Cisco Diagnostic Bridge
Installation and User Guide

Version 1.9

January 23, 2020

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS(6387)
Fax: 408 527-0883

Table of Contents

About the Cisco Diagnostic Bridge

The Cisco Diagnostic Bridge is software that can be installed in the customer network to provide device-level diagnostics of the network. It provides periodic automated scanning and problem detection for multiple network devices at the same time.

The bridge leverages digitized Intellectual Capital from Cisco's Technical Assistance Center (TAC) to provide device analysis. Cisco technical experts are constantly developing, expanding and refreshing the library of intellectual capital based on thousands of customer cases they help resolve every day.

The Cisco Diagnostic Bridge helps to:

- Prevent the impact of device issues on network availability, performance and security
- Reduce the time spent on troubleshooting the devices
- Improve overall efficiency of the customer Network Operations Center (NOC)

This is achieved using three main steps:

1. Integrate with a specific set of network monitoring and management tools to learn about and connect to the network devices in order to run diagnostics.
2. Run periodic automated diagnostics on these devices and correlate the results with digitized Cisco Intellectual Capital, to identify device issues and recommended remediation.
3. Return diagnostic results and recommended remediation to customers via the My Diagnostics user interface or through infusion of these results directly into the customer's Incident Management System via API.

Features include:

- Device Diagnostics: Utilizes Cisco TAC knowledge to analyze and detect device activities on the network.
- Data Sources: Allows the Diagnostic Bridge to integrate with multiple network management systems (NMS). You can add devices from these data sources.
- Scan Schedule: Allows you to schedule a scan on the devices daily or weekly.
- Notification Profiles: Allows you to configure notifications from the Diagnostic Bridge that are communicated outward to an existing ticketing system or email. You can add and manage notification profiles.

Note: You must have a valid Cisco.com account in order to use the Cisco Diagnostic Bridge Interface. If you do not have a valid Cisco.com account, you must register on the Cisco.com Registration page and associate a Service Contract to your Cisco.com profile.

Cisco will provide customers with specific instructions for onboarding via email after you have signed up.

Supported Technologies

The Cisco Diagnostic Bridge supports these technologies:

Scanning Devices

- ASA
- IOS
- IOS-XE
- IOS-XR
- NX-OS
- StarOS
- Wireless LAN Controller

Opening Investigations

- ACI
- CUCM
- UCCE
- UCS

Supported Browsers

Supported browsers include:

- Google Chrome
- Mozilla Firefox
- Apple Safari

Connected TAC

Connected TAC allows customers to leverage digitized Intellectual Capital and expertise from the Cisco Technical Assistance Center (TAC). It enables:

- Automated and proactive problem detection
- Faster resolution through remediation recommendations for the identified problems
- The infusion of diagnostic results directly into the most commonly used incident management systems
- Assistance from TAC to manage and resolve issues that are proactively identified and support new technologies

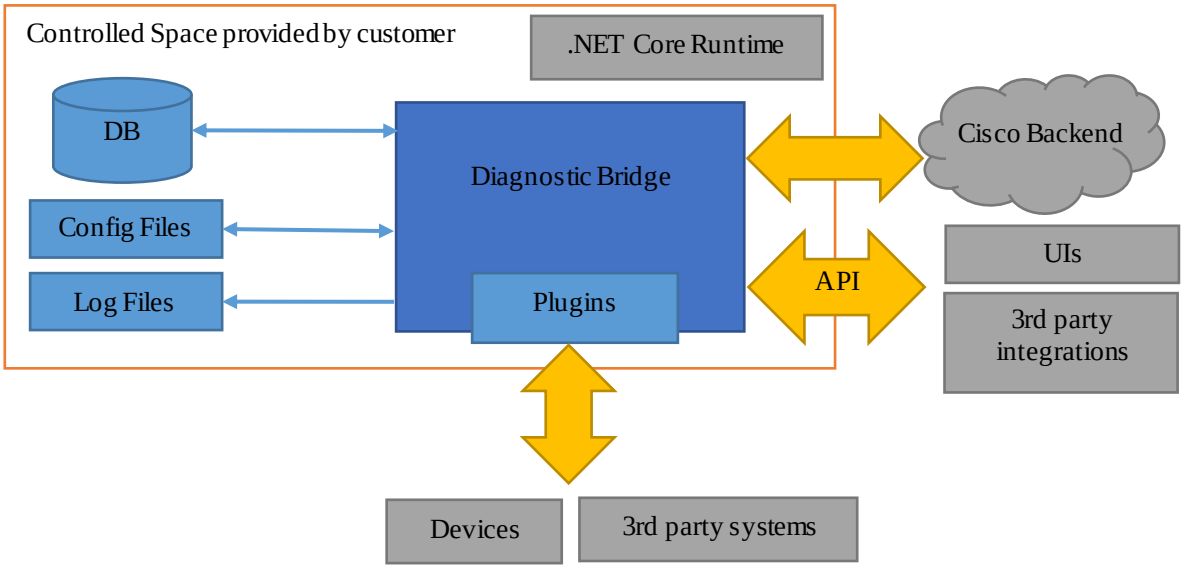
The Market Trial Components include:

- CLI Analyzer - Device Diagnostics based on digitized Intellectual Capital from Cisco TAC. Use your CCO credentials to log in.
- TAC Advisor - TAC engineer led device analysis
- Cisco Diagnostic Bridge - Automated device diagnostics for multiple devices in a network
- My Diagnostic User Interface - Provides the visualization of device history, events and configuration of Cisco Diagnostic Bridge

Customer Responsibility

NOTE: **As of version 1.9**, Cisco no longer provides an OVA that contains both the Diagnostic Bridge and the database. Customers who have an existing Cisco-provided OVA can continue to use that to host the Diagnostic Bridge and database. However, it is the customer's responsibility to keep the operating system and the database on the OVA up to date.

In the diagram below, the orange box is the "Controlled Space," the environment in which the Diagnostic Bridge runs. Typically, this is a general purpose computer or a virtual environment.



Within the Controlled Space, only authorized users should have these permissions:

- File level access to the Diagnostic Bridge binary, configuration, and log files
- Access to the Diagnostic Bridge database (whether locally, remotely, or through file storage access)
- Access to the Diagnostic Bridge or database server memory space
- Execution of arbitrary commands and software

Additionally, Customer is responsible to back up critical data such as databases and configuration files as needed.

Installation

Cisco Diagnostic Bridge Installation includes an MSI installation for Microsoft Windows servers. Manual binary deployment is also an option.

Verify Prerequisites

Software requirements:

- Microsoft Windows 7 and higher
- MySQL 5.7, Microsoft SQL Server, or PostgreSQL
- Microsoft .NET Core 2.1.10 Runtime (or a later version of the 2.1.x branch)

Network requirements:

- By default, the Diagnostic Bridge listens on port 5001. It is mandatory to configure any firewall software to allow access to this port.
- In order to establish an outbound connection for Device Analyzer, your firewall must allow a TCP connection on port 443 to these sites:
  - api.cisco.com,
  - cway.cisco.com
  - cloudsso.cisco.com
  - cloudsso2.cisco.com
  - identity.cisco.com

Note: If you intend to use WhatsUp Gold as a Data Source for the Cisco Diagnostic Bridge, the bridge and WhatsUp Gold must be installed on the same machine. Cisco Diagnostic Bridge supports WUG 2016 and 2017.

Install the SQL Database and .NET Runtime

Before you install the Diagnostic Bridge, the SQL database and .NET must be installed.

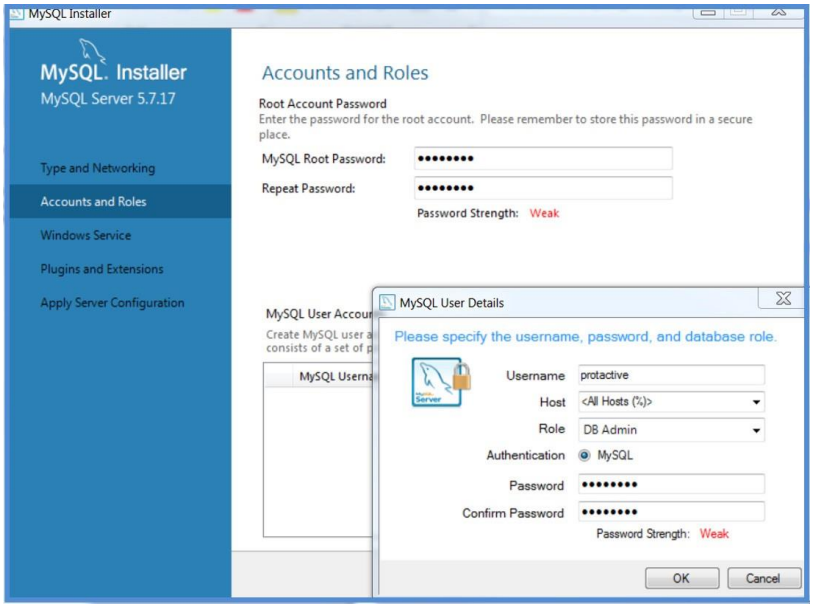
The Diagnostic Bridge is compatible with MySQL 5.7, Microsoft SQL Server, and PostgreSQL. This section illustrates the installation of a database that uses MySQL.

In order to use MySQL to install a SQL database for the Diagnostic Bridge, perform the steps in this section.

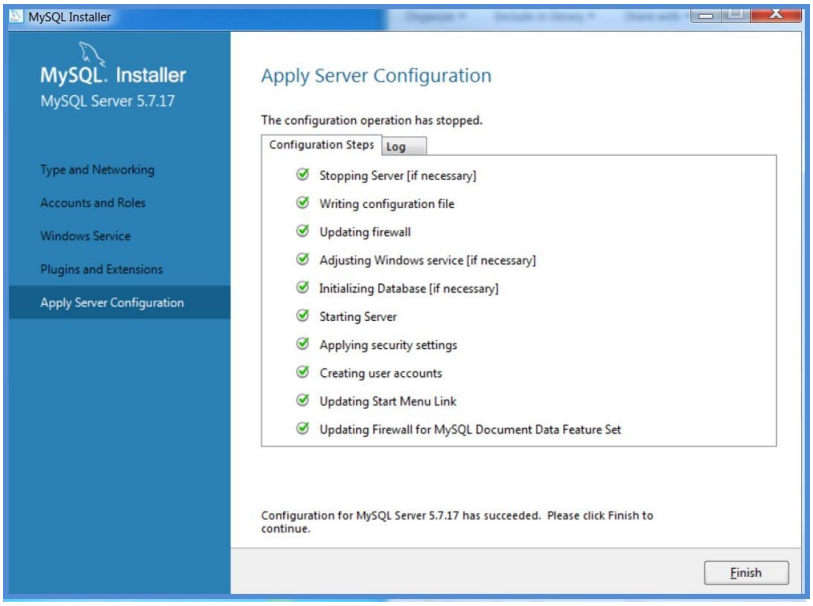
1. Download the MySQL installer from https://dev.mysql.com/downloads/installer/
2. Install MySQL with this configuration:

   – Server only

   – Remember the password that you enter; it will be configured on the Diagnostic Bridge in a future step.



– Retain default settings.



3. Download .NET Core 2.1.10 (or later version of the 2.1.x branch) from:

   https://www.microsoft.com/net/download/core#/runtime/current

Note: For Windows 7 and 2008 only, make sure that your Windows installation is up-to-date and includes hotfix KB2533623 installed through Windows Update.

4. Add this path in Windows for C:/Program Files/dotnet:

   run : Advanced System Settings > Advanced > Environment Variables > Path > Edit : C:\Program Files\dotnet > OK

Install the Diagnostic Bridge

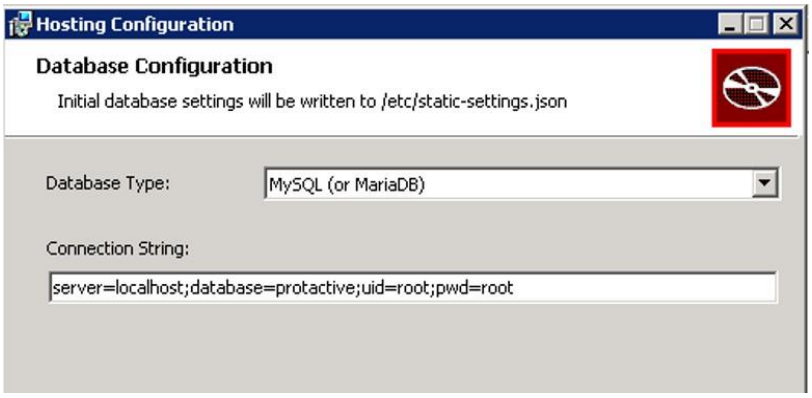
Two installation methods are available:

- MSI installer
- Binary deployment

MSI Installer

In order to use the MSI installer method to install the Diagnostic Bridge, perform these steps.

1. Download the latest MSI installer of the Diagnostic Bridge. Start the setup and follow the instructions on the wizard screens.
   a. Click **Next** in order to continue past the Welcome screen.
   b. Optionally, change the destination folder. Click **Next** in order to continue.
   c. Select whether to use HTTP or HTTPS, enter the required information, and click **Next**.
   d. Review the database settings. Change the user id and password in the connection string as required to match your SQL DB settings. Click **Next** in order to continue.



   e. When you are prompted to do so, create a self-signed security certificate. The certificate name ***must*** be a Fully Qualified Domain Name, not an arbitrary string.
   f. Click **Install** in order to start the installation. Wait for the installation process to complete.
   g. Click **Finish** in order to close the installation wizard.
2. After successful installation, the Cisco Diagnostic Bridge starts as a Windows service.
   – Link: *https://<your IP address>:5001/home*

Note: The MSI installation prompts you to enter the port number and user credentials. It is recommended to change the default credentials. You can use the link (*https://<your IP address>:5001/home*) for debugging purposes.

Binary Deployment

In order to use the binary deployment method to install the Diagnostic Bridge, perform these steps.

1. Download the latest compressed package (.zip) of the Diagnostic Bridge.
2. Extract the .zip file contents to a temporary folder of your choice on the system's local drive.
3. Open a command prompt window and change the directory to the folder that contains the extracted files.

4. Run this command:

   ```
   dotnet CiscoProTACtiveService.dll setup
   ```

   The setup wizard opens.

5. Follow the prompts on each page of the wizard in order to complete the initial configuration process.
   - When you are asked, choose the option to install the Diagnostic Bridge as a Windows service.
   - When you are prompted to do so, create a self-signed security certificate. The certificate name ***must*** be a Fully Qualified Domain Name, not an arbitrary string.

6. After installation and setup are complete, close the wizard.

   The list of Windows services should now show the Diagnostic Bridge as an active service.

   If the Diagnostic Bridge service stops and it is necessary to start it manually, open a command prompt window, change directory to `C:\Program Files (x86)\Cisco\DiagnosticBridge\bin`, and enter this command:

   ```
   dotnet CiscoProTACtiveService.dll run
   ```

Post Installation Setup

After you install the SQL database and Diagnostic Bridge, perform these tasks:

- Accept the Security Certificate as Trusted
- Configure Outbound Connections
- Upgrade the Diagnostic Bridge

Important Notes:

- If you elected to use the self-signed security certificate that is installed by default, when you access the Diagnostic Bridge via HTTPS for the first time, you must accept the certificate for secured connection between the Diagnostic Bridge and the My Diagnostic Interface.
- The security certificate uses your organization's private IP address. Network Address Translation (NAT) cannot be used for this purpose.
- The Diagnostic Bridge does not have direct communication to Cisco's My Diagnostic Interface. It needs a web browser on the client PC in order to manage the Diagnostic Bridge. All the communication to port 5001 goes through the client PC that connects to My Diagnostics.

Accept the Security Certificate as Trusted

During installation, you created a self-signed security certificate. In order to accept the certificate as trusted, perform these steps:

1. In an Internet browser, open a web connection to your Diagnostic Bridge:

   https://<your IP address>:5001

2. If a security certificate error message appears in the browser, accept the message and continue.
   - Chrome: Click **Advanced** and then click the link to proceed to the URL of your Diagnostic Bridge.
   - Firefox: Click the **Advanced** button and then click **Add Exception**.

3. Refresh the My Diagnostics web page in order to confirm that the security certificate error is resolved.

You can now access the My Diagnostics Interface (https://cway.cisco.com/mydiagnostics) with the self-signed certificate.

Note: You must accept the certificate in order to allow the My Diagnostics UI to communicate with your bridge.

You can also use the Diagnostic Bridge URL (*https://<your IP address>:5001/home*) for debugging purposes.

Configure Outbound Connections

Use the Outbound Connections settings in the Local UI to configure advanced settings for outbound connections from the bridge to Cisco or to a third-party system. Examples of advanced settings include the use of a proxy server or the acceptance of a self-signed certificate.

In the Outbound Connections settings, you can specify a list of configuration entries. For every outbound connection, the first entry with a matching HostSelector is used.

Each configuration entry can include these fields:

- **HostSelector (required):** If the host portion of an outgoing URL contains this string, there is a match. The string is not case-sensitive. If the string is "*", it matches all outgoing URLs.
- **LoggingDirectory:** HTTP logs are written to the directory in this field. It is recommended that you only include this field in order to troubleshoot an issue.
- **AllowInvalidCertificate:** If set to "true", no certificate validation is performed for URLs that match the HostSelector string. This field must be set to "true" in order to support self-signed certificates.
- **ProxyAddress:** The full address, including scheme and port, of the proxy to use for URLs that match the HostSelector string.

  Note: If the **ProxyAddress** field is set, then these additional parameters are required: **ProxyUseDefaultCredentials** (Boolean), **ProxyUsername**, **ProxyPassword**, and **ProxyCredentialDomain**.

  Note: ProxyAddress only supports http proxy. Outbound HTTPS connections are supported using HTTP proxy.

Upgrade the Diagnostic Bridge

There are two ways to upgrade:

- Use the My Diagnostic Interface
- Manually copy the new version in place

Upgrade with the My Diagnostic Interface

In order to upgrade with the My Diagnostic Bridge Interface, click the **Update** button. Refer to this figure:

Upgrade Manually

In order to upgrade manually, replace the current 'bin' folder with the contents of the update ZIP:

1. Obtain the latest ZIP and download it to the Diagnostic Bridge:

- https://cway.cisco.com/apps/mydiagnostics/v**X.Y.Z**/v**X.Y.Z**.zip

  Replace X.Y.Z with the desired version number (example: 1.5.2)

2. Stop the 'Cisco Diagnostic Bridge` in Windows Services manager.
3. Optionally, rename the Diagnostic Bridge 'bin' folder to keep a backup.

   `C:\Program Files (x86)\Cisco\DiagnosticBridge\bin\`
4. Replace the 'bin' folder with the contents of the download ZIP.

Note: It is recommended that you keep previous versions in order to revert back if you face any issues. The previous configuration settings are retained after upgrade.

Configure Application Settings

Use this URL in order to access My Diagnostics:

https://cway.cisco.com/mydiagnostics

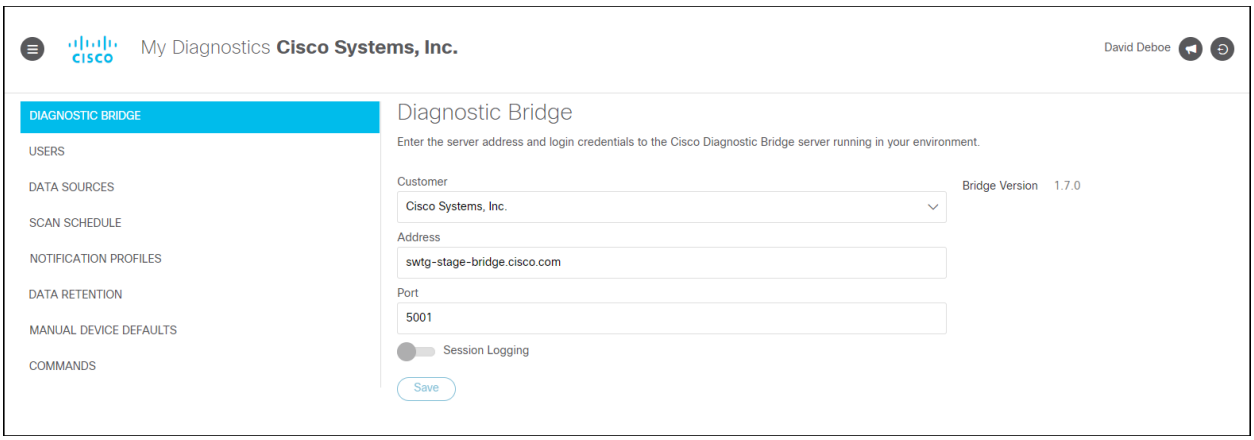
The first time you open My Diagnostics, the interface opens with the Settings page displayed. Select a customer and enter the address and port of the Diagnostic Bridge and click **Save**. This will enable the remaining options on the Settings page so that you can configure the settings.

It is recommended that you configure the remaining settings in this order:

1. Notification Profiles
2. Data Sources
3. Scan Schedule
4. Manual Device Defaults
5. Users

Diagnostic Bridge

Select a customer from the drop-down list in the Customer field. Enter the address and port of the Diagnostic Bridge and click **Save**.



Optionally, select the **Session Logging** toggle switch in order to turn session logs on or off. Normally, this feature should be turned on only temporarily, in order to help troubleshoot the application.

Notification Profiles

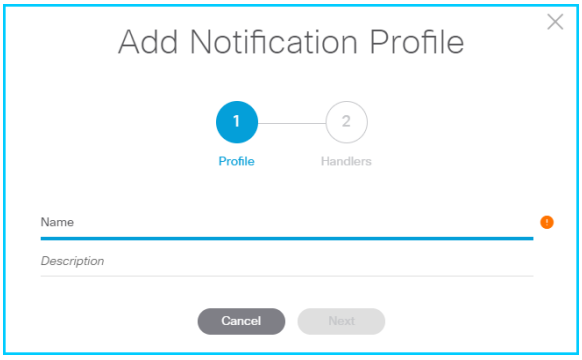
You can add and manage Notification Profiles in order to control email and event notifications for device check activities.

When the devices in the network are scanned and checked for alerts, the notification profiles help to notify customers about the events happening on the network devices via SMTP or ServiceNow plugins.

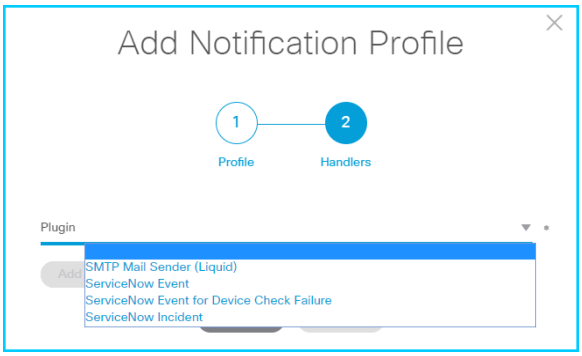
If you use ServiceNow to manage your network, you can configure the ServiceNow notification profile to integrate with the workflow of your ticket or incident management system.

Perform these steps in order to add a notification profile:

1. Click **Add**. The Add Notification Profile window appears.



2. Complete the required fields:
   - **Name:** Enter a name for the Notification Profile.
   - **Description:** Enter a description for the Notification Profile.
3. Click **Next**.



4. Complete the required fields:
   - **Plugin:** Choose the plugin for the Notification Profile.
   - **Plugin Type:** Choose the type of notification template.

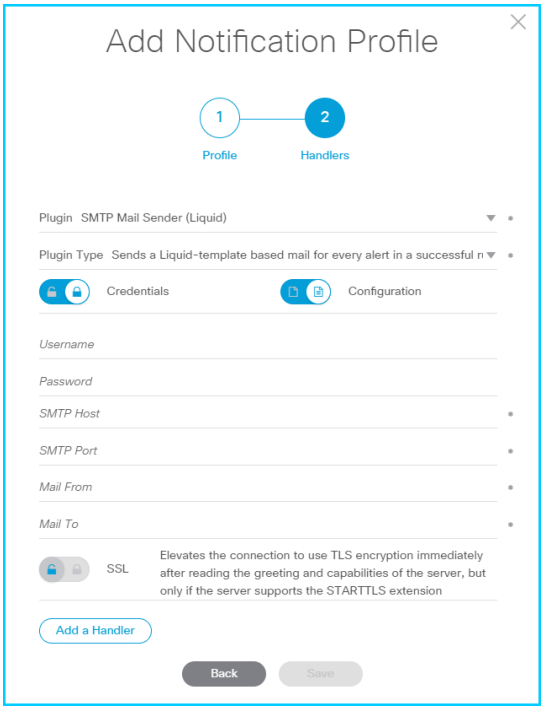
Note: The Plugin Type option appears on selecting the Plugin from the drop-down list.

5. Click **Save**.

The sections that follow describe the supported notification plugins.

SMTP Mail Sender

The SMTP Mail Sender allows you to configure email notifications for device checks. Choose this option in order to configure email notifications for alerts with a successful run, when a device or a group of devices are scanned and any changes in the state of issues. Configure user credentials and the SMTP Server when you add SMTP Mail Sender Notification Profiles.



- **Credentials:** Click the toggle button in order to provision login credentials or view credentials that you previously entered. When enabled, login credentials for each session tab persist until the session tab is closed. Enter the credentials (Username and Password) to login to the email system.
- **Configuration:** Click the toggle button in order to provision SMTP server details or view a configuration that you previously entered. When enabled, login credentials and server details for each session tab persist until the session tab is closed.

  – **SMTP Host:** Enter the outgoing mail server IP address.

  – **SMTP Port 25:** The standard SMTP port used to send out emails is port 25. To select any other port, use the up and down arrows.

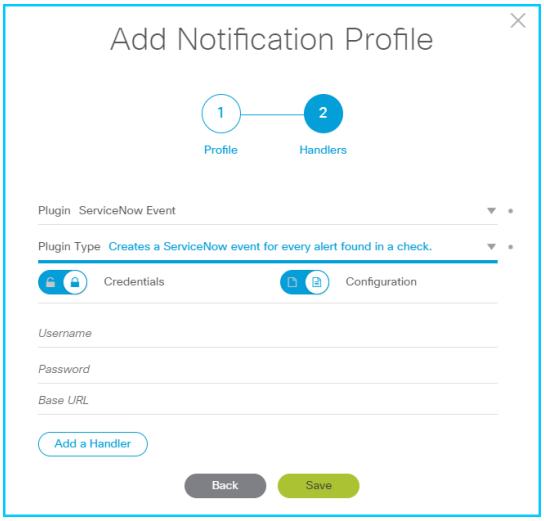
  – **Mail From:** Enter email address of the sender such as the Cisco bridge (ciscobridge@company.com).

  – **Mail To:** Enter email address of the receiver such as individual email/email alias used to create a case in Incident Management or Remedy.

  – **SSL:** Click the toggle button in order to enable or disable. This setting elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server, but only if the server supports the STARTTLS extension.
- **Add a Handler:** Click this button in order to add another handler to the notification profile.

ServiceNow Event

You can configure event notifications for every alert found during device check and when there is a change in the state of issues. This allows you to integrate with the customer's incident/ticket management system.



- **Credentials:** Click the toggle button in order to provision login credentials or view credentials that you previously entered. When enabled, login credentials for each session tab persist until the session tab is closed. Enter the credentials (Username and Password) to login to the ServiceNow at the customer's network.
- **Configuration:** Click the toggle button in order to provision SMTP server details or view a configuration that you previously entered. When enabled, login credentials and server details for each session tab persist until the session tab is closed.
  - **Base URL:** Enter the URL that is used to communicate with ServiceNow in order to accept the events received by the Customer.
- **Add a Handler:** Click this button in order to add another handler to the notification profile.

Data Sources

Data sources provide ways for the Cisco Diagnostic Bridge to learn the Cisco devices in your network. The data sources that can be added are:

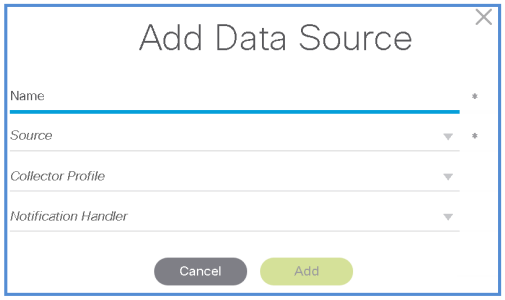
- Cisco CSP Collector
- Cisco PI
- General External Source
- ServiceNow
- WhatsUp Gold Group

You can use the synchronize option, available on the Devices page, in order to refresh the device list from the Data Source. The bridge will communicate to the Data Source and refresh the device list.

You can add and manage Data Sources using this option. You can select the collector and notification profiles to associate to the devices.

Perform these steps in order to add a data source:

1. Click **Add**. The *Add Data Source* window appears.



2. Enter the **Name** of the data source.
3. In the **Source** field, select the source of device data. Additional fields appear when you select a source.
4. In the **Collector Profile** field, select a profile. All of the profiles that that have been created on the Bridge will appear in the drop-down list.

Note: Collector Profile lets you control the way device information is gathered for Cisco Diagnostic Bridge. Some Data Sources provide their own collection system and do not require a collector profile such as CSPC.

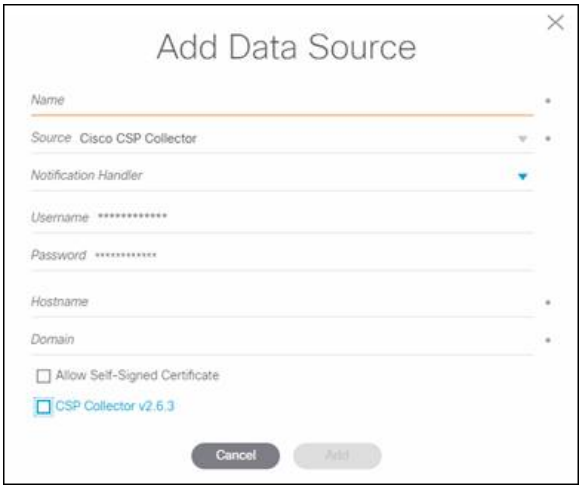
5. In the **Notification Handler** field, select the notification profile. All of the profiles that you have created appear in the drop-down list.
6. Enter source-specific information as required. Refer to the sections that follow for source specific setup.

Cisco CSP Collector

Diagnostic Bridge integration with the Cisco CSP Collector (CSPC) is approved for CSPC version 2.8.1.3 and later. Additionally, CSPC version 2.6.x is no longer supported by Cisco TAC.

When you are ready to add the CSPC as a data source, enter this information on the Add Data Source screen:

- **Notification Handler:** Optionally, select a method to use in order to send analysis results.
- **Hostname:** Enter the IP address of the CSPC.
- **Domain:** Enter the domain used by the customer, such as cisco.com.
- **Allow Self-Signed Certificate:** Check this box if the CSPC uses a self-signed certificate for the secure https connection. If you are using a certificate signed by a trusted Certificate Authority, leave this unchecked.
- **CSP Collector v2.6.3:** Check this box ***only*** if you use version 2.6.3. If version 2.7.2 or later is installed, leave the box unchecked.



Cisco Prime Infrastructure (PI)

Cisco PI must be installed and configured using the REST API before you can add it as a data source.

In order to test whether the diagnostic bridge can receive device information from Cisco PI, use a browser to run an API query manually. Ensure that the query returns the device ID. Also validate the login credentials.

Note: Group NBI Read users are not allowed to log in via a browser, so use the root user.

Direct the browser to **https://<myCiscoPI_ipaddr>/webacs/api/v1/data/Devices**, where **<myCiscoPI_ipaddr>** is the IP address of the Cisco PI.

Next, run a detailed query that uses the device ID from the previous API query. Do this for each device.

Direct the browser to **https://<myCiscoPI_ipaddr>/webacs/api/v1/data/Devices/<myDevice_ID>**, where **<myCiscoPI_ipaddr>** is the IP address of the Cisco PI and **<myDevice_ID>** is the ID of the device.

When you are ready to add the Cisco PI as a data source, enter this information on the Add Data Source screen:

- **Collector Profile:** Select a profile. Long Poll Collector uses the diagnostic bridge API in order to provide device information from a system integration. SSH CLI Collector uses SSH in order to collect device information directly; you must configure local SSH credentials and enable the password.
- **Notification Handler:** Optionally, select a method to use in order to send analysis results.
- **Username:** Enter a user account that is configured on the Cisco PI. The account must have access to the Cisco PI REST API (such as an account to which the **Group NBI Read** is assigned).
- **Password:** Enter the password for the user account.
- **URL:** Enter the HTTPS URL for the Cisco PI.
- **Allow Self-Signed Certificate:** Check this box if Cisco PI uses a self-signed certificate for the secure https connection. If you are using a certificate signed by a trusted Certificate Authority, leave this unchecked.

General External Source

System integration is possible through use of the Diagnostic Bridge API.

By default, the diagnostic bridge uses a self-signed certificate. You can use a browser in order to validate the certificate; if a security warning appears, accept the certificate.

In order to check the diagnostic bridge API functionality, direct a browser to:

https://<diagnosticBridgeIP>:5001/swagger

...where <diagnosticBridgeIP> is the IP address of the bridge.

When you are ready to add a general external source as a data source, enter this information on the Add Data Source screen:

- **Collector Profile:** Select a profile. Long Poll Collector uses the diagnostic bridge API in order to provide device information from a system integration. SSH CLI Collector uses SSH in order to collect device information directly; you must configure local SSH credentials and enable the password.
- **Notification Handler:** Optionally, select a method to use in order to send analysis results.

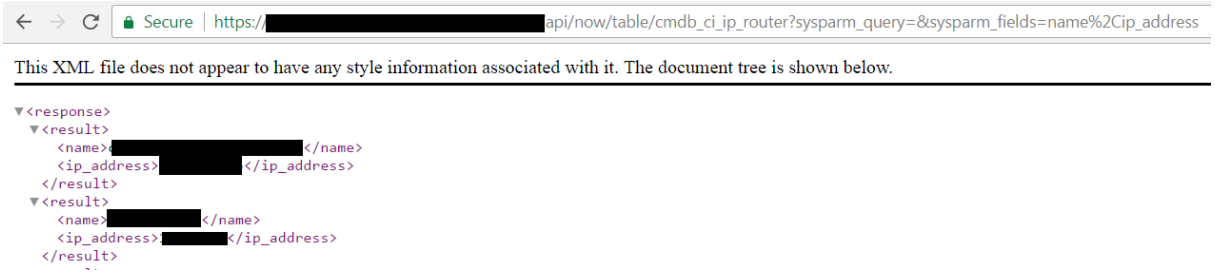
Service Now

You must have an active ServiceNow contract and user credentials in order to access your ServiceNow instance.

In order to test whether the diagnostic bridge can receive device information from ServiceNow, use a browser to run an API query manually. Ensure that the query returns the **name** and **ip_address** fields. Direct the browser to:

https://<myorganization>.service-now.com/api/now/table/cmdb_ci_ip_router
?sysparm_query=&sysparm_fields=name%2Cip_address

...where **<myorganization>** is the name of your organization that is used for your ServiceNow contract.



When you are ready to add ServiceNow as a data source, enter this information on the Add Data Source screen:

- **Collector Profile:** Select a profile. Long Poll Collector uses the diagnostic bridge API in order to provide device information from a system integration. SSH CLI Collector uses SSH in order to collect device information directly; you must configure local SSH credentials and enable the password.
- **Notification Handler:** Optionally, select a method to use in order to send analysis results.
- **Username:** Enter a user account with access to ServiceNow.
- **Password:** Enter the password for the user account.
- **URL:** Enter https://<myorganization>.service-now.com.
- **Allow Self-Signed Certificate:** Check this box; it is required in case ServiceNow uses a self-signed certificate for the secure https connection. You can use a browser in order to validate the certificate; if a security warning appears, accept the certificate.

WhatsUp Gold Group

WhatUp Gold (WUG) 2016 or 2017 can be used as a data source. Ensure that WUG is installed and configured.

Note: The diagnostic bridge ***must be installed on the same server*** as WUG. A WUG DLL (installed with the Diagnostic Bridge) requires direct access to the WUG system.

When you are ready to add a WhatsUp Gold Group as a data source, enter this information on the Add Data Source screen:

- **Collector Profile:** Select a profile. Long Poll Collector uses the diagnostic bridge API in order to provide device information from a system integration. SSH CLI Collector uses SSH in order to collect device information directly; you must configure local SSH credentials and enable the password.
- **Notification Handler:** Optionally, select a method to use in order to send analysis results.
- **Device Group:** Select the device group from which you want to collect device information.
- **Connection String:** Enter the connection string that tells the diagnostic bridge how to access WUG device information through the device group. The default connection string is:

  Data Source=localhost\WHATSUP; Initial Catalog=WhatsUp;Integrated Security=True

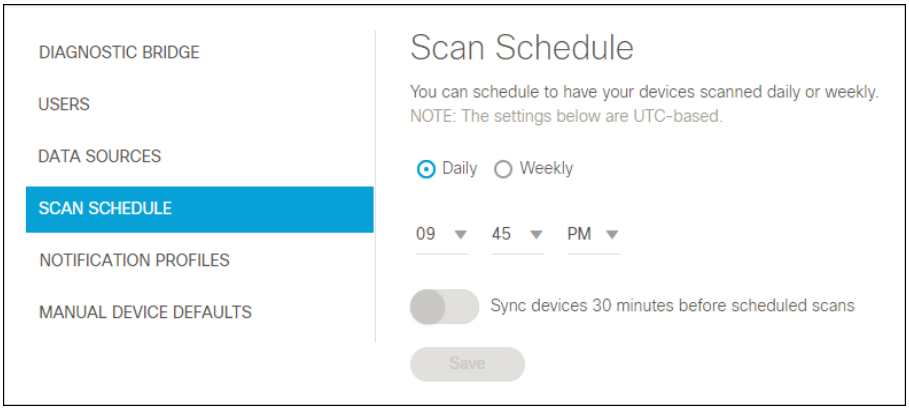
  Depending on your WUG database installation, you might need to change the string from the default.

Note: WhatsUp Gold has developed a DLL that allows secure communication between WUG and the diagnostic bridge. This DLL will send access credentials to the diagnostic bridge for access to collect direct SSH device information. You can still configure local SSH credentials and enable passwords as a fallback measure.

Scan Schedule

You can schedule a daily or weekly scan using the Schedule Scan option. Select the day and time to run device scans. The scan scheduled in this screen applies to all the devices that have the scan option enabled.

In order to schedule an automatic scan of devices in the network, choose Daily or Weekly. Use the up and down arrow buttons in order to select the hour, minutes and AM/PM.

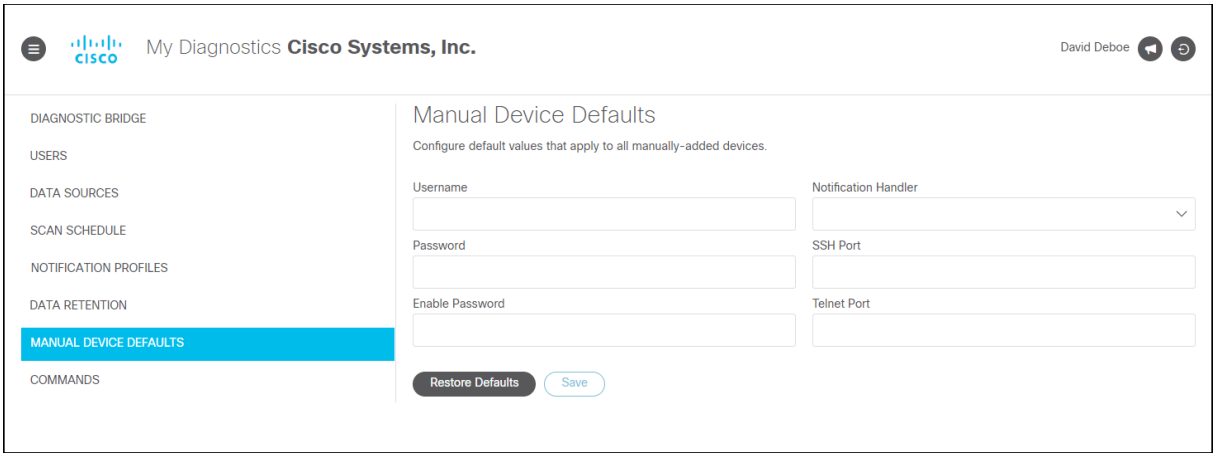


Manual Device Defaults

Set default credentials for devices that are added manually.

Enter the username and password, select the Notification Handler, and enter the port (SSH and/or Telnet).

In order to reset the password, click the **Reset Manual Defaults** button.

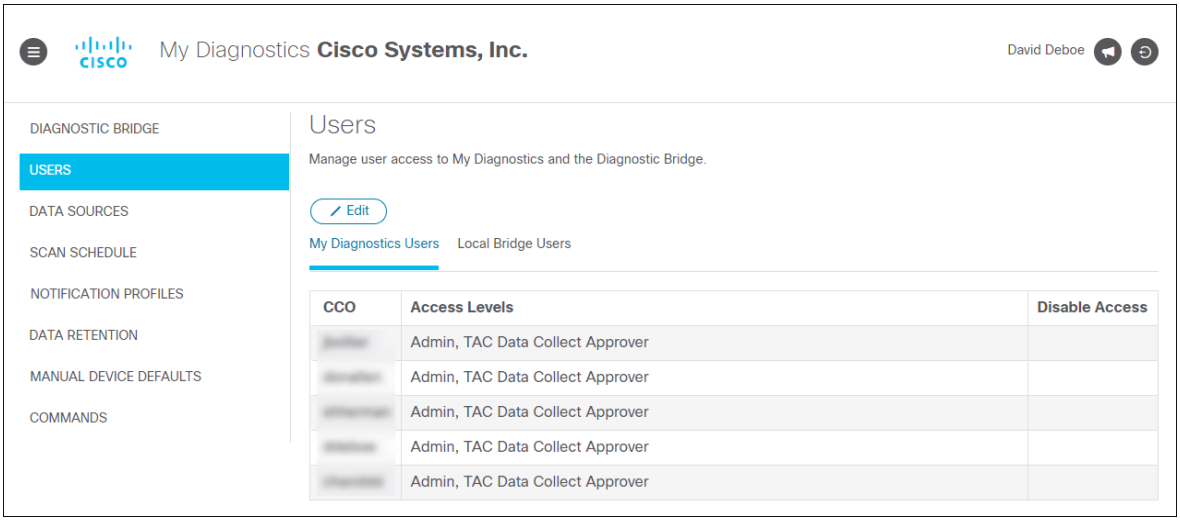


Users

On this tab, you can add and delete user accounts and assign access levels to each account. The tab displays a table of user accounts that shows the login ID and access levels.

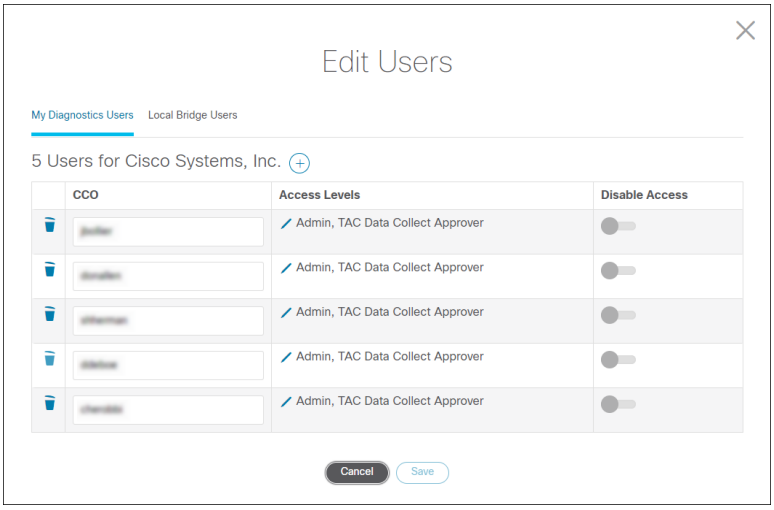
Access levels, or roles, define what functions a user is allowed to perform within the application:

- **Admin:** This access level can add user accounts, configure Diagnostic Bridge settings, and use all program features.
- **Operator:** This access level can perform the operational functions that are required in order to support the Diagnostic Bridge.
- **ReadOnly:** This access level can only view the data that is displayed on the My Diagnostics page.

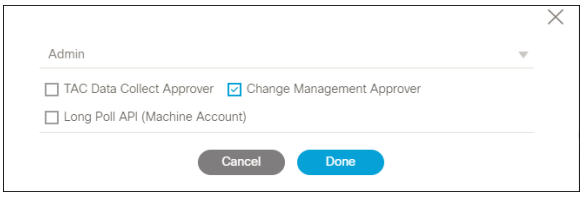


Perform these steps in order to create or modify a user account:

1. Click the **Edit** button. The Edit Users dialog opens and displays a table of user accounts.



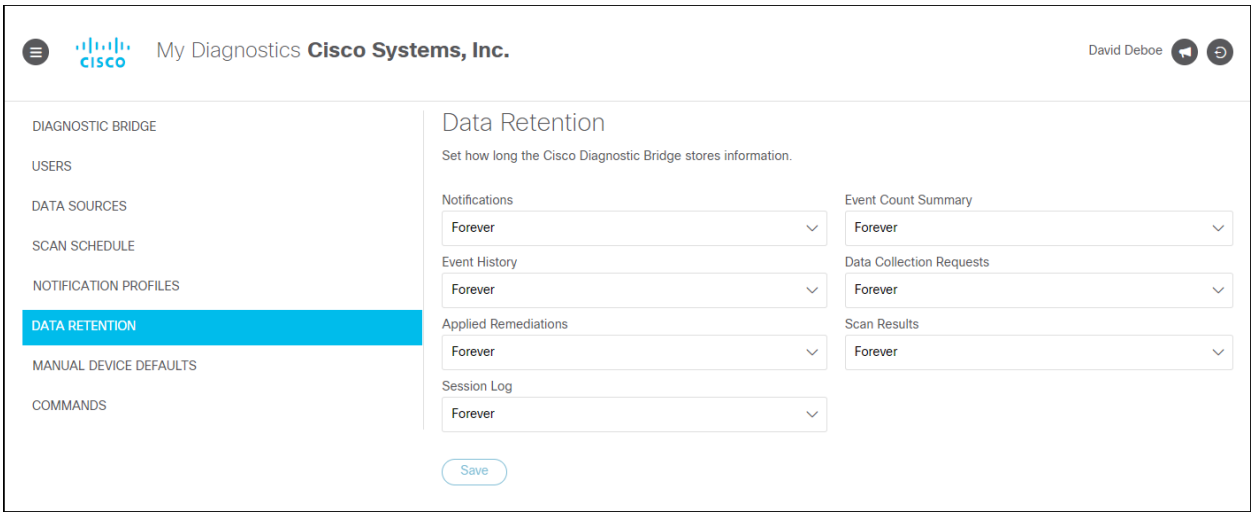
2. In order to add a user account, click the button at the top of the dialog. A new row appears in the table.
   a. Enter the login ID in the CCO column. The application validates the ID automatically.
   b. In order to modify the access levels for a new or existing account, click the Edit button in the Access Levels column. In the dialog that opens, select Read Only, Admin, or Operator from the drop-down list and select the check box beside each additional role that is desired. Click **Done**.



   c. In order to remove an account from My Diagnostics, click the trash can icon beside that account.
   d. In order to disable an account (but not delete it), click the toggle button in the Disable Access column. Click the button a second time in order to re-enable the account.
3. Click **Save** when you are finished.

Data Retention

On this tab, you can set a limit on the amount of time that My Diagnostics stores each information type.

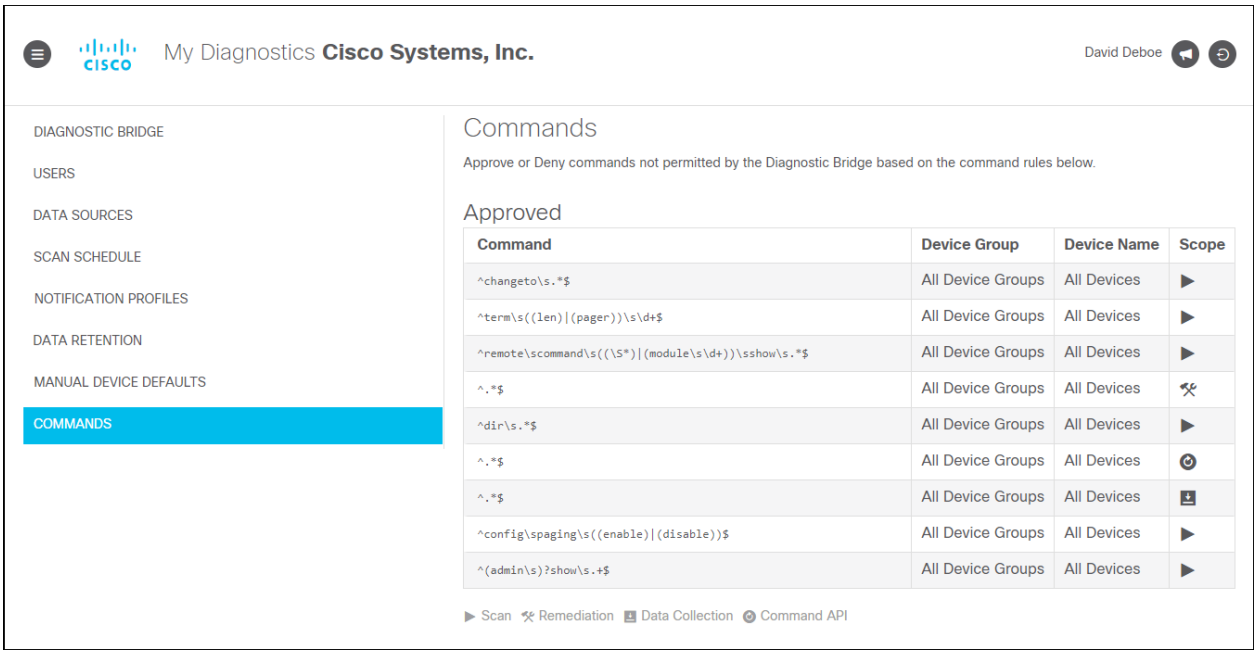


By default, all information is retained forever. If you select a limited period of time, data that is older than the selected age is deleted as soon as you click **Save**, and on a daily basis afterward.

Commands

On this tab, users who have Command Approver permissions can view the list of commands that are not permitted by the Diagnostic Bridge. Users with Command Approver permissions can approve or deny these commands.

The list of commands is not displayed if the viewer does not have Command Approver permissions.



Features

Use this URL in order to access My Diagnostics:

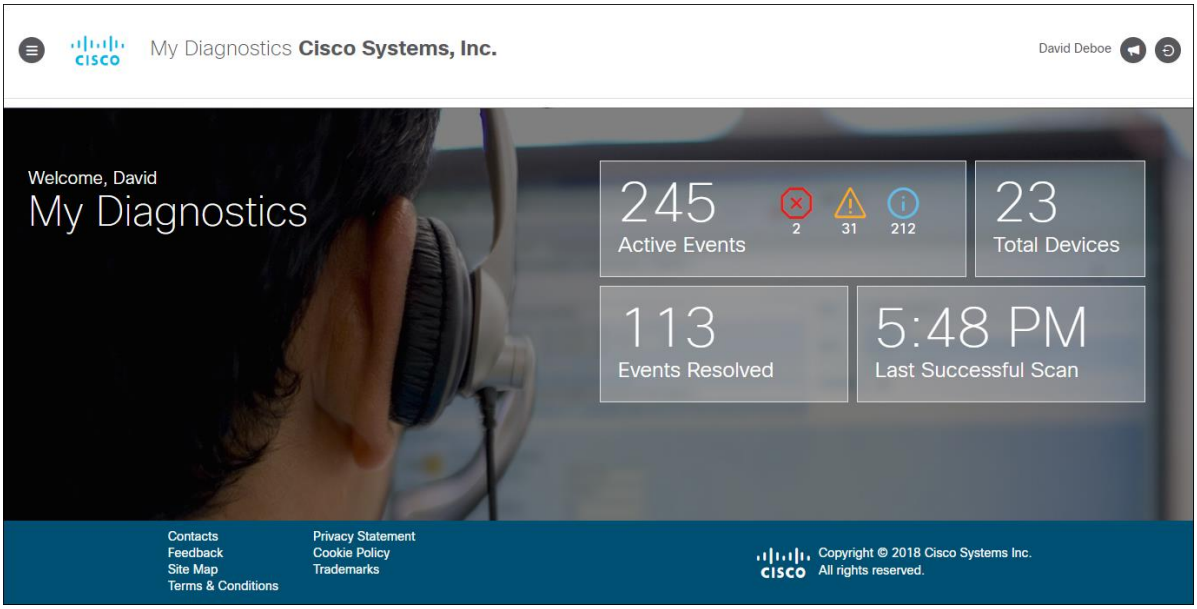
https://cway.cisco.com/mydiagnostics

Enter your Cisco user credentials.

Home Page

The Home page displays the total count of:

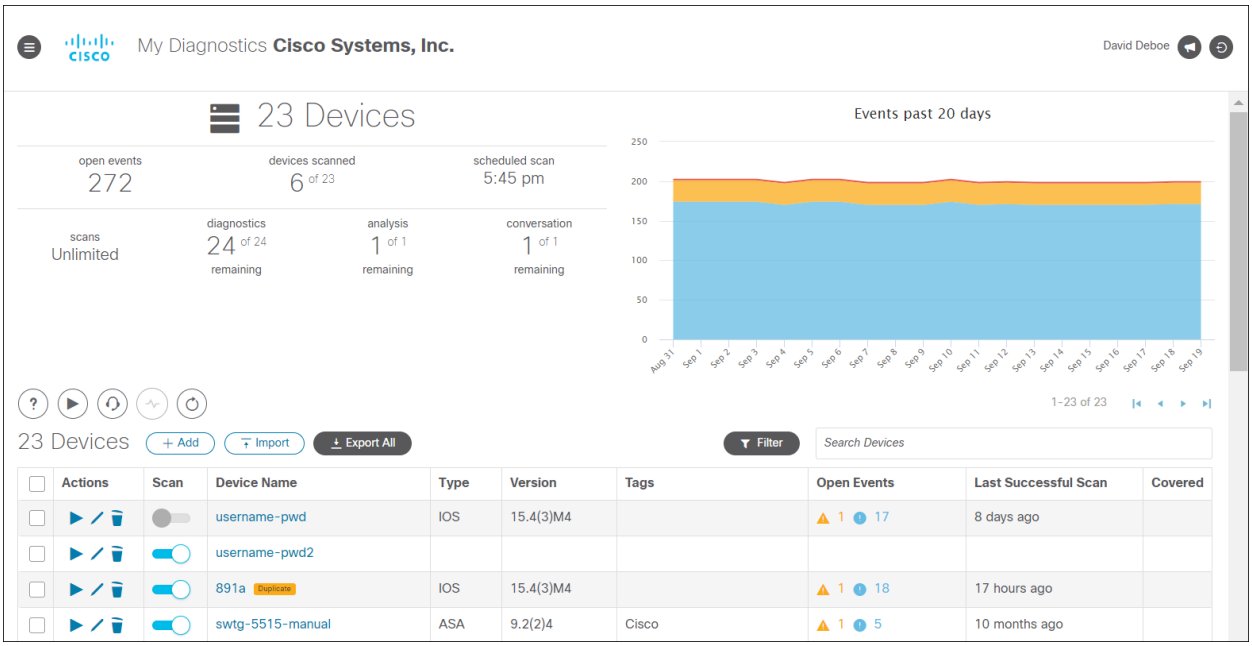
- Open Events, categorized by alert severity (Information, Warning and Danger)
- Total Devices
- Events Resolved



Click the menu button ( ) in the page header in order to show and hide a panel of links to the various pages of My Diagnostics. This menu button is available on every page.

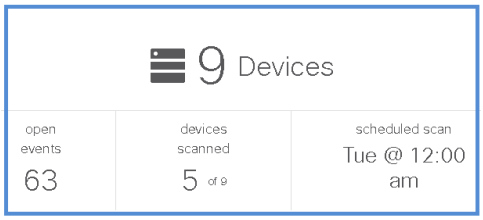
Devices Page

The Devices page allows you to add, delete and manage devices, view event trends, conduct scans, and request investigations.

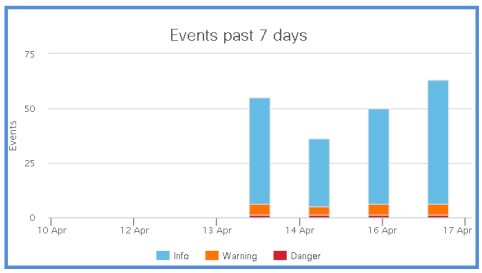


You can perform these actions on the Devices page:

- View the total device count, total number of open events, scanned devices and the scan schedule.

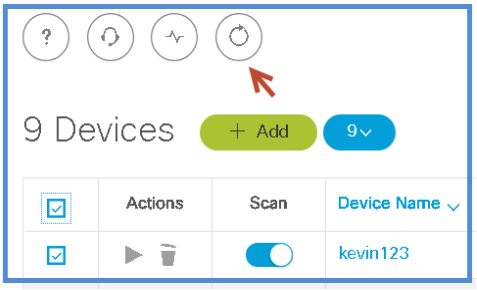


- View the trend of event details, based on severity.

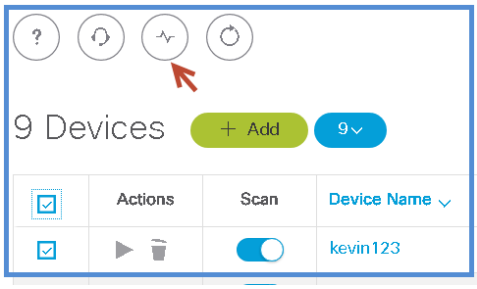


- Type the name of a device in the search box and press Enter in order to search for matching devices.

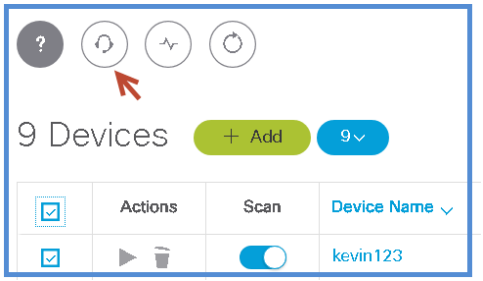
- Synchronize the bridge with external data sources in order to update any new devices to the existing list.



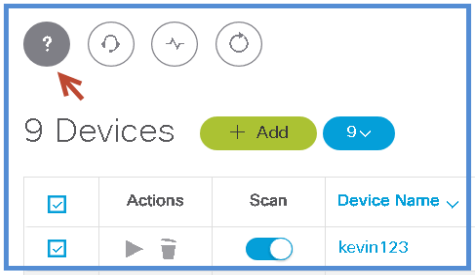
- Open an analysis investigation on the selected device. (Premium service level required.) Refer to Investigate Devices for more details.



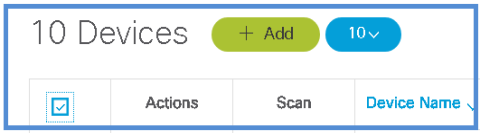
- Open a conversation. You can request a one-hour meeting with a TAC engineer in order to discuss technology, deployment and so on. (Premium service level with TAC Advisor Level 2 required.)



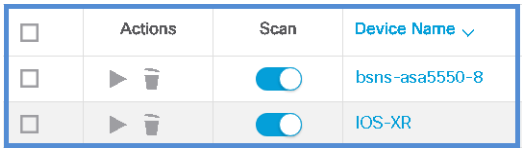
- Request application support or submit feedback.



- Add devices manually. The selected device count appears on top of the device list table. Refer to Add Devices Manually for more details.



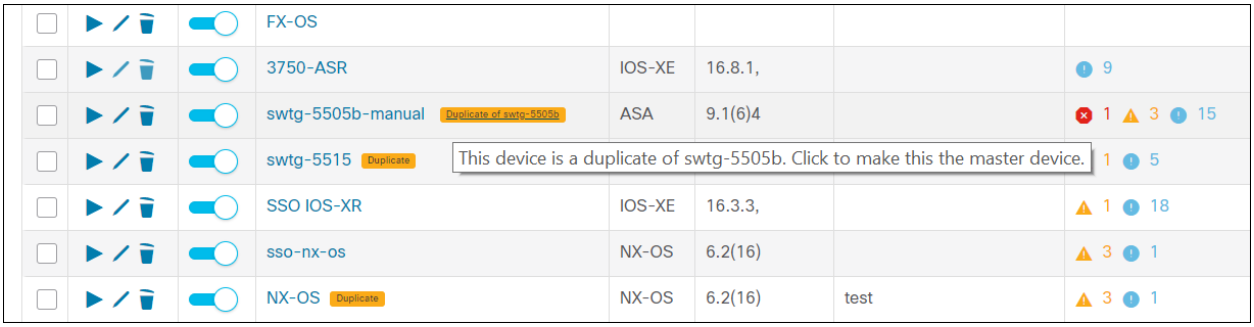
- Import devices from a CSV file. Refer to Import Devices for more details.
- Click the Play icon in order to begin a manual device scan. (Enhanced service level required.)
- Click the Pencil icon in order to edit information or tags for a device that was added manually.
- Click the Trash icon in order to delete a device that was added manually.
- Click the toggle button in the Scan column in order to enable or disable the scheduled scan for a device.



Duplicate Devices

Some devices in the Devices list might be duplicate entries of another device, based on serial number. The label "Duplicate" beside a device name indicates that it is a duplicate. When there are duplicate entries for a single device, one entry is regarded as the master device.

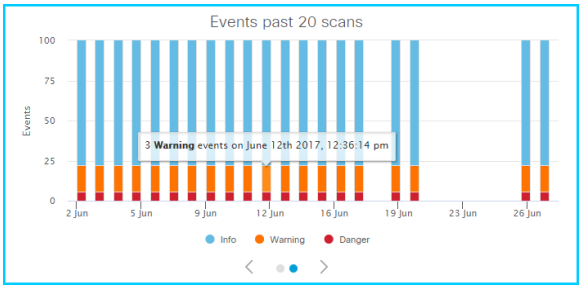
Hover the pointer over the Duplicate label in order to view information about the master device. You can also click the label in order to make this entry the master device.



Device Details

Click a device that is listed on the Devices page in order to open the Device Details page. Here, you can view and edit device information, initiate a manual device scan, and view events that affect the device.

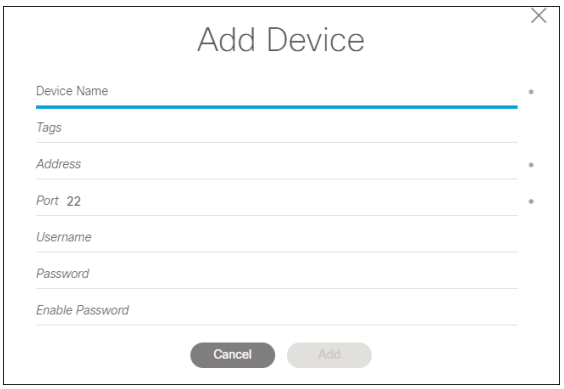
Click the left and right arrows below the event graph in order to switch between a display of open events and checks performed, and events sorted by severity.



Add Devices Manually

You can add devices manually to check the diagnostics before adding the data sources. Perform these steps in order to add a device manually:

1. On the Devices tab, click the **Add** button. The *Add Device* window appears.



2. Enter a name for the device in the **Device Name** field.
3. Enter the IP address in the **Address** field.
4. Select the check box if you want to use the default credentials entered on the General Settings tab of the Settings page in order to connect to the device.
5. Select the Port number using the up and down arrow.
6. If you selected not to use default credentials, enter the Username and Password in order to connect to the device.
7. Click **Add**. The device is added to the Devices list.

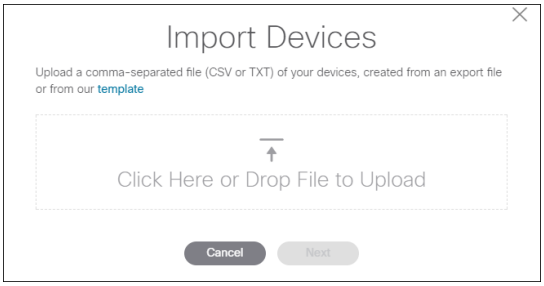
Import Devices

You can import multiple devices from a comma-separated value (CSV) file.

A template CSV file, which you can fill in with device data, is available for download within the application. In order to download the template file, click the **Import** button on the Devices tab. In the *Import Devices* window, click the hyperlinked text "template".

Perform these steps in order to import devices:

1. On the Devices tab, click the **Import** button. The *Import Devices* window appears.



2. Drag the CSV file from Windows Explorer onto the designated area of the window. Alternatively, click inside the box, browse to the file, and select it.
3. Click **Next**.
4. Enter login credentials for the first device in the import file.
5. Optionally, click the **Use for all further devices** toggle button in order to use the same login credentials for all devices in the import file. (You can enable this option at any point in order to apply the credentials that you are currently entering to all remaining devices in the import file.) If you enable this option, click **Import Devices** in order to complete the import process.
6. If you have not enabled the **Use for all further devices** option, click **Next**. Enter login credentials for each device as required. When no further credentials are required, click **Import Devices** in order to complete the import process.

Export Devices

You can export devices to a comma-separated value file.

If you want to export all the devices in the list, click the **Export All** button on the Devices tab. The file is generated and downloaded to your computer.

If you want to export specific devices, select the check boxes beside the desired devices on the Devices tab. Click the **Bulk Actions** button and select **Export Devices**. The file is generated and downloaded to your computer.

Scan Devices Manually

Note: Manual device scans require Enhanced service level or higher. The scan button does not appear for Basic service level users.

In order to perform a manual device scan, click the Play button beside that device on the Devices page. Alternatively, select multiple devices, click the Bulk Actions button, and select Scan Devices.

Enable Scheduled Scan for Devices

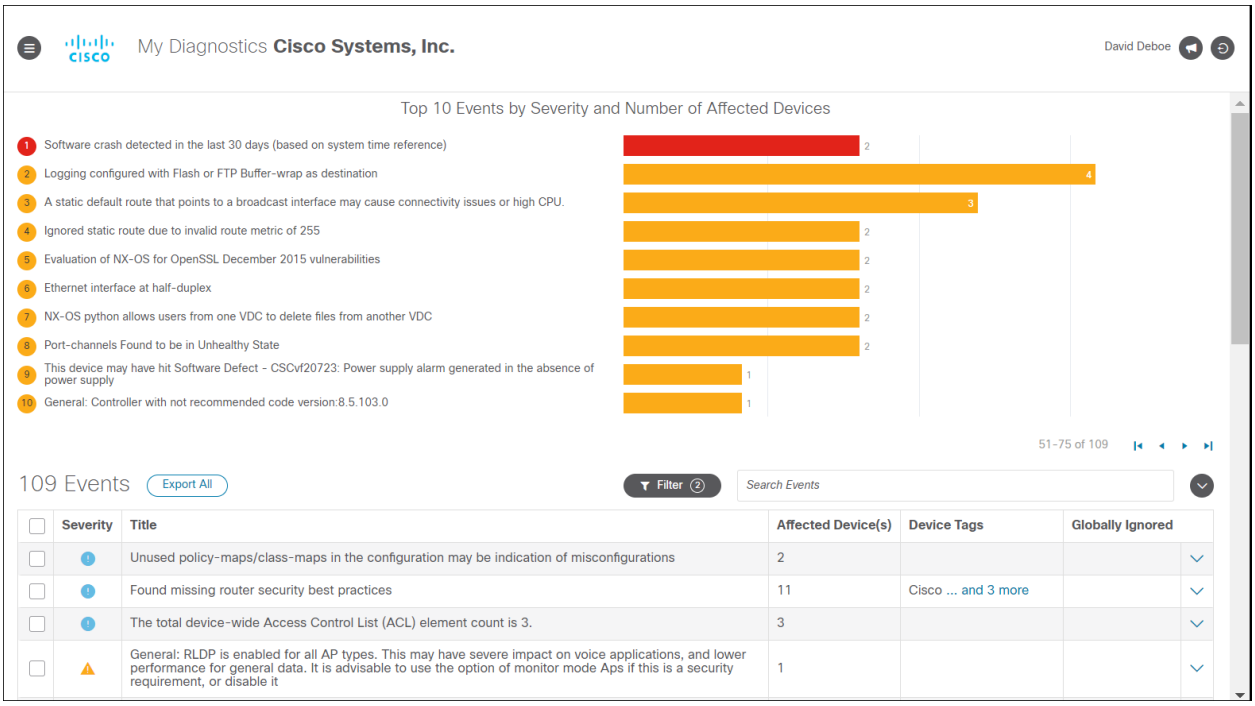
After you have used the Scan Schedule tab on the Settings page to set a day and time for automatic device scans, check the device list on the Devices page to ensure that the desired devices are enabled for the scheduled scan.

Click the toggle button in the Scan column of the device list to enable or disable the scan for each device.

Events Page

Click the Events tab in order to open the Events page. You can also open the Events page by clicking the box on the Home page that displays the number of open events.

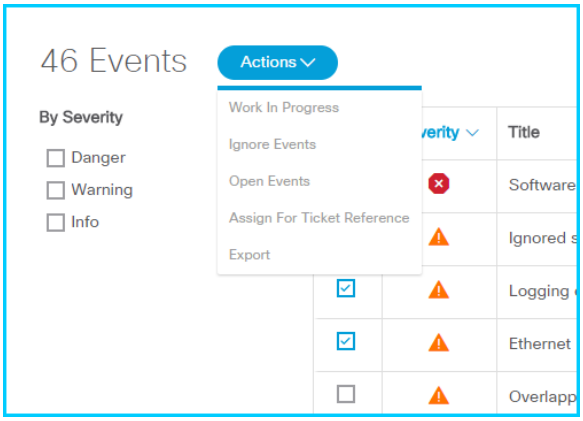
The top area of the Events page displays a graph of the top 10 events by severity and number of affected devices.



The lower area of the page displays a table of events, initially sorted by severity. You can click column headers in the table in order to change the sort order. You can also select the filter check boxes beside the table in order to show or hide severity levels.

Click an event in the table in order to expand the row and show affected devices. You can then click a device in order to open the Device Details page.

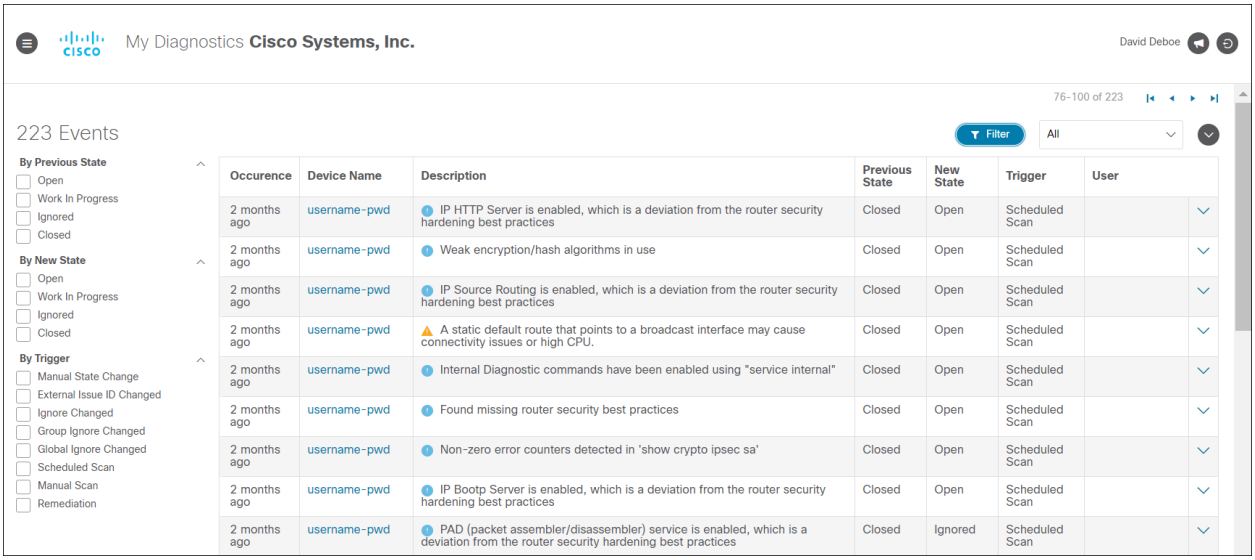
Select the check box beside one or more events in the list in order to enable the **Actions** button. The Actions button provides options to label events as "work in progress", to ignore events, assign events to a support ticket, or export events to a CSV file.



View Event History

Click the History tab in order to view information about past events.

When the page opens, it displays all events in chronological order, from most recent to oldest. In order to locate specific events, click the **Filter** button and select the states and/or triggers for which you want to display matched events. You can also select a date range from the drop-down list in the **Event Dates** box in order to display only events that originated within the selected date range.



Investigate Devices

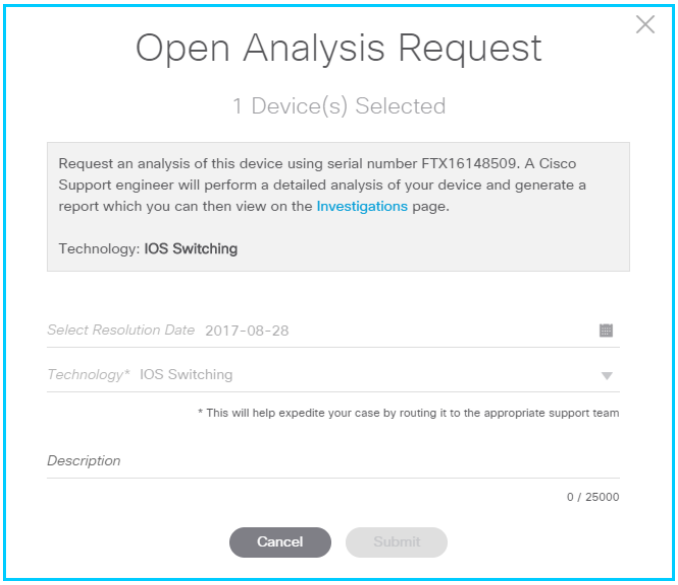
Note: Premium service level is required in order to request an investigation. The Investigate button does not appear for Basic and Enhanced service level users.

You can submit a request to investigate a list of devices or a specific device. A Cisco Support Engineer will perform a detailed analysis and submit a report that is available on the Investigations page.

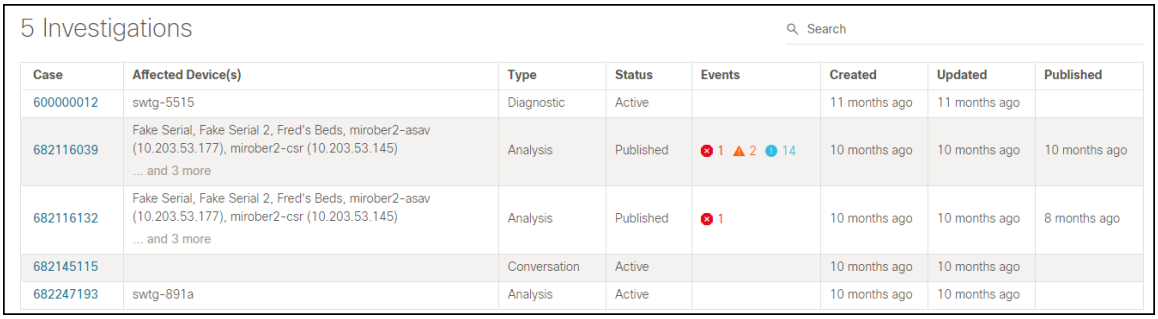
You can submit the investigation request from the Devices page or from the Individual device details page. A list of investigations that you have requested appears on the Investigations page.

Complete these steps in order to investigate a device:

1. Select the device from the Devices page, or open the Details page for that device, and click the Open an Analysis Investigation button. The *Open Analysis Request* window appears.



2. Select the Resolution date and enter a Description. Click **Submit** in order to submit the request.
3. All of the investigations that you requested will appear on the Investigations page.

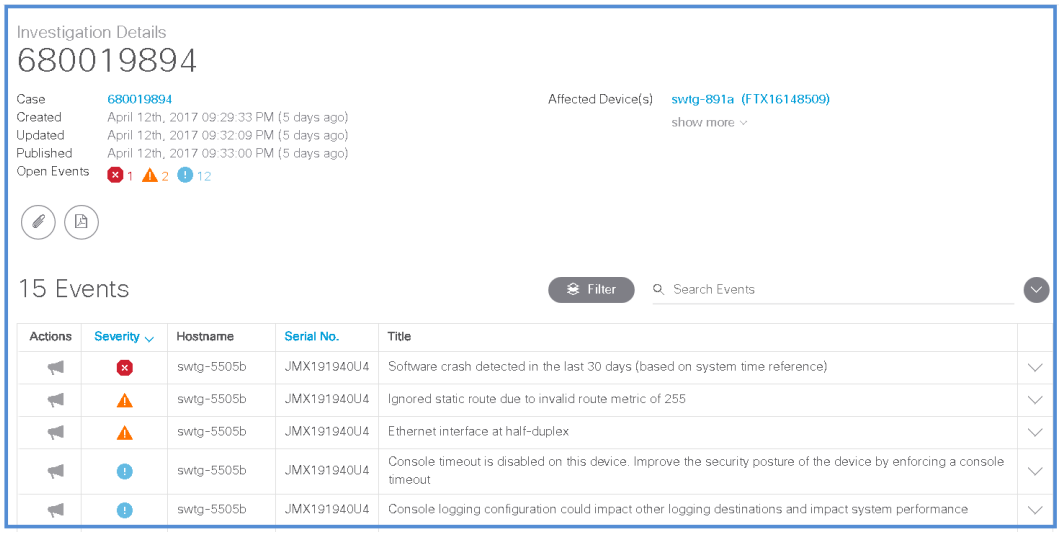


5 Investigations

Search

Case	Affected Device(s)	Type	Status	Events	Created	Updated	Published
600000012	swtg-5515	Diagnostic	Active		11 months ago	11 months ago	
682116039	Fake Serial, Fake Serial 2, Fred's Beds, mirober2-asav (10.203.53.177), mirober2-csr (10.203.53.145) ... and 3 more	Analysis	Published	1 2 14	10 months ago	10 months ago	10 months ago
682116132	Fake Serial, Fake Serial 2, Fred's Beds, mirober2-asav (10.203.53.177), mirober2-csr (10.203.53.145) ... and 3 more	Analysis	Published	1	10 months ago	10 months ago	8 months ago
682145115		Conversation	Active		10 months ago	10 months ago	
682247193	swtg-891a	Analysis	Active		10 months ago	10 months ago	

4. Click the Case link in order to view the case details. The case details page appears.



Investigation Details
680019894

Case 680019894
Created April 12th, 2017 09:29:33 PM (5 days ago)
Updated April 12th, 2017 09:32:09 PM (5 days ago)
Published April 12th, 2017 09:33:00 PM (5 days ago)
Open Events 1 2 12

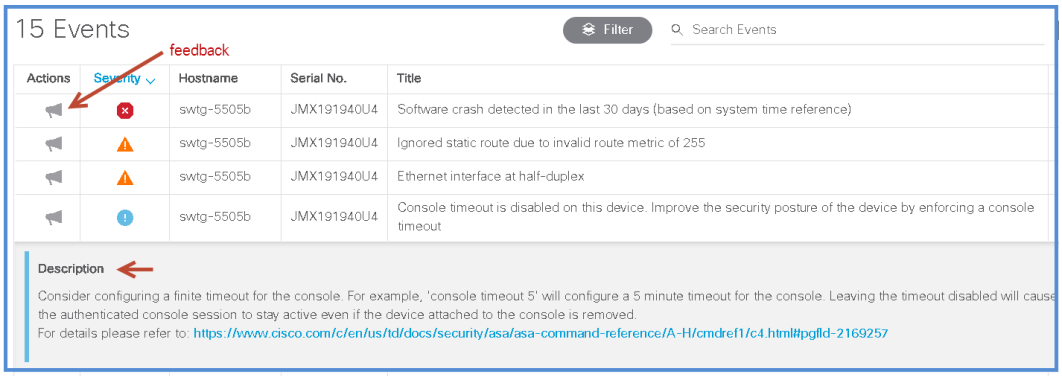
Affected Device(s) swtg-891a (FTX16148509)
show more

15 Events

Filter Search Events

Actions	Severity	Hostname	Serial No.	Title
		swtg-5505b	JMX191940U4	Software crash detected in the last 30 days (based on system time reference)
		swtg-5505b	JMX191940U4	Ignored static route due to invalid route metric of 255
		swtg-5505b	JMX191940U4	Ethernet interface at half-duplex
		swtg-5505b	JMX191940U4	Console timeout is disabled on this device. Improve the security posture of the device by enforcing a console timeout
		swtg-5505b	JMX191940U4	Console logging configuration could impact other logging destinations and impact system performance

5. Click the Title link in order to view the information provided by the TAC engineer. It includes Description, Plan, Impact, Output and Comments. In order to submit feedback, click the icon available under Actions.



Actions	Severity	Hostname	Serial No.	Title
📢	✖	swtg-5505b	JMX191940U4	Software crash detected in the last 30 days (based on system time reference)
📢	⚠	swtg-5505b	JMX191940U4	Ignored static route due to invalid route metric of 255
📢	⚠	swtg-5505b	JMX191940U4	Ethernet interface at half-duplex
📢	ⓘ	swtg-5505b	JMX191940U4	Console timeout is disabled on this device. Improve the security posture of the device by enforcing a console timeout

Description

Consider configuring a finite timeout for the console. For example, 'console timeout 5' will configure a 5 minute timeout for the console. Leaving the timeout disabled will cause the authenticated console session to stay active even if the device attached to the console is removed.
For details please refer to: https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1/c4.html#pgfId-2169257

Note: You can also request analysis for a single device from a TAC engineer. This is available to Enhanced customers who have purchased the TAC Add on Level 1 and Premium customers.

You can submit a request for analysis on the individual device details page.

Work

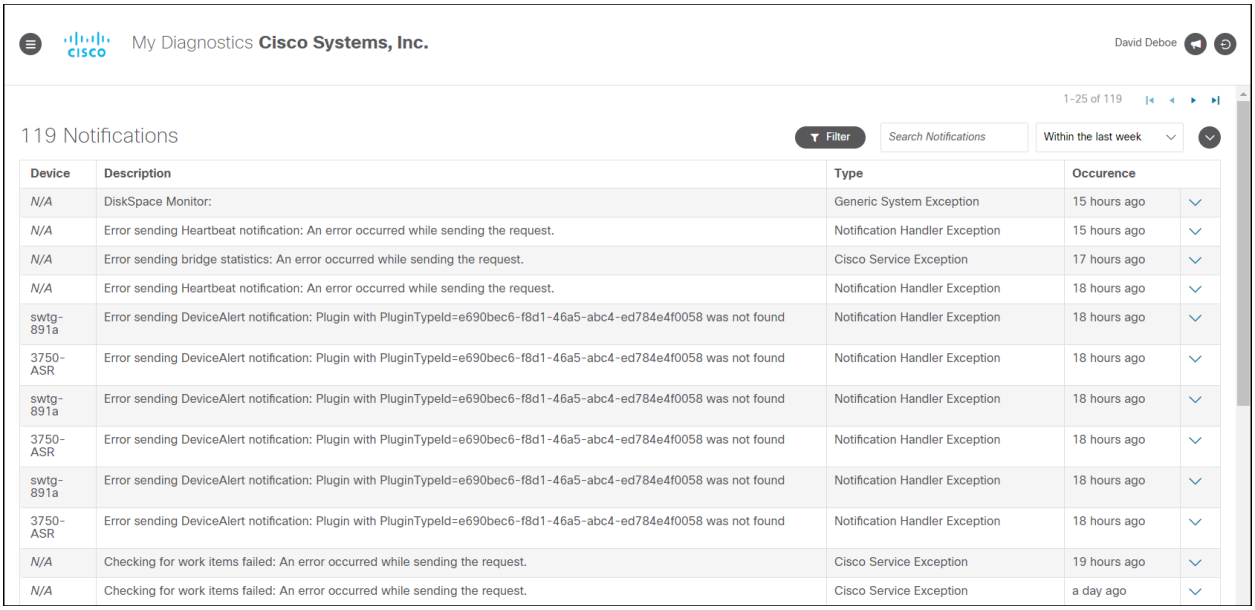
The Work tab is a future capability that will help automate the collection and upload of Service Request data that is requested by TAC.

View Notifications

Click the Notifications tab in order to view the messages that are associated with system events.

When the page opens, it displays all notifications in chronological order, from most recent to oldest. In order to locate specific notifications, enter text in the **Search Notifications** box, or click the **Filter** button and select the notification types that you want to display. You can also select a date range from the drop-down list beside the search box in order to display only notifications that originated within the selected date range.

Click the arrow beside a notification in order to show or hide the full message.



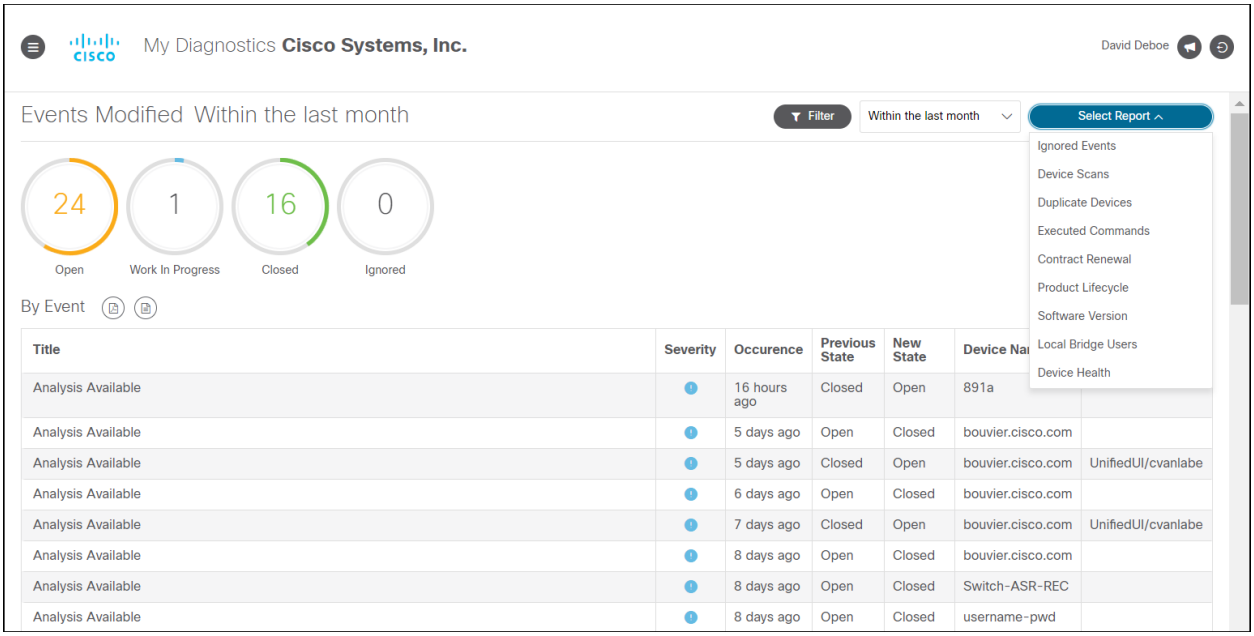
Device	Description	Type	Occurence
N/A	DiskSpace Monitor:	Generic System Exception	15 hours ago
N/A	Error sending Heartbeat notification: An error occurred while sending the request.	Notification Handler Exception	15 hours ago
N/A	Error sending bridge statistics: An error occurred while sending the request.	Cisco Service Exception	17 hours ago
N/A	Error sending Heartbeat notification: An error occurred while sending the request.	Notification Handler Exception	18 hours ago
swtg-891a	Error sending DeviceAlert notification: Plugin with PluginTypeId=e690bec6-f8d1-46a5-abc4-ed784e4f0058 was not found	Notification Handler Exception	18 hours ago
3750-ASR	Error sending DeviceAlert notification: Plugin with PluginTypeId=e690bec6-f8d1-46a5-abc4-ed784e4f0058 was not found	Notification Handler Exception	18 hours ago
swtg-891a	Error sending DeviceAlert notification: Plugin with PluginTypeId=e690bec6-f8d1-46a5-abc4-ed784e4f0058 was not found	Notification Handler Exception	18 hours ago
3750-ASR	Error sending DeviceAlert notification: Plugin with PluginTypeId=e690bec6-f8d1-46a5-abc4-ed784e4f0058 was not found	Notification Handler Exception	18 hours ago
swtg-891a	Error sending DeviceAlert notification: Plugin with PluginTypeId=e690bec6-f8d1-46a5-abc4-ed784e4f0058 was not found	Notification Handler Exception	18 hours ago
3750-ASR	Error sending DeviceAlert notification: Plugin with PluginTypeId=e690bec6-f8d1-46a5-abc4-ed784e4f0058 was not found	Notification Handler Exception	18 hours ago
N/A	Checking for work items failed: An error occurred while sending the request.	Cisco Service Exception	19 hours ago
N/A	Checking for work items failed: An error occurred while sending the request.	Cisco Service Exception	a day ago

View Reports

My Diagnostics provides a suite of reports that allow you to view information about devices and events at a glance, and drill down in order to obtain more specific information that is of interest.

In the top right corner of the Reports page, click the **Select Report** button and choose the type of report that you want to view from the drop-down list. This table describes the available report types:

Report Type	Information Shown
Local Bridge Users	Users (typically local administrative users or service users) for machine-to-machine interaction with the Diagnostic Bridge.
Software Version	The software version and status of the version on each scanned device.
Product Lifecycle	The Last Day of Support and End of Sale for devices that are known to the Bridge.
Contract Renewal	The contract status for all devices that are known to the Bridge.
Executed Commands	An audit trail of diagnostic commands that were run on each device. These commands are used in order to determine the health of scanned devices.
Ignored Events	A history of events that were "ignored", as well as the number of devices that were affected by the events.
Device Scans	The success/failure status of scans for each device.
Events Modified	The state of events that were recently modified, and an audit trail that shows the action that triggered each event's new state.
Duplicate Devices	Devices that are known to the Bridge that share the same serial number. Duplicate devices are linked together. You should designate one of the duplicate entries to be the "master device". When duplicates exist, you can only perform as scan on the master device.
Device Health	A summary of the health of each scanned device, based on open events.



Some report types provide filter and date range options. In order to filter the information that is included in the report, click the **Filter** button and select the desired categories of information. Optionally, select a date range from the drop-down list beside the **Filter** button. The report updates automatically.

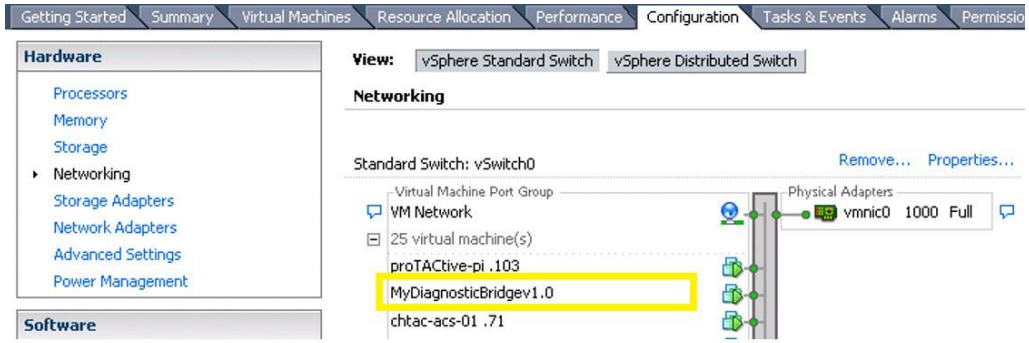
Many reports contain hyperlinked elements that provide more detailed information when you click them, or that open another page in the application (such as the Device Details page when you click the name of a device in a report).

You can export a report to a file in either PDF or CSV format. Click the button ( ) for the file format that you want to use.

Troubleshooting

Network Connectivity from the Diagnostic Bridge

1. If the deployed OVA (previous versions of the Diagnostic Bridge supported OVA installation) is unable to connect to the network, you may have provisioned the wrong VM Network in vCenter:



2. If you are unable to communicate with other servers outside of your network, you may need to configure additional proxy settings:

```
[root@localhost]# more /etc/environment
 http_proxy="http://proxy-1.cisco.com:88"
 https_proxy="http://proxy-1.cisco.com:88"
 no_proxy="127.0.0.1,10.48.71.11"


[root@localhost]# more /etc/yum.conf
 [main]
 proxy=http://proxy-1.cisco.com:88
```

Note: in the above example, `https_proxy` uses http proxy settings to establish the connection. This may be different in your environment.

3. If the Cisco Diagnostic Bridge is unable to connect to defined Data Sources, you may need to configure proxy settings in the file `outbound-connection.json`, which is located in `/Diagnostic Bridge/etc/`. A configuration example follows:

```
"HostSelector": "*",
"AllowInvalidCertificate": true,
"ProxyAddress": "http://proxy-1.cisco.com:88",
"ProxyUseDefaultCredentials": false,
"ProxyUsername": "proxyusername",
"ProxyPassword": "proxypassword",
"ProxyCredentialDomain": null
```

My Diagnostics API

System integrators can look into Cisco Diagnostic Bridge with this link:

https://your IP address:5001/swagger/

System integrators can view all the capabilities and can access the APIs to push the device list, analyze data and pull devices, and so on.