Release Notes for Cisco Industrial Network Director, Release 1.2.x

First Published: 2017-07-31

This release note contains the latest information about using Release 1.2.x of the Cisco Industrial Network Director (IND) application that supports configuration and management of Industrial Ethernet switches.

The IND application provides three types of Online Help (OLH): Context-Sensitive Help, Embedded Help such as the Guided Tours, and Tooltips.

Organization

This guide includes the following sections:

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Conventions	Indication
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

About Cisco IND

Cisco Industrial Network Director provides operations teams an easily-integrated system delivering increased operator and technician productivity through streamlined network monitoring and rapid troubleshooting. IND is part of a comprehensive IoT solution from Cisco:

- Easy-to-adopt network management system purpose-built for industrial applications that leverages the full capabilities of the Cisco Industrial Ethernet product family to make the network accessible to non-IT operations personnel.
- Creates a dynamic integrated topology of automation and networking assets using industrial protocol (CIP, PROFINET) discovery to provide a common framework for plant floor and plant IT personnel to monitor and troubleshoot the network and quickly recover from unplanned downtime.
- Rich APIs allow for easy integration of network information into existing industrial asset management systems and allow customers and system integrators to build dashboards customized to meet specific monitoring and accounting needs.

Cisco IND Features and Benefits

- Purpose-built user experience for non-IT operations personnel – Rapid adoption by operations teams for improved productivity.
- Targeted discovery of plant floor network assets customized for industrial environments – Ensures that automation devices connected to the network are not affected by discovery process.
- Automation endpoint discovery using CIP and PROFINET industrial protocols – Complete automation infrastructure inventory, not solely network inventory details.
- Optimized alarm management with real-time alerting of network events and reporting of effects to automation assets – Allows for operations and plant IT team to consume network events in context of the industrial process to simplify troubleshooting issues.
- Real-time monitoring of device metrics, traffic statistics, and network infrastructure status – Increased visibility of network health for the operations team and reduced unplanned downtime.
- Comprehensive RESTful APIs for integration with automation applications and control systems – Rapid adoption and integration with existing systems and customization by system integrators.
- Role-based access control with customizable permission mapping – Restrict system access to authorized users on a per feature basis.
- Detailed audit trails for operational visibility of network changes, additions, and modifications – Record user actions on network devices for change management.

- Search capability integrated with major functions - Easily locate functionality and mine for information.
- Cisco Active Advisor - Free cloud-based service that provides essential network life cycle information to make sure security and product updates are current.
- Guided tours - Step-by-step guidance to maximize productivity and ease adoption.

New Features

In this release of the product, there are four primary functions supported:

- Design
- Operate (Operations)
- Maintain (Maintenance)
- Settings

Note: The Design and Maintenance pages are introduced in this release.

Release 1.2.x supports the following new IND features and enhancements summarized in Table 1.

Table 1 New Features in IND 1.2.x

Feature	Description	First released	Related Documentation
Cisco Wish	Allows you to provide Cisco immediate feedback about an existing IND feature or an idea for a future feature directly from pages within the IND application.	1.2.0-180	IND Online Help
Cisco Active Advisor (CAA)	IE 1000 switches now support CAA, a free cloud-based service that provides network life cycle information to make sure security and product updates are current. You need a Cisco Connection Online (CCO) account to use CCA. Maintain > Cisco Active Advisor	1.2.0-180	IND Online Help
Plug and Play (PnP) Server	Allows you to upload a configuration file in a FreeMarker template format with dynamic variable value substitution. Enables zero touch installs. Design > Plug and Play	1.2.0-180	IND Online Help

Table 1 New Features in IND 1.2.x (continued)

Feature	Description	First released	Related Documentation
Automatic Software Update	Allows the System Administrator or User (with System Settings rights) to: ■ View the current version of IND software installed. The message, “Your IND is up to date!”, displays when you have the latest software installed. ■ Check to see if newer software is available by selecting the **Check Now** button. ■ Download the latest IND software by selecting the **Download** icon. The icon only displays when a newer software version is available. System Update page displays the time that the last check was done. Settings > System Update	1.2.0-180	IND Online Help

Table 1 New Features in IND 1.2.x (continued)

Feature	Description	First released	Related Documentation

SNMPv3 level security	Security level employed to discover and manage devices within IND application.
	Option 1: Configure IE switches (**excluding** IE 1000, Stratix 2500 switches) with the following commands to enable SNMPv3 level security:
	`snmp-server group <yourGroupName> v3 priv`
	`snmp-server user <yourUserName> <yourGroupName> v3 auth [authType] [authPassword] priv [privType] [privPassword]`
	Option 2A: Configure IE 1000, Stratix 2500 switches with the following commands to enable SNMPv3 level security:
	`snmp-server user user1 engine-id 800000090308731baf380 sha encrypted [encrpytedAuthPassword] priv aes encrypted [encrpytedPrivPassword]`
	`snmp-server security-to-group mode1 v3 name userName group yourGroupName`
	`snmp-server access yourGroupName model any level no auth read default_view`
	Note: SNMPv3 username can be up to 32 characters. Authentication and privacy passwords must be between 8 and 245 characters.
	Option 2B: Device Manager configuration to create Access Profile required for discovery and management of IE 1000 and Stratix 2500 switches:
	1. Log in to the IE 1000 Device Manager. Choose **Admin > Users**.
	2. Create Device Access User and use the same in Access Profile on IND.
	3. Configure SNMP community string for Read Only (ro):
	a. Choose **Configure > SNMP.** Click **OK**.
	b. Check box to enable SNMP Mode globally. Click **Submit**.
	4. Select Community Strings tab. Add a public Community String with read only access. By default, this is a Read Only (ro) string. *For SNMPv3:*
	a. Select Users tab. Add SNMPv3 user (name, security level, authentication protocol, authentication password, privacy protocol, and privacy password). Click **OK**.
	b. Select Group tab and select the created user, and specify the group name. Click **OK**.
	5. Choose **Admin > Access Management**. Check box for either enableSSH or Telnet. (Option determines how the IE 1000 communicates with IND). Click **Submit**.
		1.2.0-180	IND Online Help

Table 1 New Features in IND 1.2.x (continued)

Feature	Description	First released	Related Documentation
Topology enhancements	■ SNMP used to retrieve the MAC address for all managed devices during discovery. ■ New Service API used to initiate IP Scan Discovery for Plug and Play Server feature.	1.2.0-180	IND Online Help
Localization	■ Application user interface and Online help support the following four languages in addition to English: French, German, Japanese, Spanish. **Note:** Retrieved data displays in English only.	1.2.0-180	IND Online Help
IND Device Pack 1.2.0	**Note:** PnP process fails with 152-5.E2 image (CSCvf42798). Cisco Universal IOS images supported: ■ Cisco IOS Release 15.2(5)E1 ■ Cisco IOS Release 15.2(4)EC2(ED) ■ Cisco IOS Release 15.2(4)EA2 ■ Cisco IOS Release 15.2(4)EA1 ■ Cisco IOS Release 15.2(3)E3 ■ Cisco IOS Release 15.2(3)E2 The device pack supports the following Cisco and Rockwell Automation/Allen-Bradley platforms: Cisco platforms: ■ CGS 2520 ■ IE 1000, IE 2000, IE 2000U **Note:** IND only supports PROFINET clients on IE 1000. ■ IE 3000, IE 3010 ■ IE 4000, IE 4010 ■ IE 5000 Rockwell Automation/Allen-Bradley platforms: ■ Stratix 8000/8300 Modular Managed Ethernet Switches ■ Stratix 5700 Industrial Managed Ethernet Switches ■ Stratix 5700 Industrial Ethernet Switches ■ Stratix 5410 Industrial Distribution Switches ■ Stratix 5400 Industrial Ethernet Switches ■ Stratix 2500 Lightly Managed Switches	1.2.0-180	IND Online Help

IND Licenses

The Cisco Industrial Network Director is licensed on a per-device, term subscription basis and supports two licensing models. For details on the supported IND licenses, refer to the:

Cisco Industrial Network Director Data Sheet

System Requirements

Table 2 System Requirements

Desktop Requirements	Minimum Requirement
Windows Operating System (OS) English language only	Windows 7 Enterprise or Professional with Service Pack 2 Windows 10
Browser	Chrome: Version 50.0.2661.102 or later Firefox: Version 46.01 or later
CPU	Dual Core 2.4Ghz
RAM	8 GB
Storage	50 GB

Pre-Configuration Requirements for IE Switches

The following information describes the CLI configuration required for IND to discover a Supported Device and transition the device from NEW to MANAGED state and NEW to MANAGED state in secure mode.

- For IE switches running Cisco IOS, refer to Requirements for ALL IE Switches Running Cisco IOS
- For IE1000 switches, refer to Device Manager Configuration Required for IE1000 Switches

Requirements for ALL IE Switches Running Cisco IOS

- Configuration Required for Discovery
- Configuration Required for NEW to MANAGED State
- Configuration Required for NEW to MANAGED State in Secure Mode

Note: After entering the *Configuration Required for Discovery* steps, you will enter **only one** of the NEW to MANAGED State configurations referenced above: NEW to MANAGED State *or* NEW to MANAGED State.

Configuration Required for Discovery

The following configuration must be configured on the Supported Device for the system to successfully discover it:

```
# Configure SNMP server
# The <read-community> and <write-community> must match the SNMP V2 Read and Write strings
 defined in the system Access Profile which is attached to the Discovery Profile.
snmp-server community <read-community> RO
snmp-server community <write-community> RW
```

Note: After entering the *Configuration Required for Discovery* steps above, you will enter **only one** of the NEW to MANAGED State configurations referenced below:

- NEW to MANAGED State *or*
- NEW to MANAGED State in Secure mode

Configuration Required for NEW to MANAGED State

The following configuration must be configured on the Supported Device for the system to successfully transition the Supported Device from NEW to MANAGED administrative state.

```
# Configure user account with privilege level 15
# This should match the device access username and password specified in the system Access Profile
username <username> privilege 15 password 0 <password>

# Configure AAA
aaa new-model
aaa authentication login default local
aaa authorization exec default local

# Configure HTTP server
ip http server
ip http authentication aaa login-authentication default

# Configure VTY
line vty 0 4
exec-timeout 0 0
login authentication default
transport input all
transport output all
line vty 5 15
exec-timeout 0 0
login authentication default
transport input all
transport output all
```

Configuration Required for NEW to MANAGED State in Secure Mode

The following configuration must be configured on the Supported Device for the system to successfully transition the Supported Device from NEW to MANAGED administrative state in Secure mode:

```
# Configure user account with privilege level 15
# This should match the device access username & password specified in the system Access
Profile
username <username> privilege 15 password 0 <password>

# Configure AAA
aaa new-model
aaa authentication login default local
aaa authorization exec default local

# Configure HTTPS server
ip http secure-server
ip http authentication aaa login-authentication default
ip http secure-ciphersuite aes-256-cbc-sha

# Configure VTY
line vty 0 4
exec-timeout 0 0
login authentication default
transport input all
transport output all
line vty 5 15
exec-timeout 0 0
```

```
login authentication default
transport input all
transport output all
```

Device Manager Configuration Required for IE1000 Switches

1. Login to the IE1000 Device Manager.
2. Leave the username field blank and enter **cisco** as password.
3. Choose **Admin > Users**.
4. Create Device Access User and use the same in Access Profile on IND.
5. Configure SNMP community string for Read Only (ro):
   a. Choose **Configure > SNMP**. Click **OK** in the pop-up windows to confirm enabling SNMP.
   b. Check the check box to enable SNMP Mode globally. Click **Submit**
6. Select Community Strings tab. Add a *public* Community String read only access. (By default, this is a Read Only (ro) string)
7. Choose **Admin > Access Management**.
   a. Check the check box to enable either SSH or Telnet. (This option determines how the IE1000 communicates with IND)
   b. Click **Submit**.

Installation Notes

IND Application Installation

The installation procedure for IND is described in the Installation Guide for Industrial Network Director for Release 1.2.x.

Device Pack Installation

Installation Requirements

IND Device Packs can only be installed with an IND application that has a matching *version* number, and the *release number* **must be** the same or greater than the IND release number.

For example, in release 1.2.0-180, 1.2.0 is the version number and 180 is the release number.

A new Device Pack must be version 1.2.0 and the release must be 180 or higher.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.2.x.

Important Notes

Please note the following information about Cisco IOS software and PID support on IND.

Unsupported PIDs

The following IE 2000 PIDs are not supported by IND 1.1.x and are not supported by IND 1.1.0-x Device Packs:

- IE-2000-4TS-G-B-U
- IE-2000-8TC-G-B-U
- IE-2000-16TC-G-E-U

Supported Cisco IOS Software

IND 1.2.x supports the following Cisco IOS Releases:

- Cisco IOS Release 15.2(5)E1
- Cisco IOS Release 15.2(5)E
- Cisco IOS 15.2(4)EC2(ED)
- Cisco IOS Release 15.2(4)EA5
- Cisco IOS Release 15.2(4)EA2
- Cisco IOS Release 15.2(4)EA1
- Cisco IOS Release 15.2(3)E3
- Cisco IOS Release 15.2(3)E2
- Release 1.6 for Industrial Ethernet 1000

Supported IND Release Upgrades

You can perform the following IND 1.x upgrades:

- Upgrade from 1.1.x to 1.2.0
- Upgrade from 1.0.x to 1.2.0

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with IoT IND. These are known limitations that will not be fixed, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the software.

- **CSCvb24719**

  Symptom: Tasks are an asynchronous way to execute certain operations in IND. When we take a backup of the database, that backup action itself is a task and is in a RUNNING state. So, when we restore the database and startup all the tasks which were in a RUNNING state, they will be moved to FAILED.

  Conditions: During the time when we do a backup, there can be some other operations simultaneously running as a task other than the backup task itself.

Workaround: There is no workaround for this issue. But this does not impact any feature or functionality. It is expected that when we backup we are reverting to an older revision of the application and hence some tasks might have failed as you cannot re-create that operation at the current time.

- **CSCvc78199**

  Note: This caveat is applicable only when upgrading to IND 1.2.x from IND versions 1.0.1 to 1.1.x and above.

  Symptom: IE-5000-12S12P-10G - Metric data refresh fails for the Managed Device after IND upgrade to 1.1.0

  Conditions: Upon upgrading the IND from 1.0.1 to 1.1.x. This happens only if the device CLI output gets changed and those devices are in managed state of IND. Issue seen with IE-5000-12S12P-10G Cisco IOS Release (15.2(5)E or higher) IOS image.

  Workaround: Manually move the device to decommission state and move back to managed state or delete the device from the IND and discover it again.

- **CSCvd24673**

  Symptom: When the system is upgraded to 1.1 image, the saved topology will be lost. The view will be auto-layout. All the devices and groups will be auto arranged.

  Conditions: IND System is upgraded from 1.0.1 to 1.1.x and above.

  Workaround: The user has to re-arrange the topology and save the layout again.

Caveats

This section presents open caveats in this release and information on using the Bug Search Tool to view details on those caveats.

- Open Caveats, page 11
- Accessing the Bug Search Tool, page 12

Open Caveats

No open caveats.

Resolved Caveats

List below represents caveats from IND 1.1.x resolved in this release, IND 1.2.x.

- **CSCvd24709**

  Symptom: Some devices in the DB shows up as unknown devices on the connected grid of its connected neighbors. Hence, a link to the device is not available at the following places:

  - Connected Grid
  - Affected Devices
  - Dashboard Port traffic utilization widget

  Conditions: When the thread running neighbor queries finish faster than the thread updating local if table, the port on the local ifTable is not matched. Hence the topology service categorizes this device as unknown device instead of mapping the device ID 5a11.

Workaround: Re-triggering topology might solve this as it is a multi-threading/timing issue.

- **CSCvd24726**

  Symptom: When a scheduled weekly backup is deleted, it shows the scheduled day to be one day ahead of the actual schedule. Logs show the day to be incorrect as well.

  Conditions: Occurs when a weekly scheduled backup is deleted.

  Workaround: This issue is resolved in Release 1.2.0.

Accessing the Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access the Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, use the following URL: https://tools.cisco.com/bugsearch/search

To search using a specific bug ID, use the following URL: https://tools.cisco.com/bugsearch/bug/*<BUGID>*

Related Documentation

Installation Guide for Industrial Network Director Application for Release 1.2.x at:

http://www.cisco.com/c/en/us/support/cloud-systems-management/industrial-network-director/tsd-products-support-series-home.html

Find documentation for the Cisco Industrial Ethernet Switches at: (select the link for the relevant switch to access user guide)

http://www.cisco.com/c/en/us/products/switches/industrial-ethernet-switches/index.html