Release Notes for Industrial Network Director, Release 1.11.x

First Published: 2021-12-15

Last Modified: 2023-04-12

Overview

These release notes contain the latest information about using Releases 1.11.0, Release 1.11.1, Release 1.11.2, and Release 1.11.3 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: Context-Sensitive Help, Embedded Help such as the Guided Tours, and Tooltips.

Note IND Release 1.11.0 supports English, French, German, Japanese and Spanish Online Help.

IND Release 1.11.1 supports English Online Help.

IND Release 1.11.2 supports English, French, German, Japanese and Spanish Online Help.

IND Release 1.11.3 supports English, French, German, Japanese and Spanish Online Help.

The installation procedure for IND is described in Installation Guide for Industrial Network Director for Release 1.11.x.

About Cisco IND

Cisco Industrial Network Director provides operations teams in industrial networks an easily-integrated management system that delivers 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 (BACnet/IP, CIP, Modbus, PROFINET, OPC UA) 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.
- Integration with existing systems and customization by system integrators.

- User Management 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.
- Guided tours - Step-by-step guidance to maximize productivity and ease adoption.

New Platform and Features Supported

These Release Notes summarize the new features found within the four primary functions supported by IND 1.11.x and its user interface:

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

The IND 1.11.x Online Help contains information for the following new features:

Table 1: New Features in IND 1.11.0

Feature	Description	Related Documentation
Parallel Redundancy Protocol (PRP) Monitoring Phase 2: Additional Alarm Support	PRP provides hitless redundancy for zero recovery time after failures by supporting two Gigabit Ethernet network interfaces connected to two independent, disjointed, parallel networks: LAN A and LAN B. The PRP channel serves as a logical interface that aggregates the two Gigabit Ethernet interfaces into a single link. The end nodes implement the redundancy. You can set the threshold for Last Seen A and Last Seen B Alarms. PRP Phase 2 provides the following additional Alarm Support: • Mismatch in received packets between LAN-A and LAN-B (Minor). • Wrong packets on LAN-A (Minor) • Wrong packets on LAN-B (Minor) • Last seen on LAN-A Exceeded Threshold (Minor) • Last seen on LAN-B Exceeded Threshold (Minor) Operate > Alarms	IND 1.11 Online Help

Feature	Description	Related Documentation
Parallel Redundancy Protocol (PRP) Monitoring Phase 2: Device Details	The following new tables and graphs have been added to the Inventory > Device Details page: • The Statistics table shows PRP statistics for port A and port B of the selected channel. You can also display historical values for LAN A and LAN B Wrong Count and Network Fault Count in the multi-line chart. • Statistics: Duplicate Discard or Accept, Transparent Reception (remove/pass RCT), Revision, Max Instance. Number of Instance Inventory > Device Details	IND 1.11 Online Help
Parallel Redundancy Protocol (PRP) Phase 2: Topology Overlay Enhancements	The following enhancements are added in this release: • Differentiation between LAN-A and LAN-B Devices: The border of the badges are now color-coded and a Role attribute within the existing API response will be used to differentiate between LAN-A and LAN-B devices. If the same device is identified within the network to be in both LAN-A and LAN-B, two separate badges will be displayed for the device within LAN-A and LAN-B. • Color-coded status will be assigned to all LAN-A and LAN-B devices based on their PRP channel interface status. If an interface is down, it is considered a 'Bad' status and will be assigned a red badge. A green badge indicates an 'OK' status. • VLAN Overlay: This option appears when you select the 'Show PRP Node Details' option drop down from the PRP Layer drop-down. When you select a VLAN ID all the nodes that are members of that VLAN will be highlighted in a different color. Additionally, VLAN Overlay will highlight those nodes and links to neighbors that are not part of the PRP network topology. Operate > Inventory	IND 1.11 Online Help
Network Address Translation (NAT) Lookup Table	The NAT lookup table allows the IND application to translate a private IP address to a public IP address. The NAT table displays the information in the following order: Network Range, Endpoint Private, and Endpoint Public. Operate > Discovery > NAT Lookup Table	IND 1.11 Online Help

Table 2: New Features in IND 1.11.1

Feature	Description	Related Documentation
Device Replacement	Whenever IND receives a linkup trap from a switch, it proceeds to discover the neighboring device that is connected to the switch. Before discovery or when adding a device to its inventory, IND checks if there is an existing device with the same IP address, MAC address, or serial number. If there is one, IND does not perform discovery, or it fails to add the device to its inventory. If you have an existing device that is faulty, you might want to replace the device with another device in the network. Previously, you had to manually delete the existing device and add a new device. Now, IND will autonomously replace a device by deleting the existing device in its inventory and adding a new device when certain conditions are met. If you are upgrading to 1.11.2, it is mandatory to initiate a topology discovery manually before proceeding to do device replacements. To trigger topology discovery manually, navigate to the Topology page (**Operate** > **Topology** and click on **Discover Topology**. Operate > Discovery > Device Replacement	IND 1.11.1 and IND 1.11.2 Online Help

Table 3: New Features in IND 1.11.3

Feature	Description	Related Documentation
Install Boot Mode Support for IE3x00	IND supports the Install Boot mode of software image installation for IE3x00 devices along with the Bundle Boot mode, which was already supported. The software boot mode affects how the software image is booted on the device: • Bundle mode is the direct booting of an image. • Install mode allows booting with the packages.conf file, rather than the image itself. The Device Details page displays the current Software Boot Mode configured on the device. You can select the Software Boot Mode when you install a software image on the device from the Device Details page or Software Images page. Operate > Inventory > Device Details Maintain > Software Images	IND 1.11.3 Online Help

System Requirements

Table 4: System Requirements

Desktop Requirements	Minimum Requirements
Windows Operating System (OS)	• Windows 10 • Windows 2012 R2 Server • Windows Server 2016 • Windows Server 2019 R2
Browser	Chrome: Version 50.0.2661.75, 53.0.2785.116, or above Firefox: 55.0.3, 57.04, 63.0.3, or above
CPU	Quad-Core 1.8 GHz
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.

- For IE switches running Cisco IOS, refer to Prerequisite Configuration Required for ALL IE Switches Running Cisco IOS, on page 5.
- For IE1000 switches, refer to Configuration Required for Discovery and Management of Cisco IOS, on page 5.

Prerequisite Configuration Required for ALL IE Switches Running Cisco IOS

The following information describes the CLI configuration required for the system to discover a Licensed device and to transition the device from an Unlicensed to Licensed State.

This section also describes the Device Manager configuration required on IE 1000 switches.

Note A local account is not needed on the device if TACACS is available.

Configuration Required for Discovery and Management of Cisco IOS

Follow these steps to configure the switch so that IND can discover the device and transition from UNLICENSED to LICENSED state.

Procedure

Step 1 Enter global configuration mode:

configure terminal

Step 2 Configure SNMP to allow the system to successfully discover the device:

snmp-server community read-community ro

read-community must match the SNMPv2 read string defined in the system Access Profile that is attached to the Discovery Profile. the default read community string is “public”.

Step 3 Enter the following command to allow the system to discover a Licensed Device and transition the device from a UNLICENSED to LICENSED state with SNMPv3. The group that you create and the mode are used to associate with the SNMPv3 user that you configure in the next step. Based on the mode that you choose for the group, you can configure the authentication privacy protocols and passwords for the user.

snmp-server group group_name v3 mode

where mode is one of the following:

priv: Enables Data Encryption Standard (DES) packet encryption

auth: Enables the Message Digest (MD5) and the Secure Hash Algorithm (SHA) packet authentication

noauth: Enables the noAuthNoPriv security level. This is the default if no-keyword is specified.

Step 4 Add a new user to the SNMP group:

snmp-server user user_name group_name v3 [auth authentication_type authentication_password [priv privacy_type privacy_password]

Note Passwords for auth or priv should not exceed 64 characters.

— auth: Specifies an authentication level setting session that can be either the HMAC-MD5-96 (md5) or the HMAC-SHA-96 (sha) authentication level and requires a password sting auth_password. Supported privacy_type values are: {aes | 128 | des}

— priv: Configured a private (priv) encryption algorithm and password string privacy-password

Step 5 Configure the following for the system to successfully transition the device from UNLICENSED to LICENSED state.This should match the device access username and password specified in the system Access Profile.

username username privilege 15 password 0 password

Step 6 Enter the following commands to configure authentication, authorization and accounting (AAA):

aaa new-model

aaa authentication login default local

aaa authorization exec default local

Step 7 Configure the Secure Shell (SSH) server:

ip ssh version 2

Step 8 Configure the HTTP/HTTPS server:

ip http server

ip http secure-server

ip http authentication aaa login-authentication default

Step 9 Configure the number of Telnet sessions (times) and a Telnet password for the line or lines:

line vty 0 15

login authentication default

transport input all

transport output all

Step 10 Return to privileged EXEC mode:

end

Device Manager Configuration Required for Discovery and Management of IE 1000 Switches

Procedure

Step 1 Log in to the IE1000 Device Manager.

Step 2 Leave the username field blank and enter cisco as password.

Step 3 Choose Admin > Users.

Step 4 Create Device Access User and use the same in Access Profile on IND.

Step 5 Configure SNMP community string for Read Only (ro):

a) a. Choose Configure > SNMP. Click OK in the pop-up windows to confirm enabling SNMP.
b) b. Check the check box to enable SNMP Mode globally. Click Submit

Step 6 Select Community Strings tab. Add a public Community String read only access. (By default, this is a Read Only (ro) string)

For SNMPv3:

a) Select the Users tab and add an snmpv3 user with name, security level, authentication protocol, authentication password, privacy protocol, and privacy password. Click OK.
b) Select the Group tab, select the created user, and specify the group name. Click OK.

Step 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.

Bootstrap Configuration for IE Switches

The system pushes the following configuration when you move the device to the Licensed state in the system:

Note In the configuration script below, the {certificate key length} is obtained from the device access profile.

```
# Secure-mode only
# If the device has a self-signed certificate with RSA key pair length <{certificate-key-length}.The
certificate key length is obtained from the device access profile.\ (or) if the device does not have a
self-signed certificate in nvram
crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR
modulus <{certificate-key-length}>
crypto pki trustpoint IND_HTTP_CERT_KEYPAIR
enrollment selfsigned
subject-name OU=”IOT”
rsakeypair IND_HTTPS_CERT_KEYPAIR
hash sha256
crypto pki enroll IND_HTTPS_CERT_KEYPAIR
# Enable SCP server
# Used for transferring ODM file from the system to device
# For insecure mode the system uses FTP to transfer ODM file
ip scp server enable
# If AAA is not enabled on the device
ip http authentication local
#Secure mode only
ip http secure-server
ip http secure-port {secure-mode-access-port}
#Insecure mode only
ip http server
ip http port {regular-mode-access-port}
# Configure WSMA
# The system uses WSMA for management
wsma agent exec
profile exec
# Secure-mode only
wsma profile listener exec
transport https path /wsma/exec
```

```
# Insecure mode only
wsma profile listener exec
transport http path /wsma/exec
# SNMP configuration
# Trap destination. The system supports both v2c and v3
snmp-server host <ind-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp-server host {ind-ip-address} version 3 {snmpv3_mode} {snmpv3_username} udp-port 30162
# Bootstrap configuration for SNMPv3
# The system needs the following configuration to be able to query bridge-mib with SNMPv3
security in IOS devices.
# This bridge-mib is required by inventory service to get MAC-Table from SNMP when the
system moves device from new to managed state.
snmp-server group {group_name} v3 {snmpv3_mode} context vlan- match prefix
# Enable RFC2233 compliant for linkDown and linkUp trap
snmp-server trap link ietf
# Enable traps supported by the system
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rep
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps alarms informational
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
# Configure SNMP to retain ifindex across reboots
snmp ifmib ifindex persist
# Enable dual-power supply
# Not applicable for S5410, IE5K, CGS2K, IE3010
power-supply dual
```

```
# Enable SD card alarm
# Not applicable for S8000,CGS2K,IE2000U,IE3010,IE3K,IE3200,IE3300,IE34000 and S5800
alarm facility sd-card enable
alarm facility sd-card notifies
# Turn on notifies for selected facility alarms
alarm facility temperature primary notifies
alarm facility temperature secondary notifies
# Following not application for CGS2K, IE3010
alarm facility power-supply notifies
no alarm facility power-supply disable
```

Bootstrap Configuration for IE 1000 Switches

```
# Traps for IE1K
snmp.config.trap_source.add coldStart
snmp.config.trap_source.add warmStart
snmp.config.trap_source.add linkDown
snmp.config.trap_source.add linkUp
snmp.config.trap_source.add topologyChange
snmp.config.trap_source.add authenticationFailure
snmp.config.trap_source.add entConfigChange
snmp.config.trap_source.add fallingAlarm
snmp.config.trap_source.add risingAlarm
snmp.config.trap_source.add newRoot
# Trap destination
snmp.config.trap_receiver.add <ind-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp.config.trap_receiver.add {ind-ip-address} version 3 {snmpv3_mode} {snmpv3_username}
udp-port 30162
```

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.

- IND upgrades managed devices in groups of six (6). This approach is by design to ensure server resources are not overloaded.

- Make sure that the Windows server running IND is not abruptly shutdown as this might lead to a loss of files needed for IND to function.
- State transition for the devices newly discovered running a Cisco IOS Release lower than 15.2(7)E1a cannot be moved from the Unlicensed state to Licensed State in the secure mode. Metrics collection for the devices already managed by IND running a Cisco IOS Release lower that 15.2(7)E1a would fail due to self-signed certificate expiry in the secure mode. Telnet should work without any issues on a switch that is running a software version lower than 15.2(7)E1a.
- If your switch is running Cisco IOS Release 15.2(4) software, a weak cipher must be used for secure communication to the device. Weak Ciphers are disabled by default on IND. To enable, go to Settings > System Settings > Security Settings.
- Device Image upgrade in IND: An image upgrade will not be supported for devices with low memory and no SD flash support, if the device is managed on IND in secure mode. Please use Device Manager to upgrade the image.
- SNMPv3 protocol doesn't work in device IE3x00 running with 16.10.1.
- PnP process is supported only on single-homed (Single IP) IND servers for Cisco IOS Release 15.2(6)E1.

Note A PnP Service Error 1410 occurs in Cisco IOS Release 15.2(6)E0a due to the AAA command not working. (CSCvg64039). Caveat currently marked Unreproducible in CDETs. Note: This issue is resolved in software releases greater than Cisco IOS 15.2(6)E0a.

- IE 5000: Horizontal Stacking is not supported. Stacked devices can be discovered on IND but cannot be licensed.
- IOS devices should have sufficient space in flash directory for upgrading the devices from IND using software image upgrade. For low memory devices, use the removable SD flash memory card.
- PRP or MRP capable devices discovered in previous versions of IND will not support PRP or MRP after upgrading to IND 1.10. The device must be re-discovered on IND 1.10 to enable PRP or MRP support.
- When performing On Demand discovery of a network consisting of Backplane Devices and Switches that have Redundancy Ethernet Protocol (REP) enabled in them, do not select ‘Discover Related Devices’ in the Discovery Profile. It will lead to modules in the Backplane Devices to be added as duplicate devices.
- When either “Show PRP Node Details” or “Show PRP Node Connections” is selected from the PRP overlay drop-down, a text “OK” (with a green border) or “Bad” (with a red border) will be added to the badges (labels) of all of the LAN-A and LAN-B devices depending on the status of the PRP channel to which the node is participating. If there are multiple devices conflicting with their status of LAN A/B, IND will default to a “Good” (with a green border) state.
- A PRP channel with both participating interfaces down will not report any LAN-A/LAN-B devices that are part of it. Hence, IND will not consider the PRP channel with both participating interfaces down for deriving the status of LAN-A/LAN-B devices.
- IND will not be able to detect and collect DLR information accurately from devices where the DLR rings are not configured in order (for instance, configuring DLR ring 2 without configuring DLR ring 1). This limitation applies when managing switches where configuration of multiple DLR rings is possible.

  To overcome this limitation, configure the rings in order on the switch and then refresh the device in IND.

You can use the following command to configure a dummy DLR ring with default values:

```
Switch(config)# dlr ring <Ring number>
```

- IND supports IE3x00 devices running software versions through Cisco IOS XE 17.9.x only.
- Cisco Connection Online (CCO) and Device Pack pages are removed from IND.
- If a backup task fails with a message "Backup failed. Database backup failed for database [ind]", do the following for the backup to succeed:

  1. Increase the timeout for the database dump to be taken by adding a property with name backup.pgdump.time.out.ms in the file application.properties under (Installation folder)\programData\conf. The value should be in milliseconds and greater than the default value 300000, which is 5 minutes.

     For example, to set the timeout to 15 minutes add the following in application.properties:

     ```
     backup.pgdump.time.out.ms=900000
     ```

  2. Restart the IND service.

Note It is recommended to back up application.properties before editing. Do not delete any other properties in the file.

- After upgrade of IND, Software Boot Mode is not shown. Click **Retrieve Device Data** to manually refresh the device, or wait for Basic Inventory Poller to run (the default is 24 hours) and collect this information.
- If a backup is restored on a different machine other than the one from which the backup was taken, the common name in the self-signed certificates will not match the hostname of the machine where the backup is restored. This can cause SSH connections to fail between IND and other external applications such as PxGrid. This issue is seen when using self-signed certificates only and not CA signed certificates.

Caveats

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

Open Caveats

Table 5: IND 1.11.x Open Caveats

Bug ID	Headline
CSCwc38751	MRP ring information is not showing after the platform change in MRP license info in IE3x00.

Closed Caveats

There are no known closed caveats.

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 1.11.0

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

- Cisco Industrial Ethernet 1000 Series Switches
- Cisco Industrial Ethernet 4000 Series Switches
- Cisco Industrial Ethernet 4010 Series Switches
- Cisco Industrial Ethernet 5000 Series Switches