

Alarms

This chapter provides description, severity, and troubleshooting procedure for each commonly encountered alarm.

- Fault Monitoring, on page 1
- Configure Alarms and Controls, on page 2
- Display Transient Conditions, on page 3
- Display Historical Alarms, on page 4
- Sensor Alarms Supported by NCS2K-SVO-K9 Card, on page 5
- Log into the SVO Web Interface, on page 7
- Create an SVO Instance, on page 7
- Log into the Cisco SVO Admin Plane, on page 8
- ENC-CERT-EXP, on page 9
- FOIC Group ID Mismatch, on page 9
- FOIC-LDI-LD, on page 10
- FOIC-LDI-RD, on page 10
- FOIC-LOF-LOM, on page 11
- FOIC-LOL, on page 12
- FOIC-LOM, on page 12
- FOIC-PMM, on page 13
- FOIC-RPF, on page 13
- FOIC-TIM, on page 14
- PEER-CSF, on page 14
- TRUNK-PAYLOAD-MISM, on page 14
- USB-MOUNT-FAIL Alarm, on page 15

Fault Monitoring

The Fault Monitoring pane provides an alarm summary for all alarms and conditions that are encoutered. It displays the number of Critical (CR), Major (MJ), Minor (MN), Warnings (W), and Non-applicable (NA) alarms. It displays the alarms, transient conditions, and historical alarms that are related to chassis, passive devices, pluggables, line cards, amplifier cards, and control cards. You can also create custom alarm profiles and apply them on the node using this pane.

Configure Alarms and Controls

Use this task to configure external (environmental) alarms and external controls.

Note You can configure up to 14 alarms in the external alarms mode. You can configure up to 10 entities under external alarms and 4 entities under external controls in the external controls mode.

Before you begin

Log into the SVO Web Interface, on page 7

Step 1 Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

The SVO Topology page appears.

Step 2 Click the rack in the left panel.

The rack view appears.

Step 3 Left-click the chassis and select **Open**.

The chassis view appears.

Step 4 Click the **Provisioning** > **Alarm Extender** > **Alarm Dry Contacts Mode** tabs.

Step 5 Choose whether to configure the alarms as external alarms or external controls.

a. To configure external alarms, click the **External Alarm** option and click **Apply**.

b. To configure external controls, click the **External Control** option and click **Apply**.

Step 6 To configure external alarms, click the **External Alarms** tab, complete the following fields, and click **Apply**.

- **Enabled**—Check the check box to activate the fields for the alarm input number.
- **Severity**—Choose a severity from the drop-down list.

  The severity determines the alarm's severity in the Alarms and History tabs.

- **Alarm Type**—Choose an alarm type from the drop-down list.
- **Virtual Wire**—Choose the virtual wire number from the drop-down list to assign the external device to a virtual wire. Otherwise, do not change the None value.
- **Raised When**—From the drop-down list, choose the contact condition (open or closed) that triggers the alarm.
- **Description**—Enter a description.

Step 7 To configure external controls, click the **External Controls** tab, complete the following fields, and click **Apply**.

- **Enabled**—Check this check box to activate the fields for the alarm input number.
- **Control Type**—Choose the control type from the drop-down list: air conditioner, engine, fan, generator, heat, light, sprinkler, or miscellaneous.
- **Trigger Type**—Choose a trigger type: a local minor, major, or critical alarm; a remote minor, major, or critical alarm; or a virtual wire activation.
- **Description**—Enter a description.

Note External alarms and external controls must be recorded locally for the network element (NE). Both the alarm name and resolution are node-specific.

Step 8 To add new alarm types, complete the following:

a) Click the **User Defined Alarms** tab.

The user-defined alarms are displayed under the External Alarms tab if provisioned. If the user-defined alarm is configured as an external alarm, the alarm cannot be deleted. You can create up to 50 user-defined alarms.

b) Click **Add**.

c) Enter the new alarm type and click **OK**.

Display Transient Conditions

Use this task to display the transient conditions raised on a rack, chassis, or card.

Before you begin

Log into the SVO Web Interface, on page 7

Step 1 Perform this step, as needed.

a) To view the transient conditions raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Click the **Conditions** tab.

b) To view the transient conditions raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **Conditions** tab.

c) To view the transient conditions raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **Conditions** tab.

Step 2 Click **Fetch Conditions** to display the transient conditions.

Step 3 Click **Export to Excel** to export the transient conditions to the excel sheet.

Display Historical Alarms

Use this task to display the historical alarms raised on a rack, chassis, or card.

Before you begin

Log into the SVO Web Interface, on page 7

Step 1 Perform this step, as needed.

a) To view the historical alarms raised on the specific rack, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Click the **History** tab.

b) To view the historical alarms raised on the specific chassis, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Click the **History** tab.

c) To view the historical alarms raised on the specific card, perform these steps:

1. Click the hamburger icon at the top-left of the page, and select **SVO Topology**.

   The SVO Topology page appears.

2. Click the rack in the left panel.

   The rack view appears.

3. Left-click the chassis and select **Open**.

   The chassis view appears.

4. Left-click the card and select **Open Card**.

   The card view appears.

5. Click the **History** tab.

Step 2 Click **Export to Excel** to export the historical alarms to the excel sheet.

Step 3 From the **Severity** drop-down list, choose a severity to filter the alarms based on severity.

Sensor Alarms Supported by NCS2K-SVO-K9 Card

The following sensor alarms are supported by the NCS2K-SVO-9K card. All the sensor alarms are cleared when the sensor value reverts to normal or within the expected range. The default severity of all these alarms is Minor (MN), Non-Service-Affecting (NSA).

- SENSOR_HIGH_0_6V_CPU_B
- SENSOR_LOW_0_6V_CPU_B
- SENSOR_HIGH_1_2V_CPU
- SENSOR_LOW_1_2V_CPU
- SENSOR_HIGH_1_5V_CPU
- SENSOR_LOW_1_5V_CPU
- SENSOR_HIGH_1_7V_CPU
- SENSOR_LOW_1_7V_CPU
- SENSOR_HIGH_3_3V_CPU
- SENSOR_LOW_3_3V_CPU
- SENSOR_HIGH_1_05V_CPU
- SENSOR_LOW_1_05V_CPU
- SENSOR_HIGH_1_82V_CPU
- SENSOR_LOW_1_82V_CPU
- SENSOR_HIGH_1_3V_CPU

- SENSOR_LOW_1_3V_CPU
- SENSOR_HIGH_0_6V_CPU_A
- SENSOR_LOW_0_6V_CPU_A
- SENSOR_HIGH_5_0V_STDBY
- SENSOR_LOW_5_0V_STDBY
- SENSOR_HIGH_3_3V_STDBY
- SENSOR_LOW_3_3V_STDBY
- SENSOR_HIGH_3_3V
- SENSOR_LOW_3_3V
- SENSOR_HIGH_2_5V
- SENSOR_LOW_2_5V
- SENSOR_HIGH_1_8V
- SENSOR_LOW_1_8V
- SENSOR_HIGH_1_2V
- SENSOR_LOW_1_2V
- SENSOR_HIGH_1_0V_PHY
- SENSOR_LOW_1_0V_PHY
- SENSOR_HIGH_1_0V
- SENSOR_LOW_1_0V
- SENSOR_HIGH_BP_48V
- SENSOR_LOW_BP_48V
- SENSOR_HIGH_HOTSPOT2
- SENSOR_LOW_HOTSPOT2
- SENSOR_HIGH_HOTSPOT1
- SENSOR_LOW_HOTSPOT1
- SENSOR_HIGH_INLET_AIR
- SENSOR_LOW_INLET_AIR
- SENSOR_HIGH_OUTLER_AIR
- OUTLER_AIR_SENSOR_LOW
- SENSOR_HIGH_ETH_SWITCH_TEMP
- SENSOR_LOW_ETH_SWITCH_TEMP
- SENSOR_HIGH_CPU_TEMP

- SENSOR_LOW_CPU_TEMP
- SENSOR_HIGH_DDR_CH0_TEMP
- SENSOR_LOW_DDR_CH0_TEMP
- SENSOR_HIGH_DDR_CH1_TEMP
- SENSOR_LOW_DDR_CH1_TEMP

Log into the SVO Web Interface

Use this task to log into the SVO web interface (SVO instance).

Step 1 In the browser URL field, enter the IP address of the SVO instance.

The IP address to be used is the management IP address that is configured in the Create an SVO Instance, on page 7 task.

The Network Services Orchestrator login page appears.

Step 2 Enter the username and password.

Note
- Use the superuser or admin credentials (configured in the Create an SVO Instance, on page 7 task) to log into a ROADM SVO instance.
- Use the admin credentials (configured in the Create an SVO Instance, on page 7 task) to log into a ROADM SVO instance.

Step 3 Click **Login**.

Create an SVO Instance

Use this task to configure an SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 8

Step 1 Click the + button at the top-left of the SVO Instances page.

The SVO Instance Configuration page appears.

Step 2 In the **General Info** area, perform these steps:

a) Enter the name for the new SVO instance in the **Name** field.

The name is mandatory and must be unique among the SVO instances managed by the admin plane. It can contain a minimum of two characters and a maximum of 64 characters. It can include numbers, uppercase letters, lowercase letters, dashes (-), or underscores (_).

b) Choose the version from the **Software Version** drop-down list.

c) Choose the type of the SVO instance from the **TDM Terminology** drop-down list.

The two options are ANSI and ETSI.

d) Choose the label of the SVO instance from the **Type** drop-down list.

The four options are ROADM, OLA, DGE, and TXP. The type indicates the role of the SVO instance in the network.

Note When Type is selected, a default value for memory size is displayed in the **Reserved Memory GB** field.

e) Choose the memory size to be allocated to the SVO instance from the **Reserved Memory GB** field.

The user is allowed to reserve the SVO container memory in steps of 1GB. This value is visible and summarized at server level in the SVO instances table.

Step 3 In the **Admin User** area, perform these steps:

a) Enter the username in the **Username** field.

The values "admin," "oper," "private," or, "public" cannot be used as the admin username.

b) Enter the password in the **Password** field.

The password must be a minimum of eight characters. The password must contain at least an uppercase letter a number, and a special character. The special characters supported are ! $ % ^ ( ) [ ] _ - ~ { } . +

c) Enter the password again in the **Retype Password** field.

Step 4 In the **Management Network** area, the system suggests the management subnets to be used in the **IPv4 Address** or the **IPv6 Address** fields, depending on the type of addressing defined during the installation. The system checks for constraints defined in the network configuration file and ensures that the IP addresses that are assigned are not in use.

a) Enter the IPv4 Address in the **IPv4 Address** field in a SVO card model.

or

b) Enter the IPv4 or the IPv6 Address in the **IPv4 Address** or **IPv6 Address** field respectively in an external server model.

Step 5 Click **Create**.

Step 6 A message is displayed indicating the creation of the SVO instance.

Step 7 Click **OK**.

The SVO Instances page appears. The table displays the new SVO instance.

The SVO instance can now be accessed through a web browser.

Log into the Cisco SVO Admin Plane

Use this task to log in to the Cisco SVO admin plane.

Step 1 In the browser URL field, enter the IP address of the admin plane (https://*IP_address*/login).

The login page appears.

Step 2 Enter the username and password.

In an SVO card system, only the superuser is allowed to log in to the Cisco SVO admin plane.

Step 3 Click **Login**.

The SVO Instances page is displayed.

ENC-CERT-EXP

Default Severity: Minor

Logical Object: NearEnd

Resource Type: ODUK

The Encryption Certificate Expired alarm is raised on line cards such as 400G-XP-LC, WSE, and MR-MXP when the SUDI 2029 MIC encryption certificate expires.

Clear the ENC-CERT-EXP Alarm

Perform one of the following :

- Change the encryption certificate type to LSC
- Disable the Encryption
- Verify if both the near-end and far-end line cards have the software package as release 11.12 and above

FOIC Group ID Mismatch

Default Severity: Major

Logical Object: Standing

Resource Type: zrPlus

The FOIC (FlexO-SR Interface) Group ID Mismatch alarm is raised due to one of the following conditions:

- When configurations of the system are incorrect
- When unsupported trunks with the same rate are reconnected back to back

Clear the FOIC Group ID Mismatch Alarm

The alarm clears when configurations are correct or supported trunk is connected back.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-LDI-LD

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Link Degrade Indicator-Local Degrade (FOIC-LDI-LD) alarm is raised due to one of the following conditions:

- When Local Degrade Indicator CA is inserted
- When Pre-FEC degrade is detected at the near end

Clear the FOIC-LDI-LD Alarm

The FOIC Link Degrade Indicator-Local Degrade (FOIC-LDI-LD) alarm clears due to one of the following conditions:

- When Local Degrade Indicator CA is removed
- When no Pre-FEC degrade is detected at the near end

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-LDI-RD

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Link Degrade Indicator-Remote Degrade (FOIC-LDI-RD) alarm is raised due to one of the following conditions:

- When Local Degrade Indicator CA is detected at the far end

- When Pre-FEC degrade is detected at the near end

Clear the FOIC-LDI-RD Alarm

The alarm clears due to one of the following conditions:

- When Local Degrade CA is not detected at the far end.
- When Pre-FEC degrade is not detected at the near end.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-LOF-LOM

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Loss of Frame-Loss of Multi-frame (FOIC-LOF-LOM) alarm is raised due to one of the following conditions:

- High FEC error due to very low OSNR on the trunk Side
- Out of range of the OSNR
- Misconstructed or different modulation

Clear the FOIC-LOF-LOM Alarm

The alarm clears due to one of the following conditions:

- No High FEC error due to very low OSNR on the trunk Side
- The OSNR is not out of range
- No misconstructed or different modulation

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-LOL

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Loss of Lock alarm is raised due to one of the following:

- High FEC error due to very low OSNR on the Trunk side
- Out of range of the OSNR
- Misconstructed or different modulation

Clear the FOIC-LOL Alarm

The alarm clears when clearing the HIGH FEC error due to very low OSNR on the trunk side or out of range of the OSNR or misconstructed or different Modulation.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-LOM

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Loss of Multi-frame alarm is raised due to one of the following:

- High FEC error due to very low OSNR on the Trunk side
- Out of range of the OSNR
- Misconstructed or different Modulation

Clear the FOIC-LOM Alarm

The alarm clears after clearing the HIGH FEC error due to very low OSNR on the Trunk side or out of range of the OSNR or misconstructed or different Modulation.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-PMM

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Phy Map Mismatch (FOIC-PMM) alarm is raised due to one of the following conditions:

- Misconfiguration of the system.
- When unsupported trunks with the same rate are reconnected back to back.

Clear the FOIC-PMM Alarm

The alarm clears due to correct configuration or when the supported Trunk is connected back.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-RPF

Default Severity: Minor

Logical Object: Standing

Resource Type: zrPlus

The FOIC Remote Phy Fault (FOIC-RPF) alarm is raised to inform the far-end node about the locally detected failure of the PHY.

Clear the FOIC-RPF Alarm

The alarm clears when clearing the locally detected failure of the PHY.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FOIC-TIM

Default Severity: Critical

Logical Object: Standing

Resource Type: zrPlus

The FOIC Trail Trace Identifier Mismatch (FOIC-TIM) alarm is raised when there is a mismatch between the expected TTI string that is provisioned and the received TTI string from the far-end.

Clear the FOIC-TIM Alarm

The alarm clears when there is no mismatch between the expected TTI string that is provisioned and the received TTI String from the far-end.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PEER-CSF

Default Severity: Major(MJ), Service-Affecting(SA)

Logical Object: STM/OCN

Resource Type: ODUK

The Peer Client Signal Fail alarm is a secondary alarm raised on local OCN, OTU1, or SDI_3G_VIDEO ports when a remote Service-Affecting (SA) alarm causes an invalid data transmission. The alarm is raised locally on AR_MXP and AR_XP ports and does not indicate that a Service-Affecting (SA) failure has occured at the local site. Instead, it indicates that an alarm such as LOS, LOS-P, LOF, OTU-AIS is caused by an event affecting the transmission capability of the remote port.

Clear the PEER-CSF Alarm

Clear the Service-Affecting (SA) alarm at the remote data port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRUNK-PAYLOAD-MISM

Default Severity: Major(MJ), Service-Affecting(SA)

Logical Object: OCN,OTN,GE,FC

The TRUNK-PAYLOAD-MISM alarm is raised on the 10x10G-LC card, which is configured in the 10x10G muxponder mode. This occurs when the payload types configured at the near-end and far-end nodes are different.

Clear the TRUNK-PAYLOAD-MISM Alarm

Step 1 Log in to a node with Cisco SVO web user interface.

Step 2 In the rack view, click the line card.

A menu appears.

Step 3 From the menu, click **Open Card**.

Step 4 In the card slot view, Click the **Provisioning** tab.

Step 5 Click the **Pluggable Port Modules** tab.

Step 6 In the **Pluggable Port Modules** tab, click the plus (+) sign.

Step 7 Select the **Port ID**.

Step 8 Choose the same payload type from the **Port Type** drop-down list.

Step 9 Click **OK**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

USB-MOUNT-FAIL Alarm

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: USB

Resource Type: USB_FLASH

The USB Mount Fail (USB-MOUNT-FAIL) alarm is raised when the USB flash is not mounted.

Clearing the USB-MOUNT-FAIL Alarm

Step 1 Back up the database of the active control card.

Step 2 Remove the standby control card.

Step 3 Reboot the active control card.

Step 4 After the active control card is rebooted, reinsert the standby control card.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.