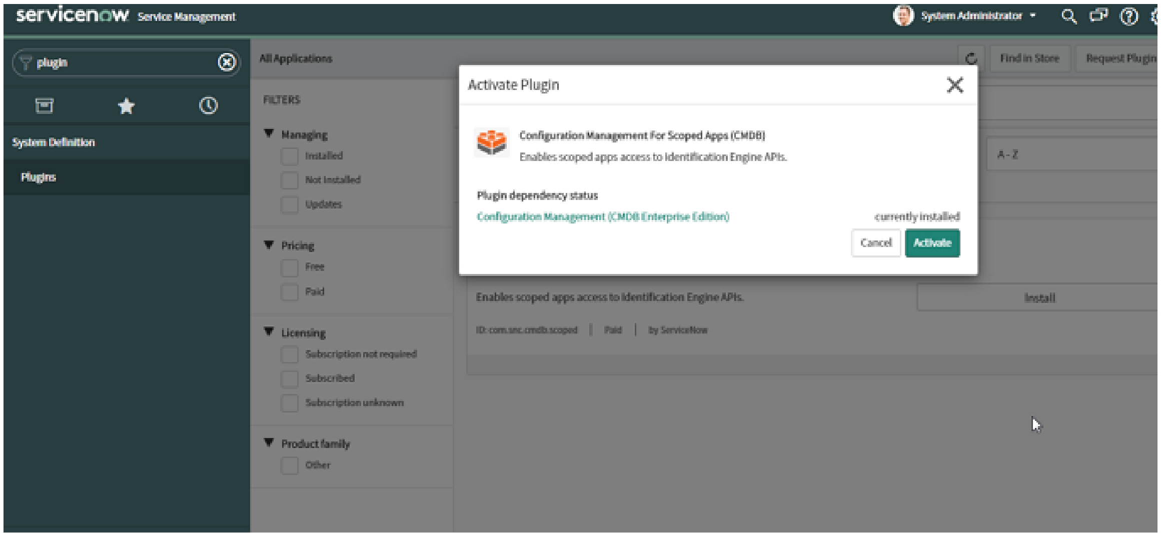
Configuration Management For Scoped Apps (CMDB)
Other

Enables scoped apps access to Identification Engine APIs.

ID: com.snc.cmdb.scoped | Paid | by ServiceNow

Figure 3.1: Activate Plugin gialog box

- In the **Activate Plugin** screen, click **Activate** to activate the plugin.



Activate Plugin

Configuration Management For Scoped Apps (CMDB)
Enables scoped apps access to Identification Engine APIs.

Plugin dependency status
Configuration Management (CMDB Enterprise Edition) currently installed

Enables scoped apps access to Identification Engine APIs.
ID: com.snc.cmdb.scoped | Paid | by ServiceNow

Figure 3.2: Activate plugin screen

What to do next

After you activate the Configuration Management for Scoped Apps plugin, import the Cytomic Orion Snow plugin.

Importing the Cytomic Orion SNOW

You can import the Cytomic Orion SNOW by either request the plugin from the SNOW store or using the xml file. Refer the following sections for more details.

> ⚠ *Only System Administrator can import the Cytomic Orion plugin to SNOW*

Requesting Cytomic Orion SNOW from the SNOW store

This section describes the steps to request the plugin through the HI service portal. You must install the plugin within a specified instance. After the plugin is installed successfully, the application is available to the users within SNOW.

Prerequisites

User role: System Administrator

Procedure

To request the **Cytomic Orion Snow plugin**:

- In the HI Service Portal, click **Service Requests** > **Activate Plugin**.

- Fill out the following details:
  - **Target Instance**: Instance on which you need to activate the plugin.
  - **Plugin Name**: Name of the plugin to activate.
  - **Specify the date and time you would like this plugin to be enabled**: Date and time must be at least 2 business days from the current time.

> Plugins are activated in two batches each business days in the Pacific time-zone, once in the morning and once in the evening. If the plugin must be activated at a specific time, enter the request in the **Reason/Comments** field.

  - **Reason/Comments**: Any information that would be helpful for the ServiceNow personnel activating the plugin such as if you need the plugin activated at a specific time instead of during one of the default activation windows.
- **Click Submit.**

The Cytomic Orion Snow plugin is installed and the available workflows are listed in the left navigation pane for the instance.

What to do next

After you have installed the Cytomic Orion Snow plugin, assign role to the users.

Installing the plugin using the xml file

This section describes the details to install the plugin using the xml file.

An XML file is provided that is the application-build for version 1.0 release. System Admin of the ServiceNow instance will install it into the ServiceNow platform.

This section describes the detailed steps to install the < cytomic_orion_snow_plugin.XML > file. You must install the plugin within a specified instance. After the xml file is committed successfully, the application is available to the users within SNOW.

Prerequisites

- **User role**: System Administrator
- ServiceNow instance should exist.

Procedure

To import the Cytomic XML file plugin to SNOW:

- Navigate to the **ServiceNow** Instance.
- On left pane, search for the **Retrieved Update Set** option, and click **Retrieved Updated Set**.
- Click the **Import Update Set from XML** link.

- Navigate to the **Import XML** page, click the **Choose File** button, and browse the XML file from local storage.
- After the XML file is attached, click the **Upload** button.
- Navigate to the **Retrieved Update** Set page, and click **Build**.
- Click the **Preview Update Set** button. The **Commit Update** screen is displayed.
- Click the **Commit Update Set** button.

After build is committed, search Cytomic Orion in left pane.

What to do next

Modify the instance scope.

Modifying the instance scope

After importing the plugin, you must modify the instance scope as follows.

Prerequisites

User role: System Administrator

Procedure

To modify the instance scope:

- Click the **Setting** icon in right most corner of the ServiceNow screen. A pop-up is displayed.
- Select the **Developer** option.
- Under the **Developer** option, click the **ON** button or activate the **Show application picker in header** listed option.
- Navigate to the home page and change the instance scope from **Global** to **Cytomic Orion**.

What to do next

Assign role to a user.

Assigning Role to a User

After you add a user (or group), you must assign a role to the user (or group).

Prerequisites

User role: System Administrator

Procedure

To assign role to a user:

- Open the required instance and login using the credentials. You must login as a System Admin.
- Search **Users** on the left navigation pane.
- Choose **System Security** > **Users** to display a list of added users in the right pane.
- To create new user:
  - In upper left corner, click **New**. The **Create New User** page is displayed.
  - Enter username and password in the **Username** and **Password** fields.
  - Click **Submit**.
- Click the user whom you want to provide the roles. The **User** details form is displayed.
- Scroll to the bottom of the form.
- Select the **Roles** tab and click **Edit**. Available roles are listed in the **Collection** slush bucket.
- Move the required roles as required using the arrows.
- Click **Save**.

The selected role is assigned to the user.

What to do next

Similarly, you can add role to groups.

Chapter 4

User Roles Supported by Cytomic Orion SNOW Plugin

Role-based access control (RBAC) is a method of restricting or authorizing system access for users based on user roles. A role defines the privileges of a user in the Cytomic Orion Snow plugin.

CHAPTER CONTENT

Supported roles -17
Plugin Admin Role -18
Plugin End User Role -18

Supported roles

The Cytomic Orion Snow plugin supports the following roles:

- **Plugin Admin**:
  - itil role
  - X_383430_cytomic_orion.Cytomic_admin
  - X_383430_cytomic_orion.Cytomic_user
- **Plugin End User**:
  - X_383430_cytomic_orion.Cytomic_user
  - itil role
- **System Admin: Admin role**

To view or edit incident, the system administrator should provide ITIL role to the user.

The following table lists features supported by different user roles:

Feature	System Admin	Plugin Admin	Plugin End User
Install Cytomic Orion Snow plugin	YES	NO	NO
User creation	YES	NO	NO
Configure Cytomic Orion	YES	YES	NO
List logs	YES	YES	NO
List indicators/incidents	YES	YES	YES
Schedule jobs	YES	YES	NO
Support	YES	YES	YES

Table 4.1: features supported by different user roles

Plugin Admin Role

The Plugin Admin role involves configuring Cytomic Orion, viewing Indicators, and Incidents.

Plugin End User Role

The Plugin End User roles can access the Cytomic Orion Snow plugin and has access to view indicators, and raise incidents. For more information on carrying out the end-user tasks, see the "**Using the Cytomic Orion Snow plugin**".

Chapter 5

Using the Cytomic Orion Snow plugin

To use the Cytomic Orion Snow plugin, you must configure Cytomic Orion SNOW. After configuring the account, indicators are imported automatically. Based on the schedule job intervals, indicators are imported. Incidents are raised based on the indicators conditions set on the configuration page.

CHAPTER CONTENTS

Configuring the Cytomic Orion SNOW Account - 19
Before you begin 19
Procedure 20
Managing Indicators - 21
Viewing indicators 21
Procedure 21
Viewing Incidents 21
Procedure 21
Deleting Indicators 22
Procedure 22
Scheduling a Job - 22
Procedure 23
To schedule jobs: 23
System Properties in Plugin - 24
Viewing the logs - 24
Procedure 25
Changing log level 25
Support - 25
Procedure 25

Configuring the Cytomic Orion SNOW Account

After you have imported the Cytomic Orion Snow plugin, you must configure Cytomic Orion so that you can import the indicators that are used to create incidents.

Before you begin

To configure Cytomic Orion, ensure that you have the username and password.

Procedure

To configure Cytomic Orion:

- Open the required instance and login using the credentials. You must login as Plugin Admin.
- Choose **Cytomic Orion** > **Configuration** from the left pane. The **Configuration** page is displayed.
- Enter the following details in the **Configuration** page:

Field	Description
Description	Enter the description in the Description field.
Username	Enter the Cytomic Orion username in the Username field.
Password	Enter the Cytomic Orion password in the Password field.
Create Security Incident	Under **Security Incidents**, select the **Create Security Incident** check box.
Minimum alert severity to create an incident	From the **Minimum alert severity to create an Incident** drop-down list, choose the required severity. Available severity are: • Low • Medium • High • Critical • Undefined ⚠ *If you want to change the severity of the client configuration, it will be applied for an indicator fetched after the setting is done. If this change needs to be done for all the already fetched indicators, the admin must delete the configuration and submit the configuration again.*
Assign to group	Search for the group to which you need to assign in the **Assign to group** search box
Populate CMDB	Under CMDB, select the **Populate CMDB** check box. ⚠ *When a user deletes the configuration, the CMDB goes in to retired state. If you want see the state of Cytomic CMDB table then you need to go in CMDB_ci table and add the status column in the Cytomic CMDB table.*

Table 5.1: Configuration page fields

- (Optional) To clear all the configuration data, click **Delete**.
- Click the **Check Connection** and **Submit** button to configure the SNOW account.

Managing Indicators

After the Cytomic Orion Snow plugin is installed, indicators are imported depending on the scheduled jobs interval. By default, indicators are imported after every 15 minutes. If you want to import indicators immediately, see "**Scheduling a Job**" on page **22**.

Viewing indicators

You can list and search for a specific indicators using the Search filter.

Procedure

To view Indicators:

- Open the required instance and login using the credentials.
- Choose **Cytomic Orion** > **Indicators of Attack** from the left pane. The **Indicators of Attach** page is displayed.
- Choose **Indicators** from the left pane.
- All Indicators are displayed on the right pane.
- The Indicators table supports the following features:
  - **Filtering**: Click the **Filter** icon on the top left of the **Indicators** page. Enter the details to filter the indicators, and then click **Run**. The Indicators list is filtered as per the inputs provided.
  - **Sorting**: You can sort the table for all columns by clicking the table heading.
  - **Pagination**: You can navigate to the required page of listed Indicators. Each page lists 20 indicators.
  - **View a particular incident for an indicator**: To view details of an incident that is created for an indicator, click the respective Incident. You are redirected to the **Incidents** page. For more information on viewing the incidents, see "**Viewing Incidents**" on page **21**.

Viewing Incidents

After the indicators are imported to the Cytomic Orion Snow plugin, depending on the Indicator Severity, incidents are created automatically. You can add a post on a specific incident. In addition, you can add attachments and change the state of an incident.

Procedure

To view Incidents

- Open the required instance and login using the credentials.
- Choose **Cytomic Orion** > **Indicators of Attack** from the left pane. **The Indicators of Attack** page is displayed.
- Choose **Incidents** on the left pane. All incidents are displayed on the right pane.

- The Incidents table supports the following features:
  - **Filtering**: Click the **Filter** icon on the top left of the Incidents page. Enter the details to filter the alarms, and then click Run. The Incidents list is filtered as per the inputs provided.
  - **Sorting**: You can sort the table for all columns by clicking the table heading.
  - **Pagination**: You can navigate to the required page of listed Incidents.
  - **View a particular incident**: To view details of an incident, click the respective Incident

Deleting Indicators

You can delete indicators if the incident associated with it is in the closed or cancelled state only.

Procedure

To delete Indicators:

- Open the required instance and login using the credentials.
- Choose **Cytomic Orion** > **Indicators of Attack** from the left pane. The **Indicators of Attach** page is displayed.
- Choose **Indicators** from the left pane. All Indicators are displayed on the right pane.

You can delete the Indicator from the Form view or List view.

- For List view:
  - Select the check box next to the Indicator that you want to delete.
  - Browse to the bottom of the list view and select **Delete** from the **Actions on selected rows** drop-down list.
- For Form view:
  - Click the Indicator. The Form view is displayed.
  - Click the **Delete** button.
- Click **OK** in the Confirmation screen

Scheduling a Job

The Cytomic Orion Snow plugin facilitates to schedule periodic jobs from ServiceNow. The Plugin Admin can configure job execution on demand basis or schedule the jobs for execution on daily, weekly, and monthly basis. You can also set a particular period to execute a job.

The **Fetch Alarms Scheduler** is a thread running every 15 minutes. It will fetch the token from the configuration table and use it for fetching the alarms. This thread dumps alarms in a dump table and using the transform map, the unique alarms are added into the mail indicators table. While this process goes on, transform map also creates incident for this alarm if the configuration permits.

In case, there are issues faced while fetching a token, the plugin will retry and fetch a new token.

By default, Cytomic Orion indicators are imported every 15 minutes. You can configure this interval based on your requirement. Jobs scheduling follows the polling mechanism. This is a one-time activity.

The Cytomic Orion Snow plugin also provides the facility to provide conditions to execute a job. Also, you can execute scripts while scheduling jobs.

Procedure

System Admin and Plugin admin can perform this operation.

To schedule jobs:

- Open the required instance and login using the credentials. You must login as Plugin Admin.
- Search *__Cytomic in the Name__ field. Available jobs are listed.
- Click the job you want to modify. The **Scheduled Script Execution** page is displayed.
- From the **Run** drop-down list, choose the pattern in which you want to schedule the jobs. Available options are:
  - **Daily**
  - **Weekly**
  - **Monthly**
  - **Periodically**
  - **Once**
  - **On Demand**

Based on the selection in this field, you can edit the **Repeat Interval** field.

Field	Description
Daily drop-down list	Indicates that the job can be executed daily at a specified time.
Weekly drop-down list	Indicates that the job can be executed by selecting a specific week day and time. The job will be executed at the specified time every week.
Monthly drop-down list	Indicates that the job can be executed by selecting a date and time. The job is executed at the specified time and date.

Table 5.2: Repeat interval options

Field	Description
Periodically drop-down list	Indicates that a job is executed periodically. For example, it can be executed after specified days at a specified time starting from a particular date and time.
Once drop-down list	Indicates the job is executed at the specified date and time only once.
On Demand drop-down list	Indicates the job is executed when the Execute Now button is clicked.

Table 5.2: Repeat interval options

For example, if you configure the interval to **Daily** and enter the **Time** as 15 minutes, the indicators are imported every 15 minutes from Cytomic Orion into the plugin.

- Click **Update** to save the job and click **Execute Now** to execute the job immediately

System Properties in Plugin

Following are the Cytomic Orion system properties:

- `x_383430_cytomic_o.fetchAlarmsFromDays`: To fetch the Indicators of Attack for the very first time (each time the configuration is saved). Default time is set to 10 days.
- `x_383430_cytomic_o.scheduler_fetchFrom`: The number of milliseconds for the past Indicators of Attack scheduler will try to fetch Indicators of Attack from the current time. The default time is set to 20 minutes, i.e. 1200000ms.
- `x_383430_cytomic_o.support_URL`: This system property points you to the support email address and is used to send queries to the support team.
- `x_383430_cytomic_o.Documentation_UR`L: This system property guides you to the documentation URL that provides you the detailed user guide

Viewing the logs

The Logs module is visible to the System Admin and plugin admin roles. Depending on the log level you select while authenticating the Cytomic Orion Snow plugin, respective level of logs will be displayed.

- **ERROR**: An error represents serious issues and the failure of an important operation in the application.
- **WARN**: It indicates that the system might have a problem or an unusual situation occur.
- **INFO**: Messages correspond to normal application behaviour and milestones.
- **DEBUG**: At this level, you can capture every detail about the application's behaviour.

For more information on configuring the log level, see "**Configuring the Cytomic Orion SNOW Account**" on page 19.

Procedure

To view logs:

- Open the required instance and log in using the plugin admin credentials.
- Search *Cytomic in the left pane.
- Click **Logs** to list the plugin logs.

Available logs are listed in the right pane.

Changing log level

This section provides the details to change the plugin log level.

Procedure:

- Search `sys_properties` in Filter navigator.
- Enter *`cytomic_orion.log_level` in the **Name** filter on system properties table.
- Click filtered property.
- Cytomic Orion generates the logs based on log level. The default log level is INFO.

Following are available log levels:

- ERROR
- WARN
- INFO
- DEBUG
- To change the log level, enter the respective log level number in the **Value** field, and click **Update**.

For example, to set the log level as **DEBUG**, enter 4 in the **Value** field, and click **Update**.

Support

This section describes the support details that you may require to raise a support request to Cytomic Orion while using Cytomic Orion Snow plugin.

Procedure

To view support details:

- Open the required instance and login using the credentials.
- Choose **Cytomic Orion** > **Support** from the left pane.

The **Cytomic Orion for Security Operations** page is displayed.

- The Support details page is displayed.

- Click the **Cytomic Orion Support** link to contact the support team.