Release Notes for Cisco Industrial Network Director, Release 1.1.x

Last Updated: 2017-05-09

First Published: 2017-02-23

This release note contains the latest information about using Release 1.1.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.

Conventions	Indication
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[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 two primary functions supported: Operations (Operate) and Settings.

Release 1.1.x supports all the IND features summarized in Table 1.

Table 1 New Features in IND 1.1.x

Feature	Description	First released	Related Documentation
Discovery enhancements	■ Ability to identify different network devices that support SNMP including access points, LAN controllers, firewall devices, routers and servers. ■ CIP device discovery allows retrieval of the MAC address attribute from CIP devices.	1.1.1-49	IND Online Help
Topology enhancements	■ User can view topology information for unsupported SNMP devices. ■ Ability to discover Layer 2 Topologies for MAC address lookup.	1.1.1-49	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.	1.1.1-49	IND Online Help

Table 1 New Features in IND 1.1.x (continued)

Feature	Description	First released	Related Documentation
IND Device Pack 1.1.0	IE 1000 is now supported by the IND application with the new device pack: ■ IE-1000-4T1T-LM ■ IE-1000-6T2T-LM ■ IE-1000-4P2S-LM ■ IE-1000-8P2S-LM **Note:** IND only supports PROFINET clients on IE 1000. Additional IE4010 system support added: ■ IE4010-4S24P ■ IE4010-16S124P **Note:** Above IE4010 PIDs support these Cisco Universal IOS images: ■ Cisco IOS Release 15.2(5)E ■ 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 2000, IE 2000U ■ 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	1.1.0	IND Online Help

Table 1 New Features in IND 1.1.x (continued)

Feature	Description	First released	Related Documentation
Simplified Pre-Configuration Steps for Managed Devices	Minimizes User configuration required to ready an IE switch for management by IND.	1.1.0	See Pre-Configuration Requirements for IE Switches section in these release notes
Login Enhancements	■ When you do not enter a username during login, an error message displays. ■ When you enter the wrong credentials during a Telnet session, an error message displays. ■ A User account must be reset by a System Admin after ten consecutive incorrect login attempts. ■ IND automatically generates a boot strap configuration, whether or not an aaa new-model is present.	1.1.0	IND Online Help
Group Dashboard	Provides a summary view of devices within a Group. You can save the Dashboard for the currently selected group as the default.	1.1.0	IND Online Help
Group Management	All devices must be assigned to a Group. By default, the IND application assigns a device to the *default Root Group* in the absence of another Group assignment. (Operate > Dashboard) Additionally: ■ Users can create Groups and manually assign devices to those groups, ■ Users have the option to assign a Supported Device to a Group during Discovery, ■ During Client Discovery, all clients and unknown devices are assigned to the Group of the connected switch.	1.1.0	IND Online Help
Group-Tree-View display	A Groups-Tree-View displays within the left pane for the following pages: ■ Operate > Dashboard, Operate > Topology ■ Settings > Group Management	1.1.0	IND Online Help
PROFINET IO support	The following data items will be retrieved from PROFINET Clients using PROFINET IO: ■ Vendor ID, Order ID, Serial Number ■ Hardware Revision, Software Revision ■ Interface and Module Version ■ Chassis Slot (submodule) ■ Revision Counter ■ Profile ID, Profile Specific Type	1.1.0	IND Online Help

Table 1 New Features in IND 1.1.x (continued)

Feature	Description	First released	Related Documentation
New Device Terminology and Definitions within the Application	■ Supported Device replaces the term Managed Device. ■ Client Device: Devices accessed through CIP and PROFINET device types into IND device type. Examples devices include Controller and I/O. ■ Group Support in Topology: On the topology page: – Users can view devices under different groups. – Users can navigate to each group and view devices under the group and its subgroups. – Topology views can be saved at the root group level for a given user. – Users can expand or collapse devices under a group and view alarm count for a group. ■ Other: Any discovered devices that are not recognized as a Supported Device or Client Device.	1.1.0	IND Online Help
Operate	You can review or perform the following actions on the **Operate** page: ■ Alarms: Open or close an alarm, view alarm details, assign an alarm to someone, add notes to the alarm (Operate > Alarms) ■ Asset Discovery: Search assets by IP Scan or Link Layer. Assets include Industrial Ethernet (IE) switches and clients that connect to IE switches (Operate > Asset Discovery) ■ Audit Trails: See a listing of all operations performed by users. Each entry includes the following information: timestamps, operation, device IP address, status, username, user IP address and details (description of the entry). (Operate > Dashboard). ■ Inventory: View all devices found from a scan of the network by the application. This page is the default opening page of the IND application. (Operate > Dashboard) ■ Tasks: Review information on tasks that are actively running or have completed. (Operate > Tasks) ■ Topology: View a full network topology map of all devices and neighbors discovered by a scan of the network. Group-Tree-View for groups displays in the left-pane for this page. (Operate > Topology)	1.0.0	IND Online Help

Table 1 New Features in IND 1.1.x (continued)

Feature	Description	First released	Related Documentation
Settings	You can view information or perform the following actions on the **Settings** page: ■ Access Profiles: Create and manage access credentials used by devices and discovery profiles. (Settings > Access Profiles), This item was formerly referred to as Network Profiles ■ Active Sessions: View information on all active sessions, which includes: user ID, login, last accessed, IP address. (Settings > Active Sessions) ■ Alarm Settings: View categories of alarms available on the system and the number of alarms in each category as well as disable/enable alarms and change alarm severity. (Settings > Alarm Settings) ■ Backup: Schedule backups or initiate on-demand backups. (Settings > Backup) ■ Device Pack: Allows you to add support for new device types to the system. (Settings > Device Pack) ■ Group Management: Create groups and assign devices to those groups. (Settings > Group Management) ■ Licenses: Manage Smart and Classic IND Licenses and their details and status. (Settings > Licenses) ■ Password Policies: Eight password policies are defined by default on the system. You can enable or disable any of the policies or the values of those policies. (Settings > Password Policies) ■ System Settings: Modify system settings for data retention, data collection, Cisco Active Advisor and log levels. (Settings > System Settings) ■ User Accounts: Add new user accounts including assigning user role (Network Administrator, Operator, System Administrator) and view existing users defined for the system. ■ User Roles: Three roles are predefined on the system: – Network Administrator: User with this role has permissions to manage network resources. – Operator: User with this role has permissions to monitor the network. – System Administrator: User with this role has all available permissions on the system.	1.0.0	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 1.1.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 1.1.1-49. 1.1.1 is the version number and 49 is the release number.

A new Device Pack must be version 1.1.1 and the release must be 49 or higher.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.1.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 1.1.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 (with some limitations as noted below):

- If you upgrade from IND 1.0.1-3 to 1.1.x, please see Open Caveats associated with the release upgrade (CSCvc78199, CSCvd24673).
- If you upgrade from any IND 1.0.x or 1.1.x release to 1.1.1-49:
  - CIP devices need to be rediscovered to collect MAC address (This item is part of Discover enhancements.)
  - Other/Unknown devices need to be rediscovered to identify these devices more accurately. (This item is part of Discover enhancements.)

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.

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

- **CSCvc78199**

  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.

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

- **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: There is no workaround.

Resolved Caveats

- **CSCvb31945**

  Symptom: The health metrics and bandwidth utilization charts are not available on IE-5000-12S12P-10G for Cisco IOS Release15.2(5)E.

  Conditions: System IE 5000, PID IE-5000-12S12P-10G, had Cisco IOS Release15.2(5)E release installed.

  Workaround: This issue is resolved in Release 1.1.0.

- **CSCvb38948**

  Symptom: In the Asset Discovery page, an Export of Discovery Profile entries to a CSV file results in a missing value. The discovery profile Type column is not populated in the CSV.

  In the VLANs section of the Forwarding tab of the Network Device Details page, an Export of VLANs entries to a CSV file results in an incorrect column formatting in the CSV file. Multiple values in the single “Switch Port Names” column are exported to multiple columns in the CSV file.

  Conditions: A Discovery Profile is of two types: IP Scan or Link Layer. This is populated in the Type column in the Asset Discovery page. An export of Discovery profile entries to CSV results in a missing value in the Type column of the CSV file.

  When a network device is moved to the Managed state, clicking on the device name in the Inventory page gives the Network Device Details page. The Forwarding tab has a VLANs column. If the “Switch Port Names” column has multiple values, then an export of VLANs to CSV gives an incorrect column formatting in the CSV file. The multiple values are formatted into multiple columns.

  Workaround: This issue is resolved in Release 1.1.0.

- **CSCvb41219**

  Symptom: The following links are broken under certain conditions:

  1. On the Device detail page, Connected Devices grid - links in Source Port and Port columns

  2. On Client Detail - link in Connected To field

  3. On topology, when a link between two connected devices is clicked - Port name link

  Conditions: Perform the following operations:

  1. Discover a device that has clients and network neighbors

  2. Discover topology

  3. Move the device to Decommissioned

  Workaround: This issue is resolved in Release 1.1.0.

- **CSCvb41224**

  Symptom: When multiple ports are in Admin State down and half-duplex mode, and a device is either moved to managed or an On demand refresh is triggered or during metrics poller run, there is only one event generated against one of the ports.

Conditions: When multiple ports are in Admin State down and half-duplex mode, and a device is either moved to managed or an On demand refresh is triggered or during metrics poller run, there is only one event generated against one of the ports instead of an alarm each for every port.

Workaround: This issue is resolved in Release 1.1.0.

- **CSCvb43029**

  Symptom: The affected devices in the alarm detail page shows client device links for devices that have been moved into the *Other* category. These links lead to an empty or misleading client detail page.

  Conditions: There are two conditions:

  1) The affected devices in the alarm detail page shows client device links for devices that have been moved into the *Other* category, or for client devices that have been deleted. These links lead to an empty or misleading client detail page.

  2) An alarm is generated where a client device becomes an affected device. Then, the client device is deleted.

  Workaround: This issue is resolved in Release 1.1.0.

- **CSCvd84224**

  Symptom: Sometimes, some of the Japanese characters translated to "???" if installed in Windows with English locale.

  Conditions: The Japanese version of IND should be installed in the Japanese locale of Windows.

  Workaround: This issue is resolved in Release 1.1.0.

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 1.1.x at:

http://www.cisco.com/c/en/us/products/cloud-systems-management/industrial-network-director/index.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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

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.

Related Documentation