CISCO DEVICE INFO USER GUIDE

REQUIREMENTS

Cisco Device Info has been developed using the Microsoft .Net Framework version 4. If not already installed it should be installed prior to Cisco Device Info. Application testing has been carried out on the following platforms:

- Microsoft Windows XP (Service Pack 3);
- Microsoft Windows 7 32 and 64-bit (Service Pack 1);
- Microsoft Windows 8 64-bit;

CISCO EQUIPMENT COMPATIBILITY

Most Cisco IOS routers should work however it is impossible for all possible devices and module configurations to be tested. The following devices and IOS versions have been verified:

Device	Type	Versions
837	Router (IOS)	12.4(5b)
861 - 891	Router (IOS)	12.4(24)T4 15.0(1)M4 15.1* 15.2(3)T
1721	Router (IOS)	12.2(8)YJ 12.4(21)
1760	Router (IOS)	12.3(5f)
1801 - 1861	Router (IOS)	12.4* 15.1(4)M3
1921 - 1941	Router (IOS)	15.0(1)M3 15.1(4)M3 15.2(3)T
2801 - 2851	Router (IOS)	12.4* 14.4(2)T6
2901 - 2951	Router (IOS)	15.1* 15.2(4)M1
2940	Switch (IOS)	12.1(22)EA12
2960	Switch (IOS)	12.2(50)SE5
3550	Switch (IOS)	12.2(25)SED
3560X	Switch (IOS)	12.2(55)SE3
3560V2	Switch (IOS)	12.2(55)SE4
3640[1]	Router (IOS)	12.4(25)
3725 - 3745	Router (IOS)	12.4*
3750	Switch (IOS)	12.2(25)SED1
3750E	Switch (IOS)	12.2(55)SE1
3750G	Switch (IOS)	15.0(1)SE2

Device	Type	Versions
3825 - 3845	Router (IOS)	12.4* 15.1(4)M4
3925 - 3945	Router (IOS)	15.1(3)T4 15.2(3)T1
4506	Switch (IOS)	12.2(46)SG
4912[2]	Switch (CatOS)	8.3(12)GLX
6509[2]	Switch (CatOS)	8.5
6509-E[2]	Switch (CatOS)	8.4(5)
7201	Router (IOS)	12.4(15)T14
7206VXR	Router (IOS)	12.4*
7301	Router (IOS)	12.4(25a)
7606	Router (IOS)	12.2(18)SXF16
7609	Router (IOS)	12.2(33)SRD5
9000	Router (IOS XR)	4.1.0 , 4.2.1
12404	Router (IOS XR)	3.6.0[00]
AP1142N	Aironet AP (IOS)	12.4(25d)JA1
AP802GN	Aironet AP (IOS)	12.4(25d)JAX 15.2(2)JA
AS5350	Router (IOS)	12.4(12)
CSR-8/S	Router (IOS XR)	4.1.2
ME340x	Router (IOS)	12.2(53)SE
UBR7100	Router (IOS)	12.3(17a)BC1
UBR7246VXR	Router (IOS)	12.3(17a)BC2
UBR10012	Router (IOS)	12.2(33)SCD7 12.3(23)BC6

[1] No model number detected

[2] CatOS devices are not currently supported, though mostly work. Interface descriptions may not correctly show port numbers.

ENABLING SNMP ON DEVICES

Before Cisco Device Information can return information on a device it must first have SNMP access enabled. The exact process depends on the security requirements and access to the device.

SNMPv2 is the most commonly deployed protocol version but has inherent security weaknesses. If possible, SNMPv3 should be used.

ENABLING SNMPv2

Enabling SNMPv2 is possible with a single command. It can optionally be restricted further with a standard access list. To enable SNMP access with a read-only community string named "CiscoRocks" the following command should be run in the global configuration mode (conf t);

```
snmp-server community CiscoRocks RO
```

ENABLING SNMPv3

Enabling SNMPv3 requires four commands to be run in the global configuration mode (conf t).

```
snmp-server group <Group Name> v3 auth read <Read-Only View name> write <Read-Write View Name>
snmp-server view <Read-Only View Name> iso included
snmp-server view <Read-Write View Name> iso included
snmp-server user cdi <Group Name> v3 auth <Auth Type> <Auth Passphrase> priv <Priv Type> <Priv Passphrase>
```

For example if it was decided that SNMPv3 using MD5 and AES-128bit should be enabled, the commands may look like the following:

```
snmp-server group V3GROUP v3 auth read V3READ write V3WRITE
snmp-server view V3READ iso included
snmp-server view V3WRITE iso included
snmp-server user cdi V3GROUP v3 auth md5 CiscoRocks priv aes 128 CiscoRocks
```

SNMP VERSION INFORMATION

Whilst SNMP versions 1 and 2 provide authentication, the community string is sent in clear-text from the manager to the agent/device. Under version 3 each message is protected, providing:

- Confidentiality (Encryption to prevent someone reading the data in transit);
- Integrity (Data integrity to prevent the communication being tampered with) and
- Authentication (To verify the person querying the agent/device is authorized to do so);

SNMPv3 is capable of supporting multiple authentication and privacy providers, the following methods have been implemented in Cisco Device Information:

- Authentication (None, MD-5, SHA-1);
- Privacy (None, AES 128bit, DES);

SNMPv1 is supported, but its use is discouraged from both a security and performance point of view. SNMPv1 does not support GetBulk PDU's resulting in significantly slower SNMP communication with devices. SNMPv2 an later resolve such issues.
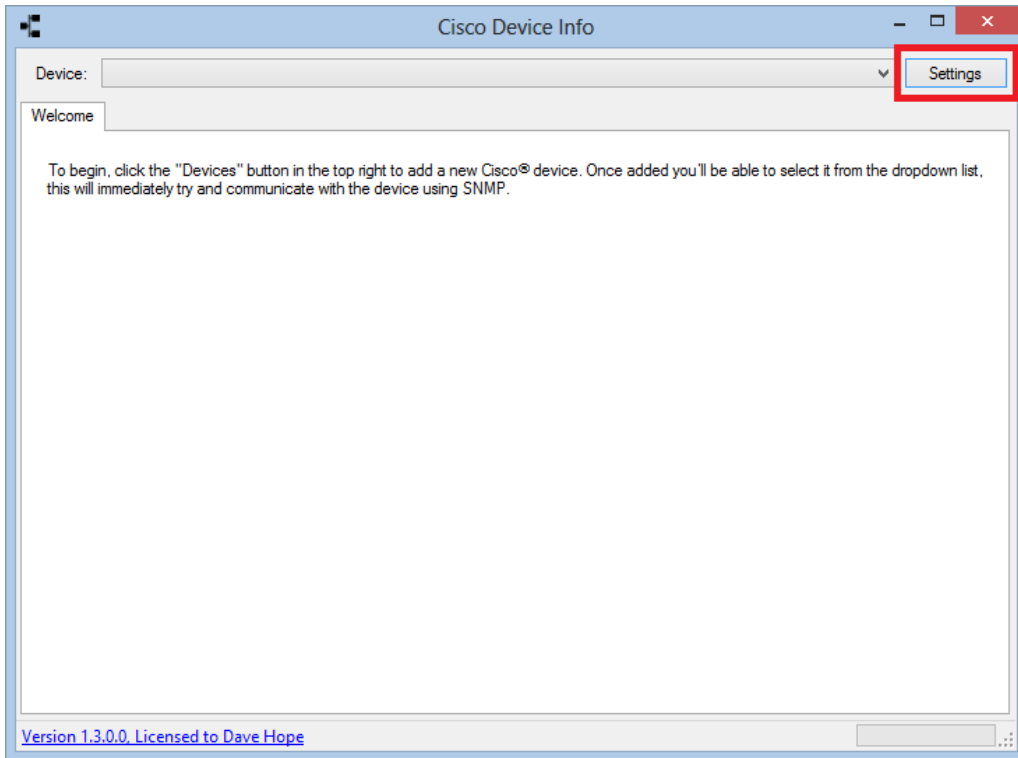
Basic usage

Once installed and run for the first time a device will need to be added to be able to connect.
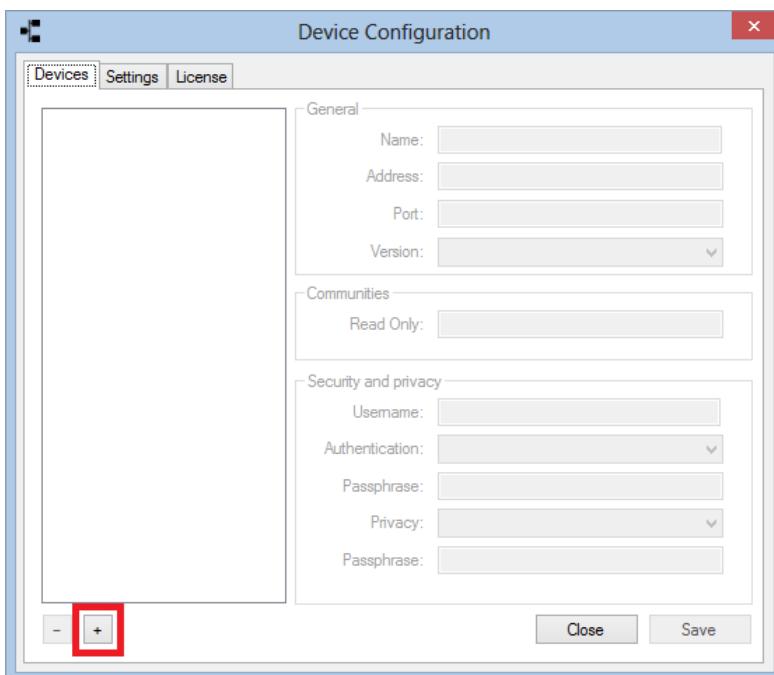
Adding a device

Before a router can be connected to it must be first be added to the list of available devices.

1. To begin, click the "Settings" button in the top right of the application to launch the "Device Configuration" window;


2. Click the "+" button in the lower-left corner of the window to create a new device;

3. On the right hand side, enter the device configuration including Name, Address (or IP), Version and authentication information. Once entered click the "Save" button to store the device and then click the "Close" button to return to the previous screen;

CONNECTING TO A DEVICE AND ACCESSING ITS INFORMATION

Once a device has been added, it can be accessed by selecting it from the dropdown list at the top of the main widow:
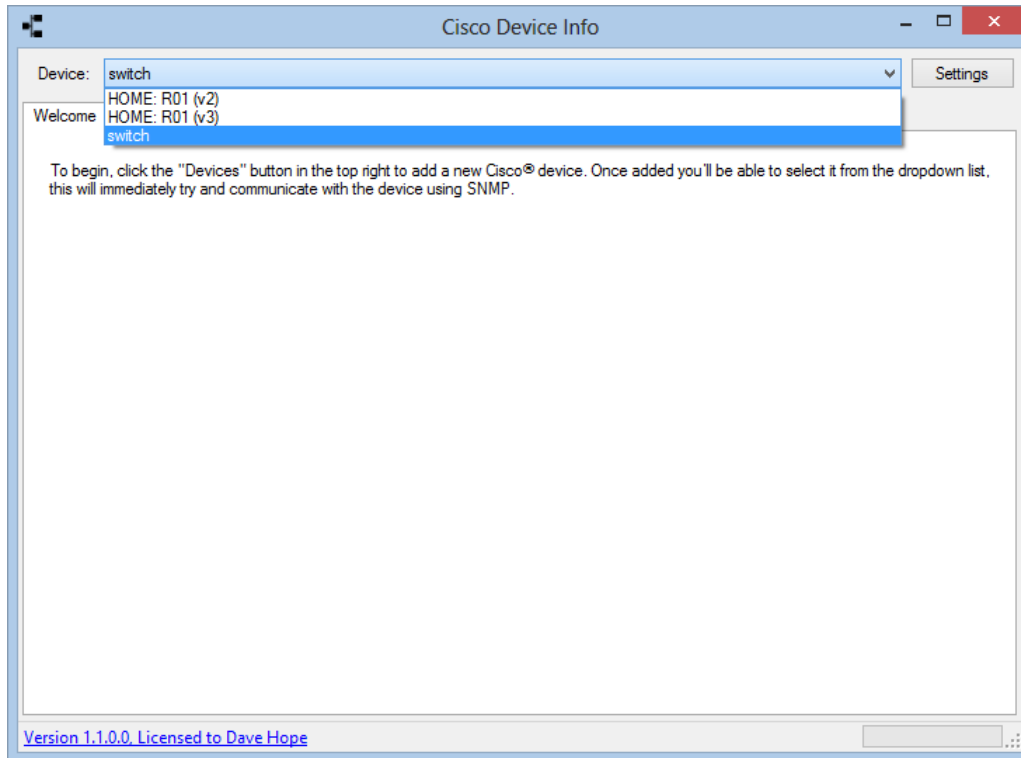
Once selected Cisco Device Information will immediately connect to it and retrieve the following information:

- General information such as hostname, model number, serial number, uptime and IOS version;
- The complete list of interfaces on the device;
- If the device is a member of a stack, the list of devices in the stack and their basic information;
- The ARP cache;
- The routing table;
- A list of all IPSec phase-2 associations;
- A list of all detected CDP (Cisco Discovery Protocol) devices;

Depending on the latency to the device in question, it may take a few seconds for the connection process to complete. This can be monitored using the progress bar in the bottom right corner of the main window.

Once device information has been retrieved a graph will be plotted showing the throughput of any of the following interface types:

- ADSL;
- Ethernet and
- GigabitEthernet;

Graphing of additional interface types will be supported in future releases.

LICENSE INSTALLATION

When purchasing you will have been provided with a file named "License.xml", this is a digitally signed XML document containing the name of the licensed individual or company.

To license the application first save the supplied license file and launch Cisco Device Info;

1. Click the "Settings" button;
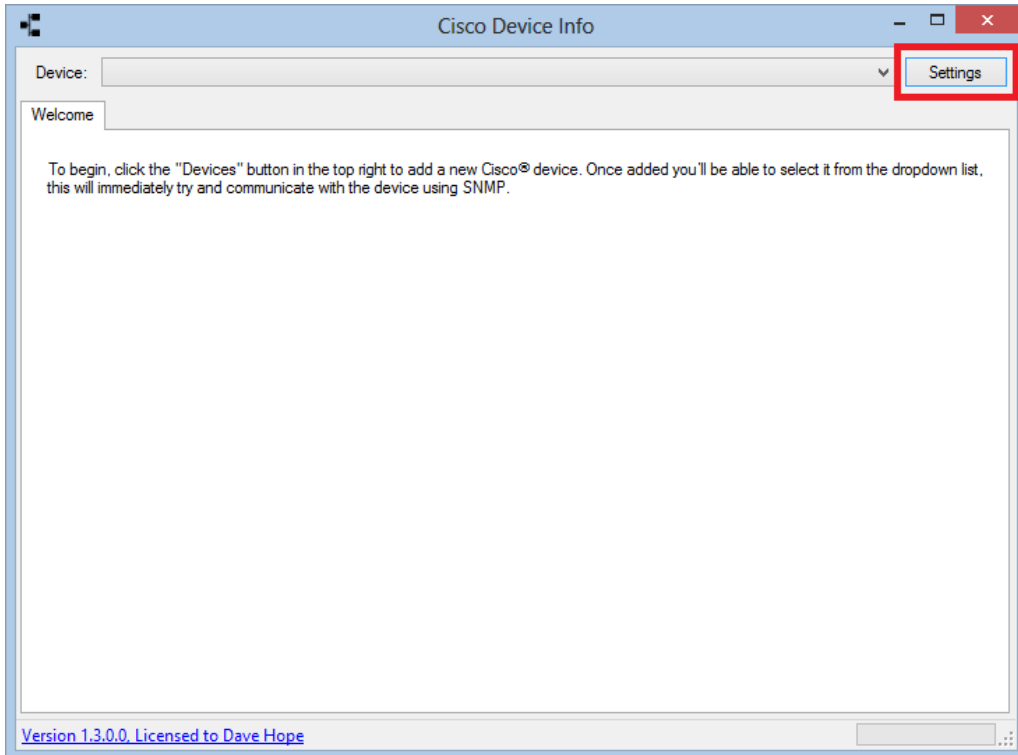
2. Select the "License" tab and then click the "Install License" button;
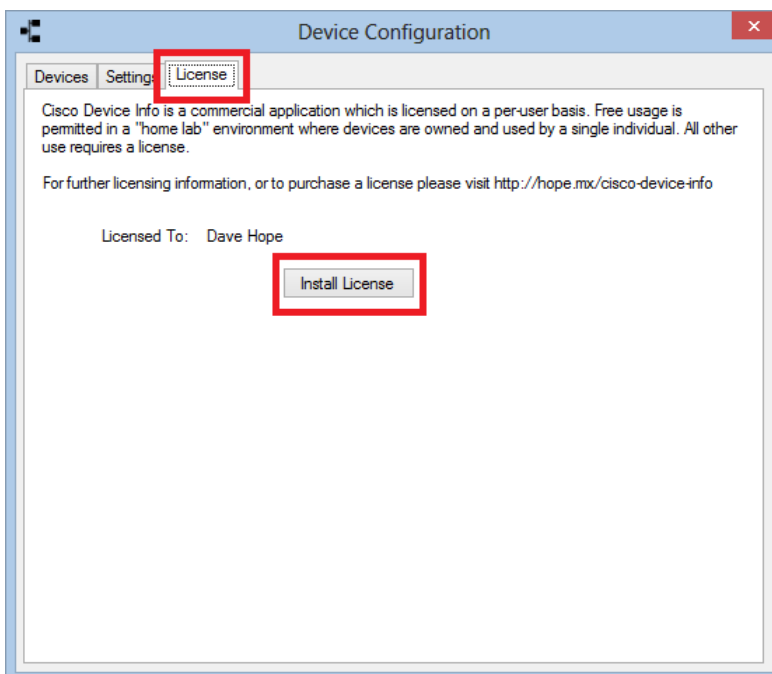
3. When prompted, browse for the license file you have been provided with and click the "Open" button;
4. Close the "Device Configuration" window;
5. Quit and re-open Cisco Device Info.

ADVANCED SETTINGS

Advanced configuration options are available however they should be used with caution.

ENABLING DNS LOOKUPS

By default, the IP addresses of IPSec endpoints will be resolved to DNS addresses to simplify identification of these remote devices.

If a device has a significant number of IPSec tunnels, an equally significant number of DNS queries will be made in an attempt to resolve these IP addresses to their hostnames.

To enable DNS lookups:

1. Click the "Settings" button;
2. Select the "Settings" tab;
3. Tick the "Resolve IP addresses to hostnames" tickbox;
4. Click the "Save" button followed by the "Close" button;

STORING DEVICE SETTINGS IN A CENTRAL LOCATION

In certain environments such as a helpdesk team it may be desirable to store device configuration in a central network location. By default, the configuration file storing device settings is stored in the following location:

`%AppData%\CiscoDeviceInformation\DeviceSettings.dat`

If the settings are to be stored on a network location this file can be copied to the location in advance so that the settings are immediately available. If the file does not already exist it will be created. To change the location of the device configuration information:

1. Click the "Settings" button;
2. Select the "Settings" tab;
3. Tick the "Store device configuration information in a different location" tickbox;
4. Type the address of the new location in the text box below;
5. Click the "Save" button followed by the "Close" button;

INCREASING THE SNMP TIMEOUT

If you have devices in remote locations that are typically slow to respond from the computer running Cisco Device Info, the default timeout can be increased.

1. Click the "Settings" button;
2. Select the "Settings" tab;
3. Tick the "Adjust the timeout for SNMP operations" tickbox;
4. Using the up and down arrows, adjust the timeout value up to a maximum of 30 seconds;
5. Click the "Save" button followed by the "Close" button;

VERSION HISTORY

VERSION 1.3.0
Released on 27th November 2012.

1. Fixed bug where interfaces with speeds greater than 4GB/s were misreported;
2. Fixed bug were user interface could be left in an inconsistent state following a router failing to respond;
3. Enhanced the way additional columns can be shown (Right-Click table headers);
4. Added the name of a chart series on mouse over to the Interface usage chart;
5. Improved error handling experience of interface usage chart following SNMP timeouts due to slow responding, or no longer available devices;
6. Where no data for one tab is available for that device, the tab will be hidden;

VERSION 1.2.0
Released on 16th October 2012.

1. Fixed bug limiting the valid characters in SNMP community strings. Any character can now be used providing the overall SNMP community string is less than 32 characters;
2. Editing of exiting devices is now supported by selecting them, updating their properties and clicking the "Save" button. The user will be prompted before overwriting a device;
3. Added the ability to increase the timeout on SNMP queries via the "Settings" tab;
4. Added the ability to display interface descriptions on newer IOS images. This setting can be enabled on the "Settings" tab;

VERSION 1.1.0
Released on 16th September 2012.

1. Initial release.