



Cisco Diagnostic Bridge Getting Started Guide

Version 1.0
May 3, 2017

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.



CHAPTER 1

Introduction	1-1
Connected TAC	1-1
About Cisco Diagnostic Bridge	1-1

CHAPTER 2

Installation	2-1
About Cisco Diagnostic Bridge OVA	2-1
Verifying Prerequisites	2-1
Downloading the OVA File	2-1
Installing the OVA	2-2
Configuring Self-Signed Certificate	2-8
Verifying JSON Files	2-8
Upgrading Diagnostic Bridge CentOS	2-9
Installing MSI on Windows	2-9
Accessing Cisco Diagnostic Bridge	2-17

CHAPTER 3

Configure Application Settings	3-1
Notification Profiles	3-2
Data Sources	3-5
Schedule Scan	3-6
General Settings	3-7

CHAPTER 4

Features	4-1
My Diagnostics	4-1
Devices	4-2
Add Devices Manually	4-4
Setting Same Credentials for Devices	4-5
Scan Devices	4-6
Investigate Devices	4-6

APPENDIX A

CSPC Add-On for Cisco Diagnostic Bridge	A-1
Requirements	A-1

[Code Installation](#) A-1

[My Diagnostic API](#) A-5



Introduction

Connected TAC

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

It enables:

- Automated and proactive problem detection
- Faster resolution by providing remediation recommendations for the identified problems
- The infusion of diagnostic results directly into the most commonly used incident management systems
- Assistance from TAC in managing and resolving 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 login
- 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

About Cisco Diagnostic Bridge

The Cisco Diagnostic Bridge is a 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:

1. Prevent the impact of device issues on network availability, performance and security
2. Reduce the time spent on troubleshooting the devices
3. Improve overall efficiency of the customer 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 existing 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 NMS systems. 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 on-boarding via email after you have signed-up.

Supported Technologies

The Cisco Diagnostic Bridge supports the following technologies:

Basic/Enhanced

- IOS
- IOSXR
- ASA
- Wireless LAN Controller

Premium

- UCS
- ACI
- CUCM
- UCCE



Installation

Cisco Diagnostic Bridge Installation includes:

- OVA Installation
- MSI Installation

About Cisco Diagnostic Bridge OVA

An Open Virtual Appliance (OVA) is a prebuilt software solution that comprises one or more virtual machines (VMs) that are packaged, maintained, updated, and managed as a single unit. The Cisco OVA has a preinstalled operating system (CentOS) and includes application functionality that is necessary for Cisco Diagnostic Bridge. This OVA can be deployed on a VMWare client infrastructure.

This OVA includes:

- CentOS Linux release 7.3.1611 (Core). Special curl is compliant with OpenSSL

Verifying Prerequisites

OVA Requirements:

Before you install the Cisco OVA, you must meet following software and database requirements:

- Linux OVA running on VMware ESXi 5.5 or later that requires 2 CPU, 8GB RAM and 50 GB HDD

Windows Requirements:

- Windows 7 and higher with dotnet Core 1.1.1 and mysql
- Diagnostic bridge can also be running as CLI on Windows



Note

It is mandatory to keep the firewall port such as 5001 open.

Downloading the OVA File

The first step to install OVA is to download the latest version of OVA file. You will point to that file on your computer when deploying the OVF template.

To download the file, perform the following:

1. Go to the following site:
https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=Cisco_Diagnostic_Bridge
2. Locate the OVA Installer and click the **Download** button.
3. Save the file to your computer in a place that will be easy to find when you start to deploy the OVF template.

Installing the OVA

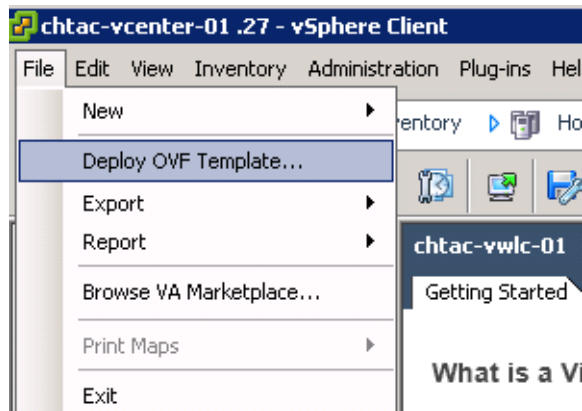
After you download the Open Virtual Appliance file, deploy the OVF template from the vCenter Client application.



Note

You must change the password and IP address as per your requirement. The default credentials are: root/Cisco123, admin/Cisco123

1. Login to your vCenter client application on your desktop.
2. Connect to the vCenter Server with your vCenter user credentials.
3. Use the vCenter Client to access the OVF template:
 - a. Choose **File > Deploy OVF Template** to open the Deploy OVF Template window.
 - b. Choose the host on which the OVF template will be deployed.



4. Choose the Source location:
 - a. Click **Browse** and locate the OVA file that you downloaded to your computer and click **Next**.

Deploy from a file or URL

C:\temp\MyDiagnosticBridge-v1.0.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

- b. You can choose to rename the downloaded OVA file.

Deploy OVF Template

Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)

Name and Location

Host / Cluster
Resource Pool
Disk Format
Ready to Complete

Name:
MyDiagnosticBridgev1.0
The name can contain up to 80

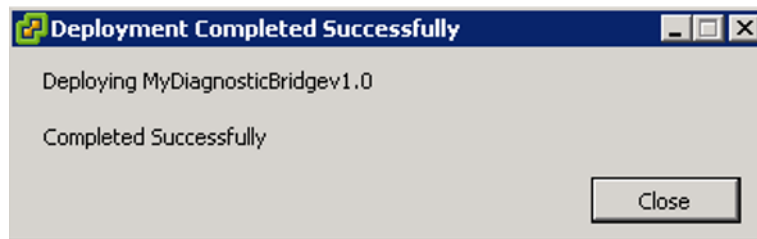
Inventory Location:
 chtac-vcenter-01
 chtac

5. Install OVA on datastore and choose the disk format, according to your setup requirements such as Thin Provision (1.4 GB) or Thick Provision (50 GB).
6. Choose your Network Mapping.
7. Refer to the figure below for deployment settings:

Deployment settings:

OVF file:	C:\temp\MyDiagnosticBridge-v1.0.ova
Download size:	1.1 GB
Size on disk:	2.8 GB
Name:	MyDiagnosticBridgev1.0
Folder:	chtac
Host/Cluster:	10.51.82.25
Datastore:	Oelberg_DS
Disk provisioning:	Thin Provision
Network Mapping:	"VM Network" to "VM Network"

8. After successful deployment, the following window appears:



9. After deploying the OVA file successfully, start the diagBridge CentOS VM guest device using VM client console:
 - login: **root**
 - Password: **Cisco123**
10. You will be prompted to change the password. It is recommended to change the password.
11. The CentOS runs on English/US settings due to installation equipment. To change the language settings, use the command:

man localectl

Example:

```
changing keyboard layout and locale:
#localectl set-locale LANG=en_US.UTF-8
#localectl set-keymap us
```

12. To change the keyboard layout and locale, use the following commands:

```
#localectl set-locale LANG=en_US.UTF-8
```

```
#localectl set-keymap us
```



Note

Ensure you have the accurate time settings and synchronization to start the Diagnostic Bridge.

13. To modify the IP address and default gateway, there are two options:

- a. Using the following set of commands:

```
nmcli c mod ens32 ipv4.address 192.168.1.2/24 ipv4.gateway 192.168.1.1
```

```
nmcli c down ens32
```

```
nmcli c up ens32
```

- b. Using the NetworkManager TU. To open the NetworkManager TUI, use the command:

```
nmtui
```

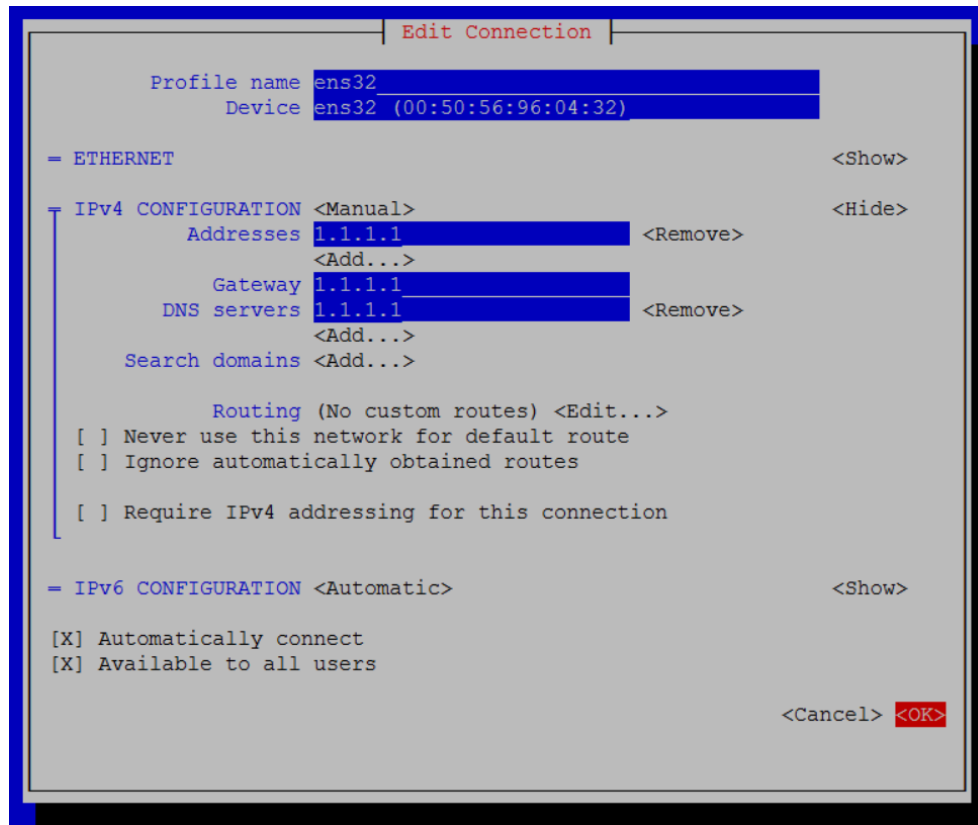
The following window appears:



- c. Edit Connectivity. Replace ens32 with the required IP address.



- d. Enter the IP address.



- e. Click **OK** to continue.
14. Restart the Network Card, for the changes to apply.

```
systemctl restart network.service
```

15. Verify network connectivity using commands:

```
route -n {only one default gateway}
```

```
ifconfig {your ip address}
```

```
ping {ping api.cisco.com} (If this fails check the DNS setting and/or PROXY in your network)
```

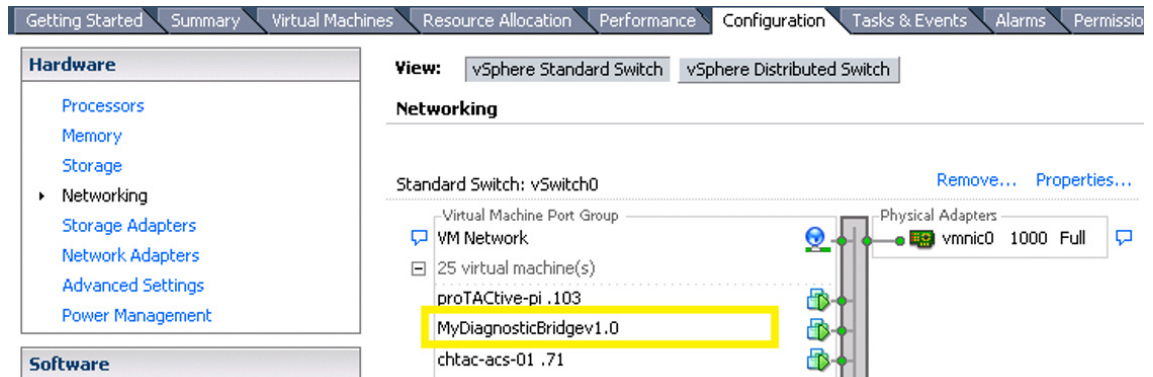
**Note**

If you have the API to get the device list from data source such as Cisco Prime (PI), raise an exception, if the customer is using proxy server.

For example: The device list can be fetched using API in the PI server (10.48.71.11)

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

16. You can choose to map the VM Network correctly.



17. Reboot the Diagnostic Bridge from the VM Client Console, using the command **Reboot**, the Diagnostic Bridge boots automatically:



Note

The SSH session timeout is 5 minutes.

18. To start, stop, restart and verify the diagBridge client, use the following commands from the VM Client Console:

```
systemctl start rc-local
```

```
systemctl stop rc-local
```

```
systemctl restart rc-local
```

```
systemctl status rc-local
```

19. To verify the Diagnostic Bridge installation, use the command:

```
ps -ef | grep dotnet
```



Note

Ensure you configure the timezone and setup the date on your system before accessing MyDiagnostic.

20. To change the DiagnosticBridge timezone settings depending on the VM host settings, perform the following:

- Login as admin and change to root.
- To verify the settings use the command **timedatectl**.
- To change the time and date use the commands **timedatectl set-time** and **timedatectl set-timezone** respectively. Refer to the example below:

```
timedatectl set-time "2017-04-28 06:00:00"
timedatectl set-timezone America/New_York
```

- To view the syntax for timezone use the command **timedatectl list-timezones**.

21. To access and configure the My Diagnostic Bridge Interface using a browser, go to <https://cway.cisco.com/mydiagnostics>.

**Note**

- When you access the Diagnostic Bridge for the first time, you must accept the certificate for secured connection between the Diagnostic Bridge and the My Diagnostic Interface. To replace the certificate, refer to [Configuring Self-Signed Certificate](#).
 - The Diagnostic Bridge does not have direct communication to Cisco's My Diagnostic Interface. It needs a web browser of the client PC, managing the Diagnostic Bridge. All the communication to port 5001 goes through the host connecting to My Diagnostics.
22. You can now add and analyze the devices. To configure settings, refer to [Configure Application Settings](#).

Configuring Self-Signed Certificate

After the installation is completed successfully, the **TestCertificate** is installed automatically in the following folder:

- For OVA Installation: **/DiagnosticBridge/etc** folder
- For MSI Installation: **C:\Program Files (x86)\Cisco\DiagnosticBridge\etc** folder

This enables a secured connection between Diagnostic Bridge and the Interface.

You can replace this certificate with a self-signed certificate or an official certificate from your certificate signing authority. If you replace this certificate, you must edit the **static-settings.json** file to point to the new certificate. After making the changes, access the Diagnostic Bridge URL (<https://<Your IP Address>:5001/home>) and accept the new certificate.

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

**Note**

- If you generate your own self-signed certificate, you must accept the certificate before the Cisco MyDiagnostics UI will be allowed to communicate with your bridge.
- If the certificate installed is signed by an approved Internet Certificate Assigning Authority, the browser will automatically trust the communication from Cisco MyDiagnostics UI to the bridge.
- You can also use the Diagnostic Bridge URL: <https://<Your IP Address>:5001/home>, for debugging purpose.

Verifying JSON Files

After the installation is completed successfully, the following json files are available in the **/DiagnosticBridge/etc** folder:

1. **api-users.json**: This file contains the login credentials. You can choose to enter user credentials. This can be used for API authorization.
2. **static-settings.json**: This file contains ports 5001 and mysql root password (default: Cisco123) and my diagnostic URL.
3. **settings.json**: This file includes the Client ID and Client Secret details.
4. **outbound-connections.json**

5. Installation-settings.json

Upgrading Diagnostic Bridge CentOS

There are two ways to upgrade:

- Using SSH
- Using the My Diagnostic Interface

Upgrade Using SSH

To upgrade the diagnostic bridge using SSH, replace the folder in /DiagnosticsBridge/bin.

1. Login using SSH to your diagnostic bridge using **root/Cisco123** (default).
2. Stop the Cisco Diagnostic Bridge Service.
3. You can choose to keep the previous version as a sample backup by renaming the folder bin to old_bin.



Note It is recommended to keep previous versions to revert back if you face any issues.

4. To install the new version, copy the bin folder to DiagnosticBridge with all the files for example, using WinSCP:

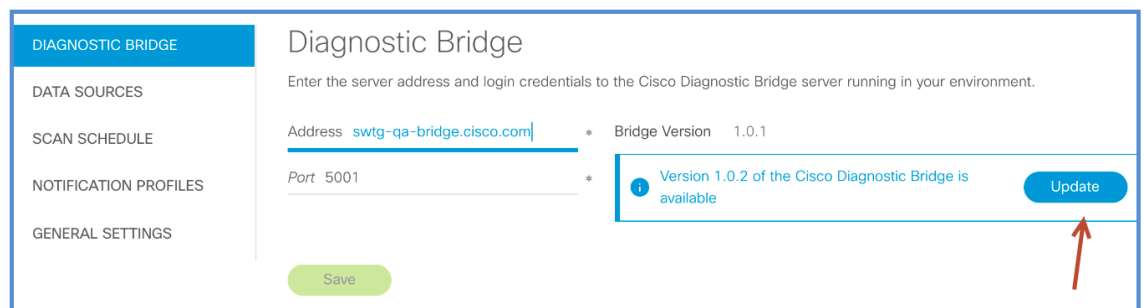
```
/DiagnosticBridge/etc
/DiagnosticBridge/bin
/DiagnosticBridge/old_bin (renamed with previous version)
```



Note The previous configuration settings are retained after upgrade.

Upgrade Using My Diagnostic Interface

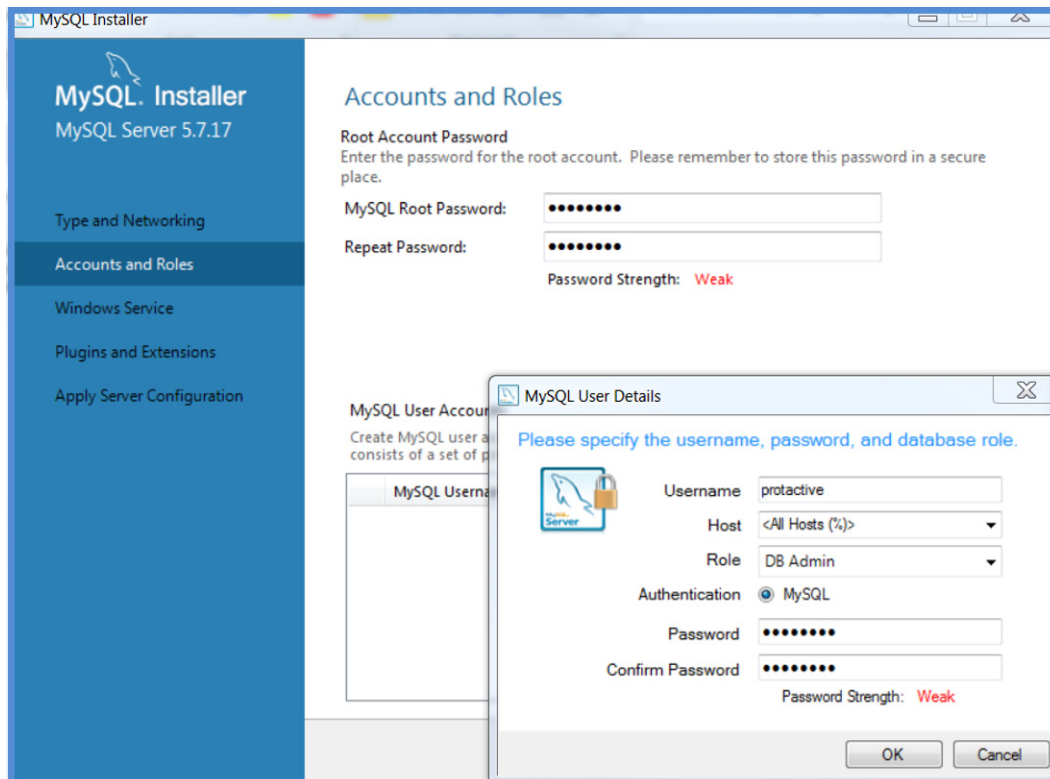
To upgrade from the My Diagnostic Bridge Interface. Click the **Update** button to upgrade to next version. Refer to the figure below:



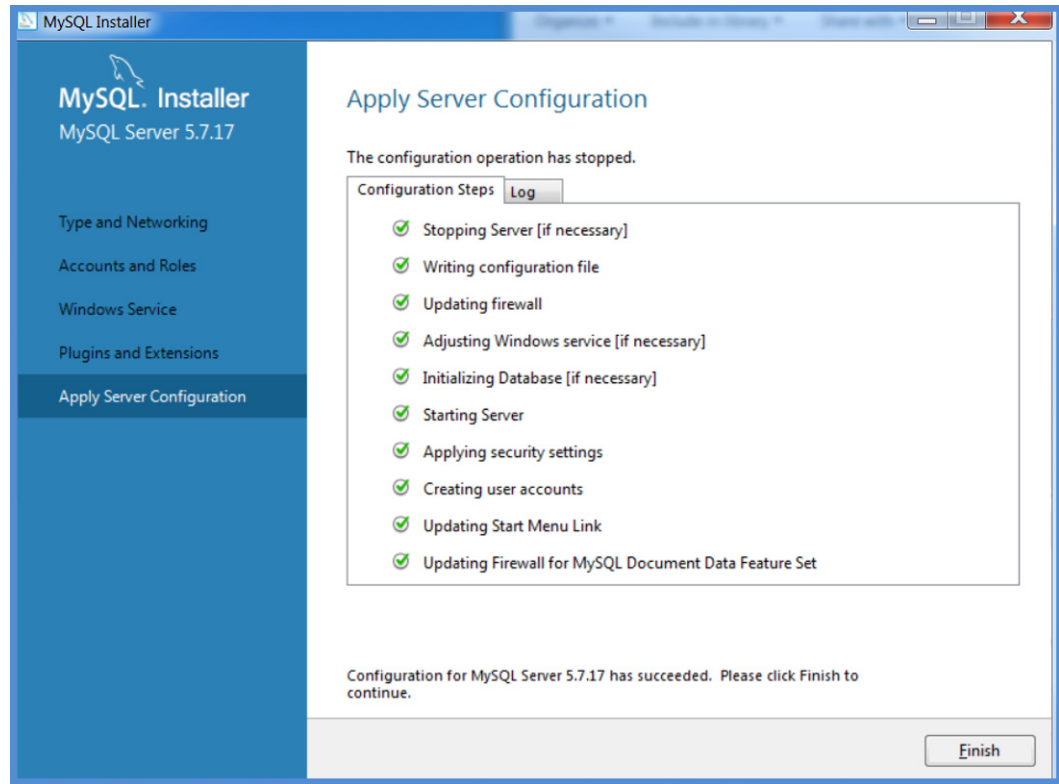
Installing MSI on Windows

To install Diagnostic Bridge on Windows system, perform the following:

1. Download MySQL from <https://dev.mysql.com/downloads/installer/>
 - Server only – all Password: **Cisco123** (This password is used for settings-fallback.json configuration that requires root access to the DB).



- Retain default settings.



2. Download .Net Core 1.1.1 from:

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



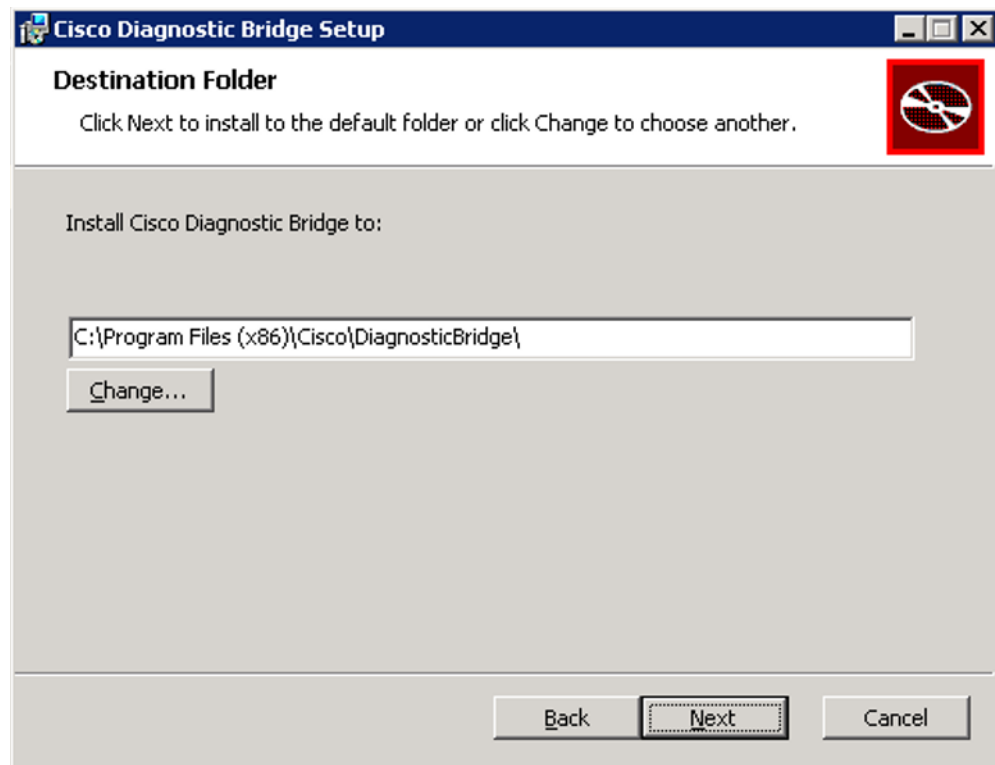
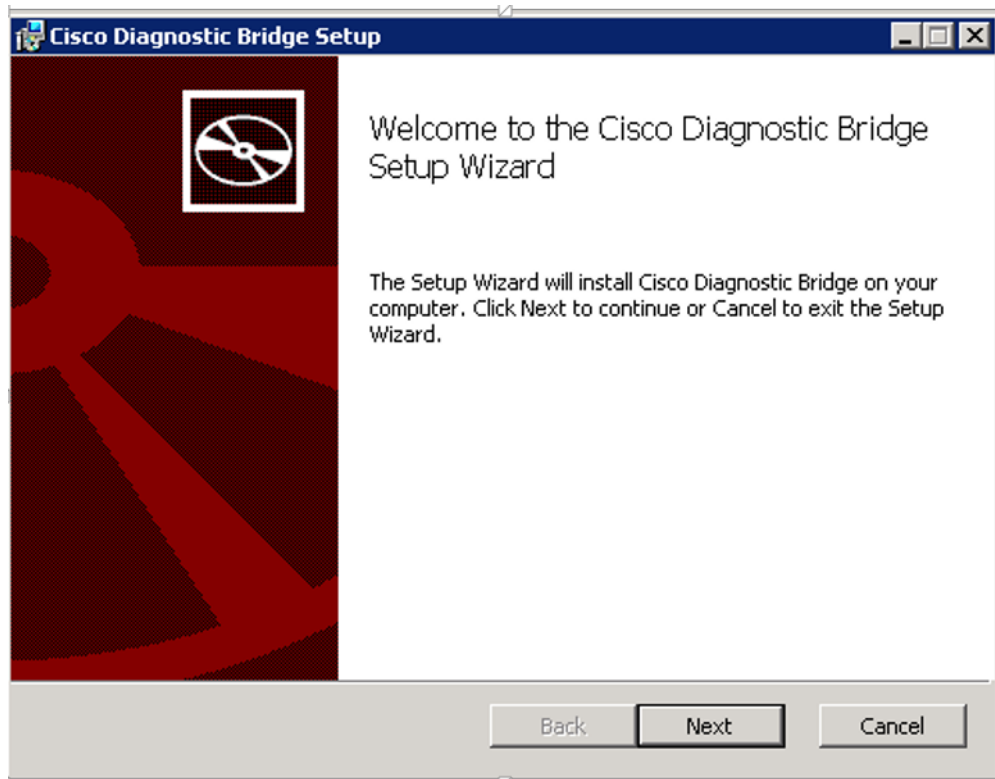
Note

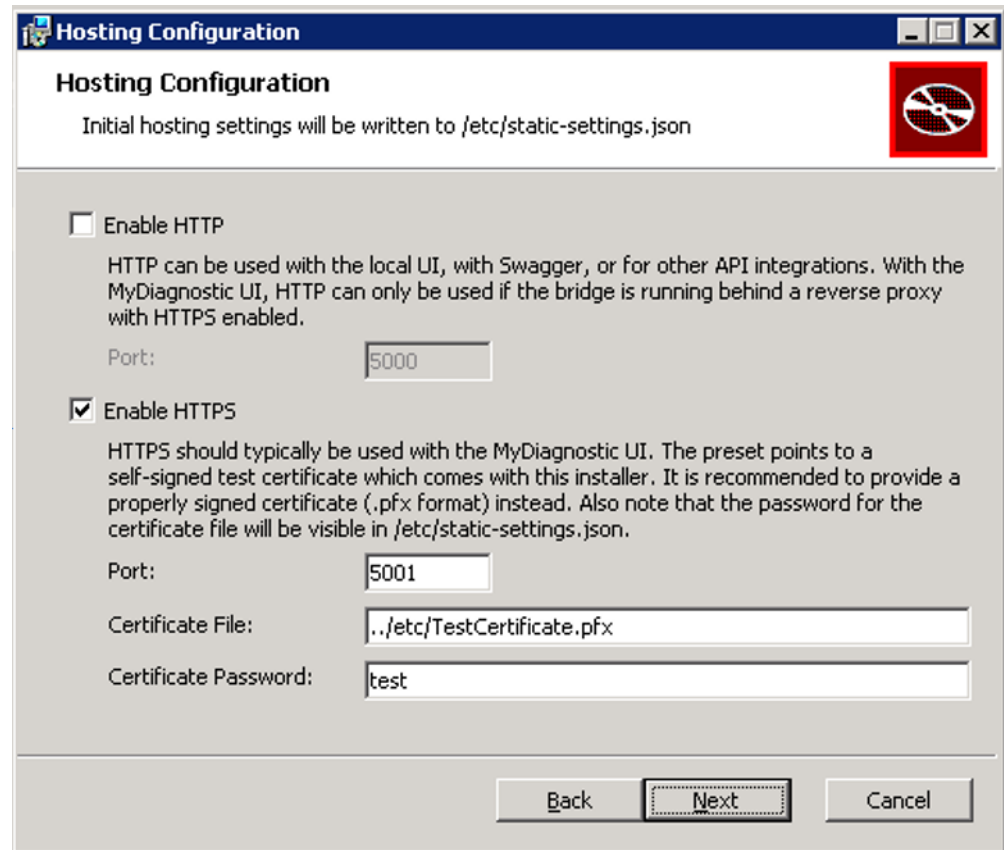
For Windows 7 and 2008 only, make sure that your Windows installation is up-to-date and includes hotfix KB2533623 installed through Windows Update.

3. Add the following path in windows for C:/Program Files/dotnet:

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

4. Download the latest MSI installer of the diagnostic bridge. Start the setup and follow the wizard based instructions:





Hosting Configuration

Initial hosting settings will be written to `/etc/static-settings.json`

Enable HTTP

HTTP can be used with the local UI, with Swagger, or for other API integrations. With the MyDiagnostic UI, HTTP can only be used if the bridge is running behind a reverse proxy with HTTPS enabled.

Port:

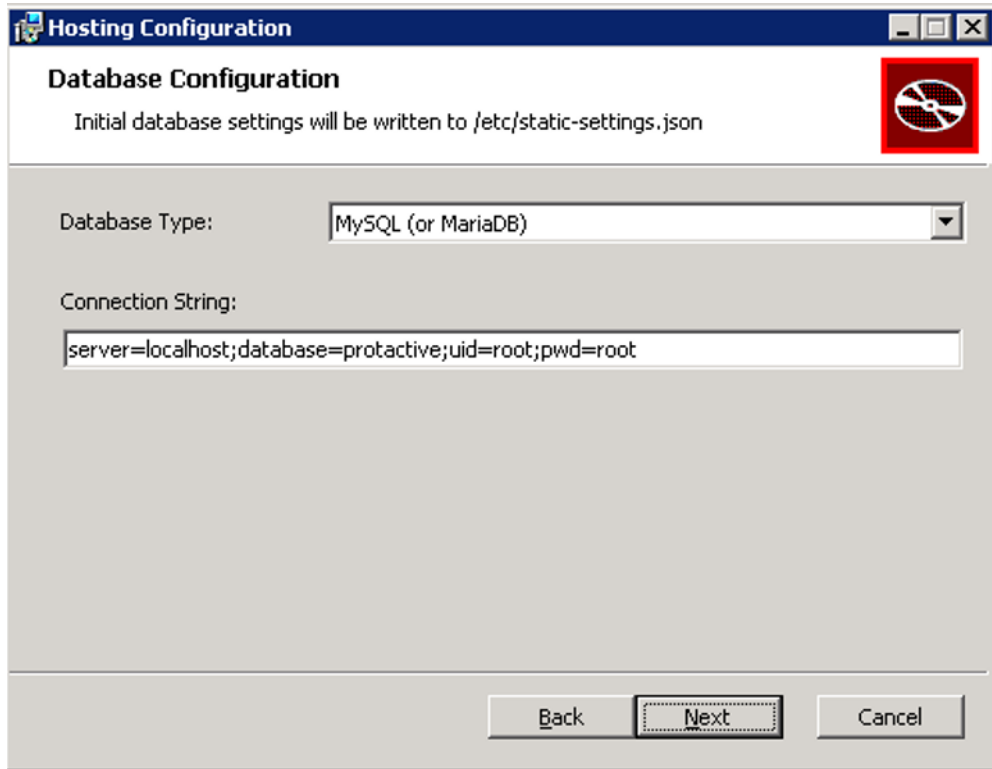
Enable HTTPS

HTTPS should typically be used with the MyDiagnostic UI. The preset points to a self-signed test certificate which comes with this installer. It is recommended to provide a properly signed certificate (.pfx format) instead. Also note that the password for the certificate file will be visible in `/etc/static-settings.json`.

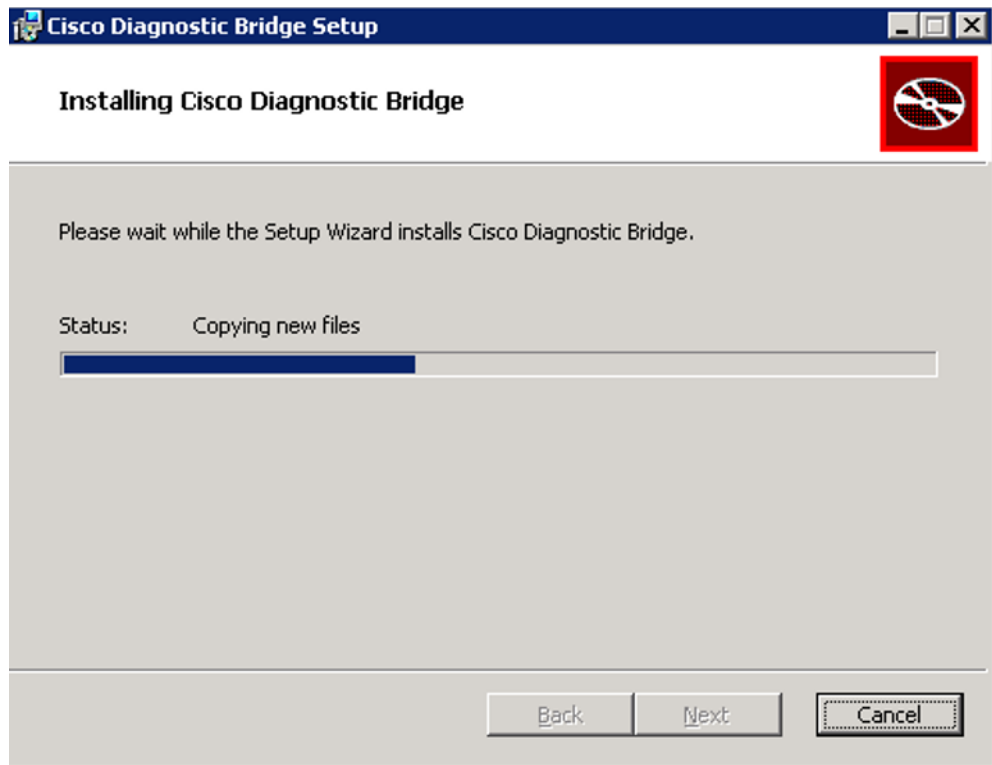
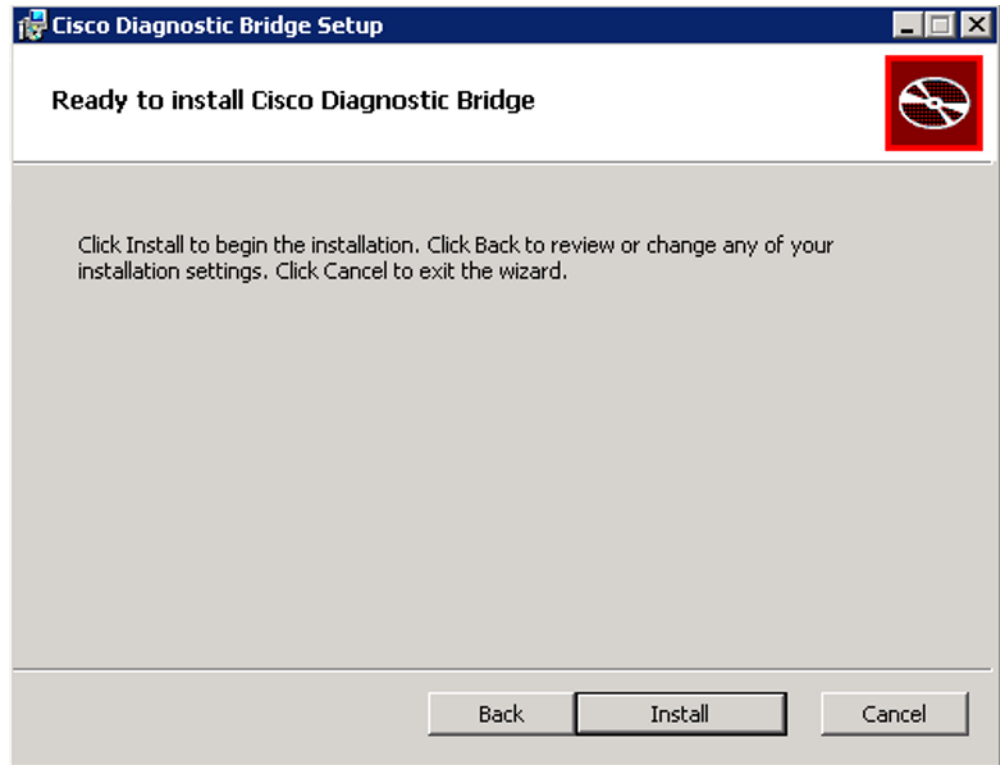
Port:

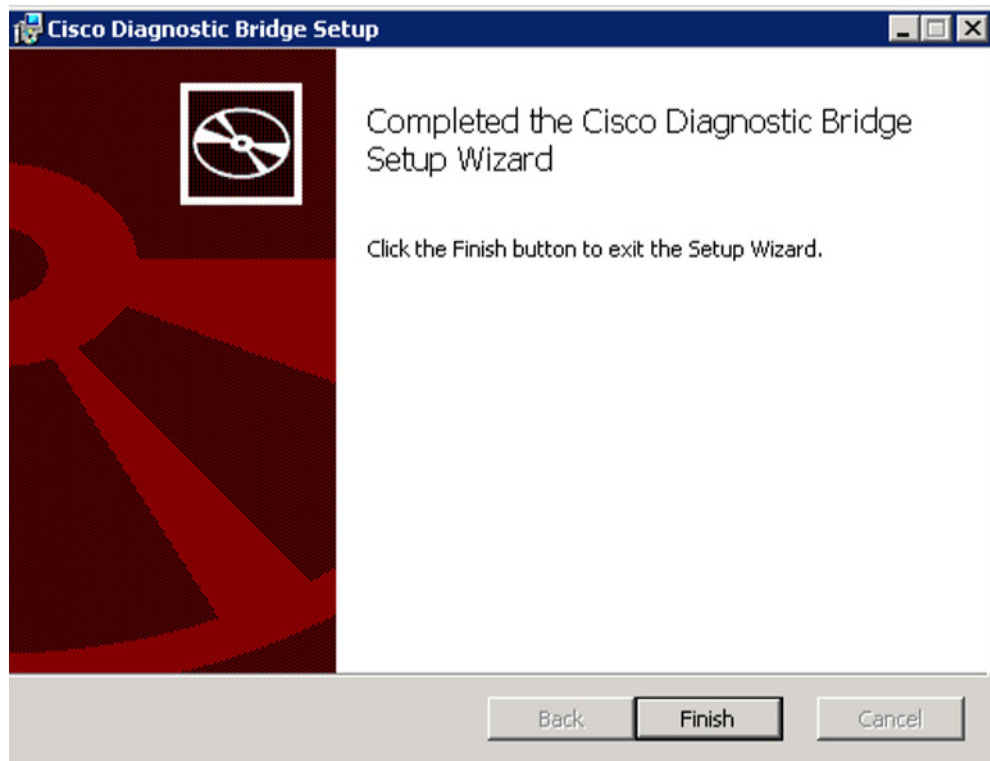
Certificate File:

Certificate Password:

**Note**

Change the userid and password according to the SQL DB settings as required.





5. Click **Finish** to complete the Installation process. Refer to [Verifying JSON Files](#) to verify the json files after successfully installing the Diagnostic Bridge.
6. After installing the Cisco Diagnostic Bridge setup successfully, it will start as a service in Windows machine.
 - Link: *https://Your IP Address/home*



Note During MSI installation the user is prompted to enter port number and user credentials. It is recommended to change the default credentials. You can use the link (*https://Your IP Address/home*) for debugging purpose.

7. To access and configure the My Diagnostic Bridge Interface using a browser, go to <https://cway.cisco.com/mydiagnostics>.



Note

- When you access the Diagnostic Bridge for the first time, you must accept the certificate for secured connection between the Diagnostic Bridge and the My Diagnostic Interface. To replace the certificate, refer to [Configuring Self-Signed Certificate](#).
 - The Diagnostic Bridge does not have direct communication to Cisco's My Diagnostic Interface. It needs a web browser of the client PC, managing the Diagnostic Bridge. All the communication to port 5001 goes through the host connecting to My Diagnostics.
8. You can now add and analyze the devices. To configure settings, refer to [Configure Application Settings](#).

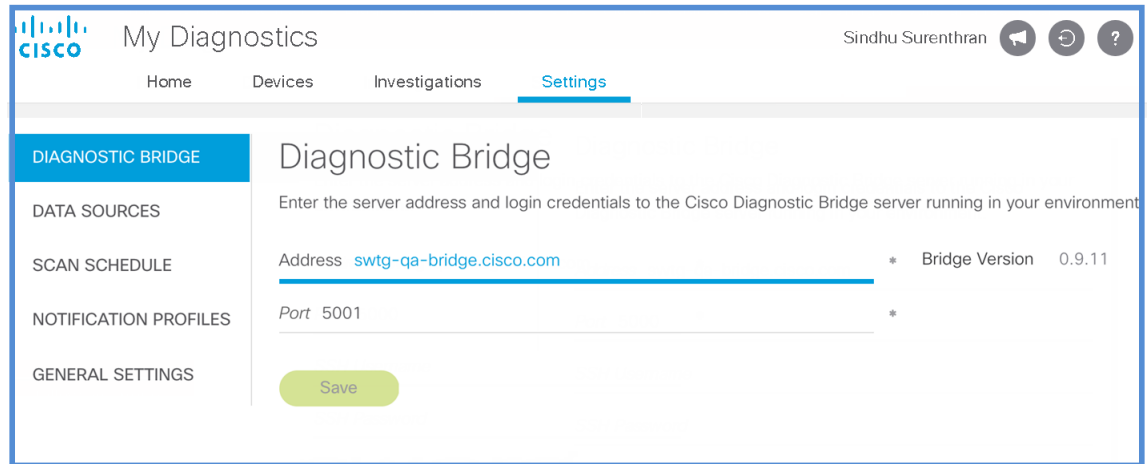
Accessing Cisco Diagnostic Bridge

After the Cisco Diagnostic Bridge is installed, access My Diagnostics to complete configuration of the Bridge from the following URL:

<https://eway.cisco.com/mydiagnostics>

Configuration of the Cisco Diagnostic Bridge is performed from the **Settings** tab.

The Cisco Diagnostic Bridge interface appears with the Settings tab selected. Enter the bridge's address and the port. Click **Save**, the options under the Settings tab will be enabled. You can then configure the settings.



Supported Browsers

The supported browsers are Chrome, Firefox and Safari.

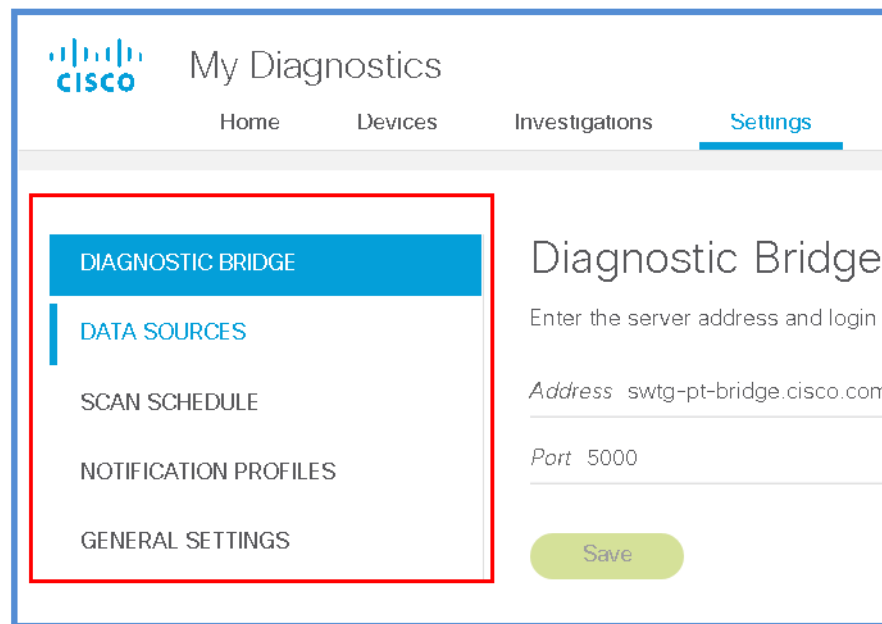


Configure Application Settings

After successfully installing the bridge, launch the My Diagnostics Interface, the **Settings** tab appears. You must first configure the application settings to proceed. Enter the server address and login credentials of the Cisco Diagnostic Bridge server running in your environment and click **Save**.

After saving the bridge's details, the following options are enabled and can be configured. These settings apply across the device sessions.

1. Notification Profiles
2. Data Sources
3. Scan Schedule
4. General Settings



Note

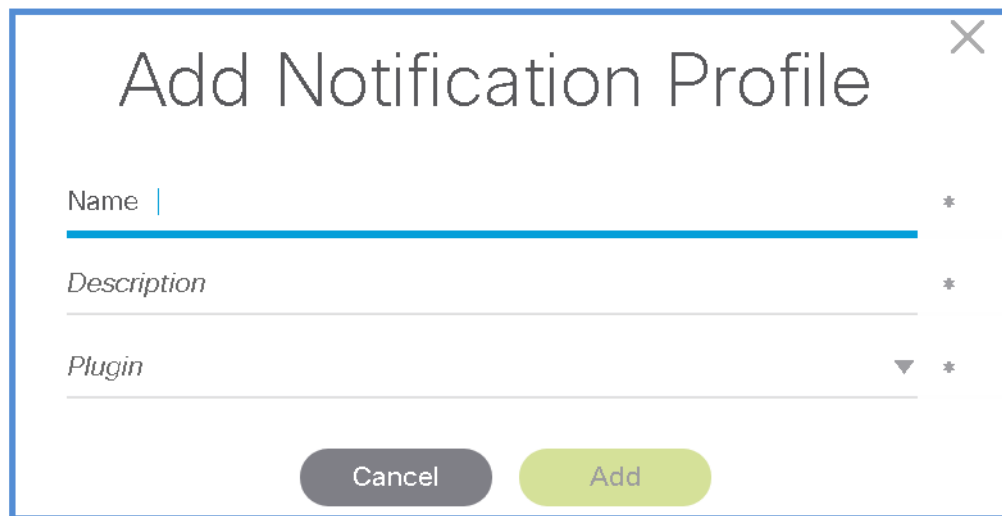
You must first add the Notification Profiles. After adding these profiles, add the Data Sources and schedule periodic scan.

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 in notifying the customers about the events happening on the network devices via SMTP or ServiceNow plugins.

If the customer is using ServiceNow to manage their network, you can configure the ServiceNow notification profile to integrate with the workflow that the customer has, for their ticket or incident management system. This integration helps to create tickets or incidents for the customers in their system.



To add a notification profile, click **Add**, the *Add Notification Profile* window appears. Enter the Name, Description and select the Plugin and the Plugin Type.

- **Name:** Enter a name for the Notification Profile
- **Description:** Enter a description for the Notification Profile
- **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.

SMTP Mail Sender

The SMTP Mail Sender allows you to configure email notifications for device checks. Choose this option 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 while adding SMTP Mail Sender Notification Profiles.

Add Notification Profile ✕

Name !

Description *

Plugin SMTP Mail Sender ▼ *

Plugin Type Sends a template based mail for every alert in a successful run ▼ *

Credentials

Configuration

Username

Password

SMTP Host

SMTP Port 25

Mail From

Mail To

SSL

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

Cancel
Add

- **Credentials:** Click the toggle button in order to enable or disable the ability to reconnect with the login 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 enable or disable the ability to reconnect with the login credentials and SMTP server details 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 the 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 to enable or disable SSL. It is recommended to enable SSL in order to secure the communication between Cisco bridge and the email server.

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. It allows you to integrate with the customer's incident/ticket management system.

- **Credentials:** Click the toggle button in order to enable or disable the ability to reconnect with the login 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 enable or disable the ability to reconnect with the login credentials and SMTP server details 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.

Data Sources

Data sources provide a source of truth 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



Note

Collector Profile allows you to 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 to be identified such as CSPC.

You can use the synchronize option, available in 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 connect to the devices.

To add a data source, click **Add**, the *Add Data Source* window appears. Enter the Name. Select the Source, Collector Profile and the Notification handler. Enter the SSH user credentials to connect to devices.

- **Name:** Enter a name for the data source
- **Source:** Select the source of device data
- **Collector Profile:** Select the collection profile. All the profiles that you created will be listed in the drop-down.

**Note**

You must configure outbound connection for Cisco Prime and CSPC in order to collect the device list. Refer [Verifying JSON Files](#).

- **Notification Handler:** Select the notification profile. All the profiles that you created will be listed in the drop-down
- You must enter the login credentials to connect to Cisco PI and ServicesNow. The Username and Password fields appear on selecting Cisco PI and ServiceNow Sources
- **URL:** Enter the URL to connect to CSPC and ServiceNow
- **Connection String:** Enter the database connection string, to allow the bridge to communicate to Whatsup Gold.

**Note**

The bridge and Whatsup Gold must be configured on the same machine. Cisco Diagnostic Bridge supports WUG 2016 and 2017. For NetBrain, you must contact NetBrain to get the specific version.

- **Username:** Enter the SSH username to connect to the data source
- **Password:** Enter the SSH password
- **Enable Password:** Re-enter the password

Refer to [CSPC Add-On for Cisco Diagnostic Bridge](#) for CSPC Add-on details.

Schedule Scan

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

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

Scan Schedule

You can schedule to have your devices scanned daily or weekly.
NOTE: The below settings are UTC based.

Daily
 Weekly

12 ▾ 00 ▾ AM ▾

General Settings

This option allows you to set default credentials for all devices. This includes manually added devices and data sources using SSH to perform device information gathering.

Refer to [Setting Same Credentials for Devices](#).



Features

My Diagnostics

The My Diagnostics page displays the total count of:

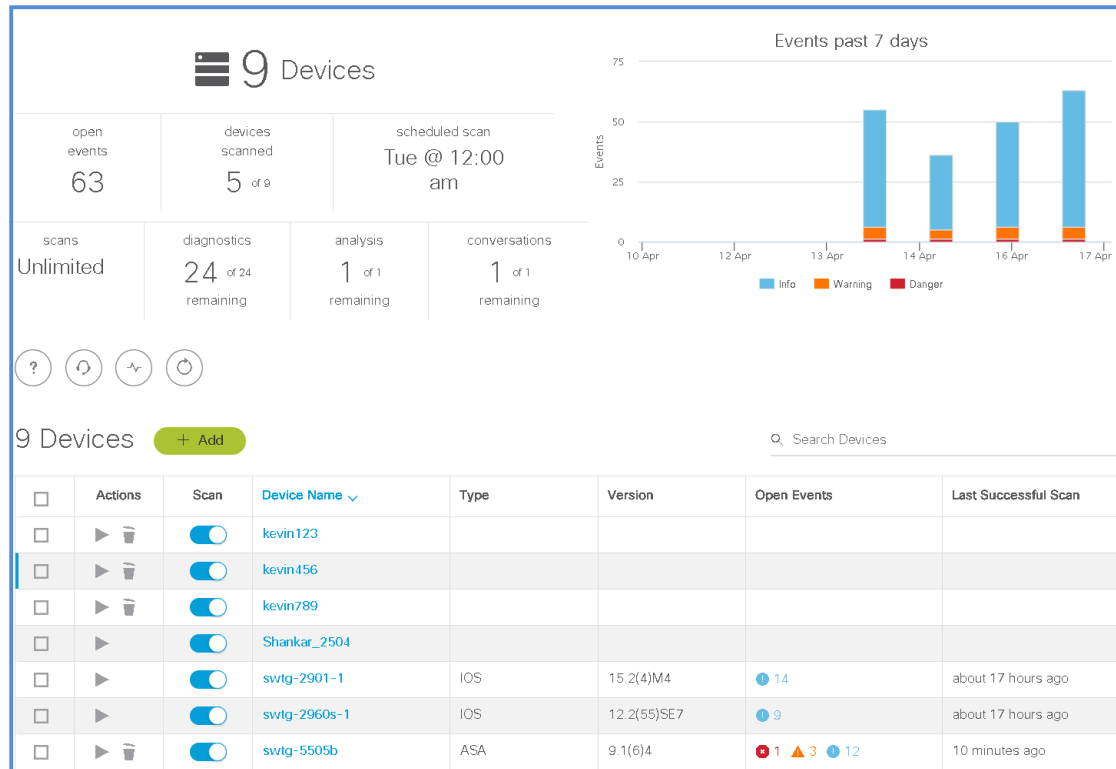
- Open Events
 - Alerts with severity as Information, Warning and Danger
- Total Devices
- Events Resolved

The screenshot shows the Cisco My Diagnostics interface. At the top left is the Cisco logo and the page title 'My Diagnostics'. The user 'Sindhu Surethran' is logged in, with navigation icons for home, refresh, and help. A main navigation bar contains 'Home', 'Devices', 'Investigations', and 'Settings'. The main content area features a 'Welcome Sindhu' message and a large 'My Diagnostics' title. Below this are three summary cards: '63 Open Events' (with sub-counts of 1 Information, 5 Warning, and 57 Danger), '9 Total Devices', and '2 Events Resolved'. The footer contains links for 'Contacts', 'Feedback', 'Site Map', 'Terms & Conditions', 'Privacy Statement', 'Cookie Policy', and 'Trademarks', along with the Cisco logo and copyright notice: 'Copyright © 2017 Cisco Systems Inc. All rights reserved.'

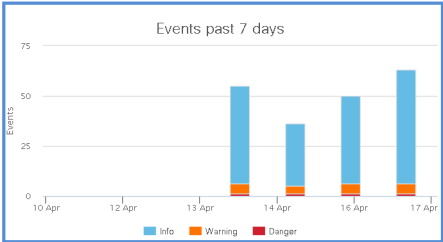
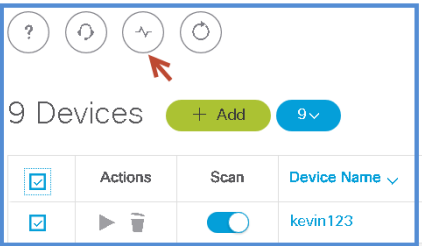
Click on the count to view the events and devices in detail. The *Devices* page appears.

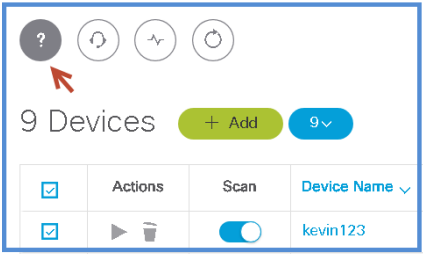
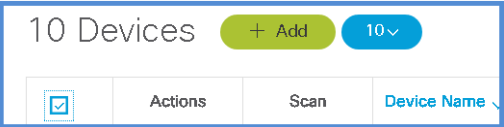
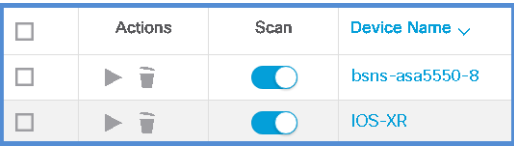

Devices

The Devices tab allows you to add, delete and manage devices. The trend of events is also represented in a graphical manner on the Devices screen.



You can perform the following actions on this screen:

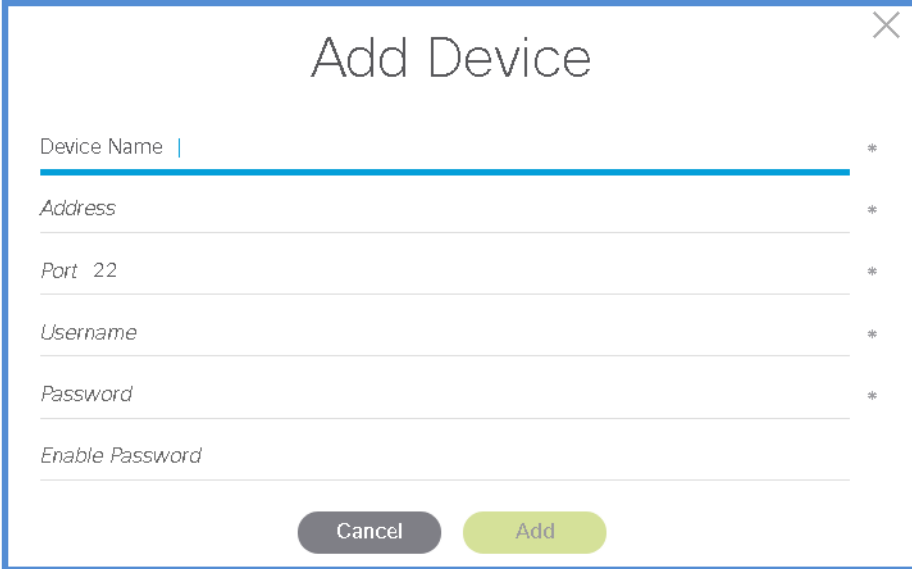
Screen Options	Description
	<p>View the total device count, total number of open events, scanned devices and the scan schedule</p>
	<p>View the trend of event details based on the severity</p>
	<p>Click this to synchronize the bridge with external data sources to update any new devices to the existing list</p>
	<p>Select a device and click this to open an analysis investigation. Refer to Investigate Devices for more details</p>
	<p>Click this to open a conversation. You can request for an hourly based conversation/phonecall/webEx with a TAC engineer to discuss technology, deployment and so on</p> <p>Note This option is only available to Premium customer who have purchased TAC Add on Level 2.</p>

Screen Options	Description
	<p>Click here to request for application support or submit a feedback</p>
	<p>Click Add button to add devices manually. The selected device count appears on top of the device list table. Refer to section Add Devices Manually for more details</p>
	<p>Click the play icon to start scanning a device instantly</p> <p>Click the bin icon to delete a device</p> <p>Click the toggle button to enable or disable the scheduled scan for a device</p> <p>Refer to the section Scan Devices for more details</p>
	<p>Click this to search any specific device</p>

Add Devices Manually

You can add devices manually to check the diagnostics before adding the data sources. To add devices manually, perform the following:

1. In the My Diagnostics Interface, click the **Devices** tab, and click the **Add** button. The Add Device window appears.



The screenshot shows a modal dialog box titled "Add Device". It contains the following fields and controls:

- Device Name**: A text input field with an asterisk (*) on the right.
- Address**: A text input field with an asterisk (*) on the right.
- Port**: A dropdown menu showing "22" with an asterisk (*) on the right.
- Username**: A text input field with an asterisk (*) on the right.
- Password**: A text input field with an asterisk (*) on the right.
- Enable Password**: A text input field with an asterisk (*) on the right.
- Buttons**: "Cancel" (grey) and "Add" (green) buttons at the bottom center.

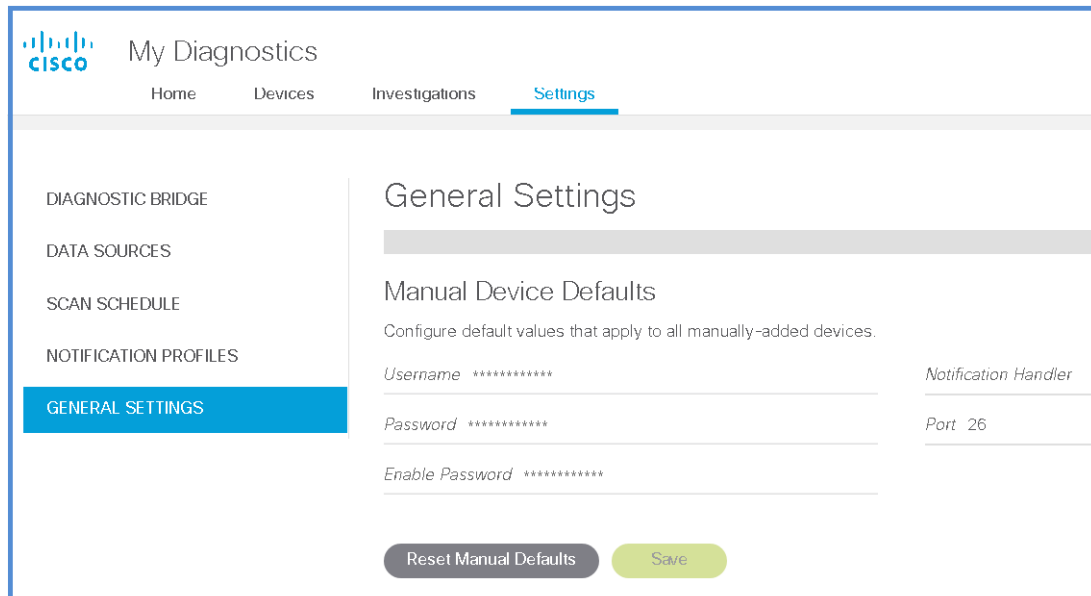
2. Enter a name for the device in the Device Name field.
3. Enter the IP address in the Address field.
4. Select the Port number using the up and down arrow.
5. Enter the Username and Password in order to connect to the device.
6. Click Add. The device is added to the Devices list.

Setting Same Credentials for Devices

You can set default password for the device list.

Complete the steps below to set the password for all the devices added manually.

1. In the Settings tab, click General Settings.



2. Enter the Username and Password. Select the Notification Handler and click **Save**. You can choose to reset the password using the Reset Manual Defaults button.

Scan Devices

After scheduling the scan on the Settings tab, the devices will be scanned periodically for the scheduled day and time. You can run the scan for a device instantly using the play icon available for each device on the Devices page. Click the toggle button to enable or disable the scan. The scan will run for all the devices that are enabled for scan.



Note

The play button (scan now) is not available for basic customers.

Investigate Devices

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 will be available on the Investigations page.



Note

This option is available only for Premium customers.

You can investigate a device from the Devices page or from the Individual device details page. The list of investigations requested by you appear under the Investigations tab.

Complete the steps below to investigate a device:

1. Select the device from the Devices page and click on the Open an Analysis Investigation on the selected device icon. The *Add Serial Number window* appears.

2. Enter the Serial Number and click Continue. The *Open Analysis Request* window appears.

3. Select the Resolution date, Sub-Technology and enter a Description. Click **Submit** to submit the request.
4. All the investigations you requested will appear under the Investigations tab.

Case	Affected Device(s)	Type	Status	Events	Created	Updated	Published
680019894	swtg-891a	Analysis	Published	1 2 12	5 days ago	5 days ago	5 days ago

1-1 of 1 | << < > >>

- Click the Case link to view the case details. The case details page appears.

Investigation Details

680019894

Case [680019894](#) Affected Device(s) [swtg-891a \(FTX16148509\)](#)
 Created April 12th, 2017 09:29:33 PM (5 days ago) show more
 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

15 Events

Filter

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

- Click the Title link to view the information provided by the TAC engineer. It includes Description, Plan, Impact, Output and Comments. You can submit a feedback by clicking on the icon available under Actions.

15 Events

Filter

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#pglid=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. Refer to the figure below.













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

Device Details
mirober2-asav

Serial Number 9APE10XVL4K
Model ASAv
Type ASA
Version 9.7(1)
Last Scheduled Scan about 15 hours ago
Last Successful Scan 3 days ago
Times Scanned 15
Total Health Checks 179

11 Events |  3  6

Actions	Severity	State	Title
 		Open	ARP processing will fail after 213 days of uptime (CSCvd78303)
 		Open	ASA Security Best Practice Recommendation: Unicast RPF Verifica
 		IGNORED	ASAv is not allocated correct resources by the hypervisor
 		Open	ASAv throughput and maximum connections severely limited due t



CSPC Add-On for Cisco Diagnostic Bridge

This chapter details the Installation and usage notes (ptao-1.0.0 Installation/Usage Notes) for the add-on piece, which is installed in the same VM where the CSPC collector is installed. Topic include:

[Requirements](#)

[Code Installation](#)

[My Diagnostic API](#)

Requirements

CSPC host with CSPC 2.6.3.3 is required for Add-on.

Code Installation

1. You require root access to the collector VM.
2. These instructions assume that you have already configured and are running the CSP Collector, v2.6.3.3.
3. Download the version of the add-on from:
https://upload.cisco.com/cgi-bin/swc/fileexg/main.cgi?CONTYPES=Cisco_Diagnostic_Bridge
4. Copy the file, as root, into the collector's VM. This can be placed anywhere on the server:

Example

```
Downloads$ scp ptao-1.0.0.tar.gz root@172.18.204.206:/tmp
Warning private system unauthorized users will be prosecuted.
root@172.18.204.206's password:
ptao-1.0.0.tar.gz
Downloads$      100%   25MB  12.8MB/s   00:01
```

5. Connect to the collector using SSH, as root and shutdown the collector:

Example

```

Downloads % ssh root@172.18.204.206
Warning private system unauthorized users will be prosecuted.
root@172.18.204.206's password:
Warning: your password will expire in 82 days
Last login: Tue Jan 31 19:22:32 2017 from 10.82.238.198
#####
#   This system is hardened and for the use of authorized users only. #
#   Individuals using this computer system without authority, or in #
#   excess of their authority, are subject to having all of their #
#   activities on this system monitored and recorded by system #
#   personnel. #
# #
#   In the course of monitoring individuals improperly using this #
#   system, or in the course of system maintenance, the activities #
#   of authorized users may also be monitored. #
# #
#   Anyone using this system expressly consents to such monitoring #
#   and is advised that if such monitoring reveals possible #
#   evidence of criminal activity, system personnel may provide the #
#   evidence of such monitoring to law enforcement officials. #
#####
[root@swtg-rtp-poc-206 ~]# service cspc stop
Stopping tomcat:
Stopped tomcat:
Stopping Common Services Platform Collector:
Shutting down Base Collector.
    waiting for add-ons to shutdown.....
Shutting down MySQL.. SUCCESS!
nohup: ignoring input and appending output to `nohup.out'
Stopped tomcat service
[root@swtg-rtp-poc-206 ~]#

```

**Note**

The SSH timeout must be set to 40 seconds in CSPC. To set the SSH timeout, go to **Settings > Inventory Settings > Global timeouts**. The default value is 10 seconds.

- Remove any existing ptao installation with the following command:

Example

```

[root@swtg-rtp-poc-206 ~]# rm -rf ${CSPCHOME}/add-ons/ptao
[root@swtg-rtp-poc-206 ~]#

```

- Extract the tar file in the \$CSPCHOME/add-ons directory:

Example

```
[root@swtg-rtp-poc-206 ~]# tar xzf /tmp/ptao-1.0.0.tar.gz -C ${CSPCHOME}/add-ons --warning=no-timestamp
[root@swtg-rtp-poc-206 ~]#
```

8. Open up a port in the firewall for the Diagnostic Bridge to be able to access the add-on's API's.
 - First, shut down iptables with "service iptables stop" as root:



Note The firewall is off at this point.

Example

```
[root@swtg-rtp-poc-206 ~]# service iptables stop
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: Unloading modules: [ OK ]
[root@swtg-rtp-poc-206 ~]#
```

- Manually edit the /etc/sysconfig/iptables file to add the lines shown below referencing port 39386. These lines have to be at the end of the list of other ports that are allowed and before any drop statements.

```

:
:
-A INPUT -p tcp -m tcp --dport 2424 -j ACCEPT
-A INPUT -p udp -m udp --dport 3478 -j ACCEPT
-A INPUT -s 10.1.2.3/32 -p tcp -m tcp --dport 39386 -j ACCEPT
-A INPUT -s 127.0.0.1/32 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.1/32 -d 127.0.0.1/32 -j ACCEPT
-A INPUT -p icmp -j icmp_packets
-A INPUT -j LOG_DROP
:
:
-A OUTPUT -p tcp -m tcp --dport 7337 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 7337 -j ACCEPT
-A OUTPUT -d 10.1.2.3/32 -p tcp -m tcp --dport 39386 -j ACCEPT
-A OUTPUT -d 127.0.0.1/32 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -j ACCEPT
-A OUTPUT -p icmp -j icmp_packets
-A OUTPUT -j LOG_DROP
:
:

```

- Start iptables back up with "service iptables start".

```

[root@swtg-rtp-poc-206 ~]# service iptables start
iptables: Applying firewall rules: [ OK ]

```

9. Restart the collector. The add-on should start up automatically.

Example

```
[root@swtg-rtp-poc-206 ~]# service cspc start
Starting Common Services Platform Collector:
Starting MySQL.... SUCCESS!
Starting Base Collector and add-ons
Starting CSPC server with Java memory as 2200
nohup: ignoring input and appending output to `nohup.out'
Starting tomcat:
Started tomcat:
Started tomcat service
[root@swtg-rtp-poc-206 ~]#
```

My Diagnostic API

The system integrators can look into Cisco Diagnostic Bridge using the following link:

<https://IP Address:5001/swagger/>

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

