



CHAPTER 17

Checking Bug Status Using Bug Toolkit

Bug Toolkit is an application in Resource Manager Essentials that helps the user identify the bugs filed against devices in their network and check the status of the bugs.

You can generate reports based on bugs filed against IOS and CATOS devices that are managed in the your network.

To generate reports using Bug Toolkit from the CiscoWorks desktop:

-
- Step 1** Select **RME > Reports > Report Generator**.
The Report Generator dialog box appears.
 - Step 2** Select **Bug Toolkit** from the Select an Application drop down list box.
You can then generate reports using Bug Toolkit.
-

Bug Summary Report

The Bug Summary Report option allows you to view a summary of the software image bugs for a group of devices.

If you do not have a user account and password on Cisco.com, contact your channel partner or enter a request on the main Cisco web site at www.cisco.com.

To create a Bug Summary report:

-
- Step 1** Select **RME > Reports > Report Generator**.
The Report Generator dialog box appears.
 - Step 2** Select **Bug Toolkit** from the Select an Application drop down list box.
 - Step 3** Select **Bug Summary Report** from the Select a Report drop down list box.
 - Step 4** Select the devices for which you want a summary of outstanding bugs using device selector.
 - Step 5** Select the hyperlink **Click Here** below the Device Selector to launch the Cisco.com Bug Toolkit.
The Bug Toolkit is launched in a separate browser window where you can view bugs on any Cisco IOS version.
 - Step 6** Enter the information required to generate a report:

Field	Description	Usage Notes
Scheduling		
Run Type	Schedules the job to run immediately or in the future.	Select one of the following options from the drop-down list box: Immediate—Runs the report immediately. Once—Runs the report once according to the date and time that you specify. 6-hourly—Runs a job every six hours. 12-hourly—Runs a job every twelve hours. Daily—Runs everyday according to the time that you specify. Weekly—Runs weekly according to the day of the week and the time that you specify. Monthly—Runs monthly according to the day of the month and the time that you specify.
Date	Date on which you want to run the job.	Click on the calendar icon and select the start date. If Run Type is Immediate, the system date is automatically selected.
At	Time when you want to run the job in the future.	Select the hours and minutes from the drop-down lists. If Run Type is Immediate, the system time is automatically selected.
Job Info		
Job Description	Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.	Make each description unique so you can easily identify jobs.
E-mail	Enter e-mail addresses to which the job sends messages at the end of the job. You can enter multiple e-mail addresses separated by commas. Configure the SMTP server to send e-mails in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). We recommend that you configure the CiscoWorks E-mail ID in the View / Edit System Preferences dialog box (Common Services > Server > Admin > System Preferences). When the job starts or completes, an e-mail is sent with the CiscoWorks E-mail ID as the sender's address.	Send an e-mail notification when a job is completed.

Field	Description	Usage Notes
Criteria		
Report Bugs From	Displays bugs filed from a particular date.	Select the date from which you wish to run a query.
Cisco.com Profile		
User Name	Cisco.com user name.	Enter your Cisco.com login ID.
Password	Cisco.com password.	Enter your Cisco.com password.
Proxy Username	Proxy Username	Enter Proxy Username.
Proxy Password	Proxy Password	Enter Proxy Password You are prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in: Common Services > Security > Cisco.com Connection Management Proxy Server Setup

The Cisco Username, Cisco Password, Proxy Username and Proxy Password textboxes will be auto-populated while scheduling a Bugtool Kit report job, if the Username and Password is already provided under:

Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup

However, you can still change the credentials while generating the report.

Step 7 Click **Finish**.

The Software Image Bugs Summary Report appears.

Logging Into Cisco.com

To access Cisco.com, login privileges are required. You can login to Cisco.com by entering your Cisco.com username and password. If you enter Cisco.com credentials in this workflow, these credentials are valid only for that session.

You are also prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in:

Common Services > Security > Cisco.com Connection Management Proxy Server Setup



Note

Cisco.com account credentials from **Common Services > Security > Cisco.com Connection Management > Cisco.com User Account Setup** and proxy username/password credentials from **Common Services > Security > Cisco.com Connection Management Proxy Server Setup** will not be used henceforth.

RME will use the central Cisco.com credentials as default if they are configured under **Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup**, while generating reports based on PSIRT data or End of Sale/End of Life data or Bug Tool Kit. You can still change these credentials when you are scheduling the report jobs. You will be prompted to enter these Cisco.com credentials if they are not configured.

However tasks like Contract Connection, which are User-specific will not use these credentials.

Understanding the Bug Summary Report

The Bug Summary Report is a high-level summary, sorted by device family, of software bugs that apply to your network.

You cannot view device bug details of devices that are not listed in the Cisco.com Bugtoolkit database. The devices not listed in the Cisco.com Bugtoolkit database are listed in the “Device(s) not supported by Cisco.com Bugtool System” row of the Bug Summary Report.


Note

The Bug Summary Report is categorized based on device type.

The Bug Summary Reports displays the following information.

Column	Description	Usage Notes
Summary		
Total number of submitted devices	Total count of all devices submitted for report generation.	None.
Number of devices with Inventory ¹ data	Count of devices that contain inventory data in the database. You can generate reports for these devices.	None.
Devices without Inventory data	Devices which do not have inventory data in the database. You cannot generate reports for these devices.	None.
Device not supported by Cisco.com Bugtool System	Devices that contain inventory data but do not display a report when the URL is posted to Cisco.com. This may be because Cisco.com does not have data for the device.	None.
Devices timed out	Devices that did not report results because of a connection timeout with Cisco.com.	None.
Bug Toolkit Summary Report		
Device Name	Display name of the device.	None.
Category	Device type of the device.	None.
Image Version	Software version running on a device in your network	None.
Image Status	Status of the image running on the device. The status can be: LD — Latest Deployment ED — Early Deployment GD — Global Deployment	None.
Total Bugs ²	Number of bugs filed against a software release.	Click digit to view all bugs.

Column	Description	Usage Notes
Catastrophic	Number of catastrophic bugs	Click digit to view the list of catastrophic bugs.
Severe	Number of severe bugs	Click digit to view the list of severe bugs.

1. Inventory Data refers to running image filename and image version.
2. The maximum number of bugs displayed for a device is 2500. 2500 is the Bugtoolkit query limit for a device.

Inconsistencies may occur in the number of bugs displayed in the Bug Summary Report archived in the server and the Bug Details Report information on Cisco.com.

Locate Device Report

The Locate Device Report option allows you to search for known bugs that could affect the devices on your network.

To generate a Locate Device report:

-
- Step 1** Select **RME > Reports > Report Generator**.
The Report Generator dialog box appears.
- Step 2** Select **Bug Toolkit** from the Select an Application drop down list box.
- Step 3** Select **Locate Device Report** from the Select a Report drop down list box.
- Step 4** Enter the information required to generate a report:

Field	Description	Usage Notes
Bugs Input		
Enter bugs separated by commas	Bug IDs of known problems separated by commas.	Enter the Bug ID. You can enter multiple bug ID with comma separators.
Upload bug list from file	File that contains the list of Bug IDs. The file extension can be anything, but the file should contain the comma separated or space separated or line separated bug list.	<ol style="list-style-type: none"> Click Browse. The External Config Selector dialog box appears. Enter the following information: File—Location of the file. For example, D:/CSCOp Directory content—Name of the directory. For example, \bin Drive—Name of the drive. For example, D:\

Field	Description	Usage Notes
Scheduling		
Run Type	Schedules the job to run immediately or in the future.	<p>You can specify when you want to run the job. To do this, select one of these options from the drop down menu:</p> <ul style="list-style-type: none"> • Immediate—Runs the report immediately. • 6- hourly—Runs the report every 6 hours, starting from the specified time. • 12- hourly—Runs the report every 12 hours, starting from the specified time. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified time. • Weekly—Runs weekly on the day of the week and at the specified time. • Monthly—Runs monthly on the day of the month and at the specified time. <p>For periodic jobs, the subsequent instances of jobs will run only after the earlier instance of the job is complete.</p> <p>For example, if you have scheduled a daily job at 10:00 a.m. on November 1, the next instance of this job will run at 10:00 a.m. on November 2, only if the earlier instance of the November 1 job has completed.</p> <p>If the 10.00 a.m. November 1 job has not completed before 10:00 a.m. November 2, the next job will start only at 10:00 a.m. on November 3.</p>
Date	Date on which you want to run the job.	<p>Click on the calendar icon and select the start date.</p> <p>If Run Type is Immediate, the system date is automatically selected.</p>
at	Time when you want to run the job in the future.	<p>Select the hours and minutes from the drop-down lists.</p> <p>If Run Type is Immediate, the system time is automatically selected.</p>

Locate Device Report

Field	Description	Usage Notes
Job Info		
Job Description	Enter job description.	Enter a unique description for each job so that you can easily identify jobs.
E-mail	Allows you to enter the e-mail addresses to which the job will send status notices. Separate multiple addresses with commas.	E-mail notification is sent when job is created, started, deleted, canceled, and completed.
Cisco.com Profile		
User Name	Cisco.com user name.	Enter your Cisco.com login ID.
Password	Cisco.com password.	Enter your Cisco.com password.
Proxy Username	Proxy Username	Enter the Proxy Username
Proxy Password	Proxy Password	Enter the Proxy Password. You are prompted to enter your Proxy Username and Proxy Password only if a Proxy Server hostname/IP and port are configured in: Common Services > Security > Cisco.com Connection Management Proxy Server Setup

The Cisco Username, Cisco Password, Proxy Username and Proxy Password textboxes will be auto-populated while scheduling a Bugtool Kit report job, if the Username and Password is already provided under:

Common Services > Server > Security > Cisco.com Connection Management > Cisco.com User Account Setup

However, you can still change the credentials while generating the report.

Step 5 Click **Finish**.

Understanding the Locate Device Report

The locate device report contains the following information:

Column	Description	Usage Notes
Summary		
Devices with Inventory ¹ Data	Devices that contain inventory data in the database. Reports can be generated for these devices.	None.
Devices without Inventory Data	Devices which do not have inventory data in the database. Reports cannot be generated for these devices.	None.
Affected Device Report		
Bug ID	Bug identification number	None.
Affected Devices	Names of the devices affected	None.
Headline	Headline of the bug	Click the headline to view the detailed description of the bug.
Found Version	Software version in which the problem was cited.	None
Fixed Version	Software version in which the problem was resolved.	None
Severity	Severity of the bug	None
Status	State of the bug.	None

1. Inventory Data refers to the image version.

