Release Notes for Cisco Industrial Network Director, Release 1.7.x

First Published: 2019-08-09

Last Updated: 2019-09-25

These release notes contains the latest information about using Release 1.7.0 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.

Note: IND Release 1.7.0 Online help is **only available in the English language**.

In IND 1.7.1, the following additional language support will be available: French, German, Japanese, and Spanish-Latin America.

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.
[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 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.
- 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 Platform and Features Supported

These Release Notes summarize the new features found within the four primary functions supported by IND:

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

Release 1.7.0 supports the following new IND features and enhancements summarized in Table 1.

Table 1 New Platforms and Features Supported in IND 1.7.0

Feature	Description	Related Documentation
Cisco Catalyst IE3400 Rugged Series Switches	IND now manages the following Industrial Ethernet systems using SNMPv2 and supports the following MIBs (CDP, LLDP, and VTP): IE-3400-8FT-MC IE-3400-16FT-MC IE-3400-24FT-MC	Cisco Catalyst IE3400 Rugged Series IND Online Help

Table 1 New Platforms and Features Supported in IND 1.7.0

Feature	Description	Related Documentation
Delete User: Personal Information Protection	**Local Users** with RBAC permissions **can** delete users under the following condition: ■ User is disabled Local Users with RBAC permissions **cannot** delete users when the following conditions exist: ■ An Assigned state alarm is assigned to the user ■ A Closed state alarm is assigned to the user. However, once you reassign the alarm to another user, you can delete the user. Additional considerations: When you delete a local user, you must also delete the preferences for that user in the following areas of the IND application: Topology and Dashboard preferences and Email Subscription settings. **External Remote Users** ■ Last Login now exists for all remote users to support automatic pruning of users, when their last login is greater than 180 days **except** in cases where an alarm is assigned to that remote user. Additional considerations: When an alarm is in a closed state, you must remove the alarm assignment from the remote user, as well as delete all Topology and Dashboard preferences and email subscription settings.	IND Online Help
User Profile Page	A new User Profile Page consolidates the following two actions for users: ■ Change Password and Email address update ■ Subscribe for email alerts for IND generated alarms To access the User Profile page, do the following: At the User Icon (top-right) of IND page, click Profile Settings	IND Online Help
Certificate Page	You can now add, delete, and assign certificates to different services (pxGrid, PnP/Web UI, OPC UA) in this page. By default, all the services are mapped to a self-signed certificate. Settings > Certificate Management	IND Online Help

Table 1 New Platforms and Features Supported in IND 1.7.0

Feature	Description	Related Documentation
Certificate for SSH/SCP/HTTPs and OPC UA	In the Device Access Profile page, IND has an option to select either a self-signed or a CA-signed device certificate for SSH/SCP/HTTPs. Similarly, you can assign the certificate for OPC UA, if the Security' & Security Policy setting is not as 'NONE'. Settings > Certificate Management	IND Online Help
Allow Software Updates for Stratix 5700 (Rockwell Automation, Allen-Bradley) Switches with Limited On-Board Flash Memory	New command option, **archive download-sw override** {**ftp |https**} allows software image installation when an onboard memory limitation exists on the Stratix 5700. Maintain > Software Images Operate > Inventory > Device > Details	IND Online Help Stratix 5700
OPERATE menu changes		
New look and feel to Operate > Topology page and icons that support Page views, Search field and Legend bar	New page design includes: ■ Groups search field (upper-left hand corner of page) that determines what Groups display in the Left tree). For example, if you search by DLR or PTP it will display only those Groups related to those items. ■ Tool bar at top of page: Layer, Refresh, Save and Discover Topology ■ Search by Device Name, IP or Type (upper-right hand search field) to display panel with details for that system and highlight related icons and links in bold blue in network topology (center of page) ■ New icons support these actions (lower-right-hand side of page): – Display Full Screen or Minimize (double-headed arrow) – Zoom in (+) and Zoom Out (-) – Legend (i) These items were formerly seen in the upper-left hand corner of the page. ■ New Menu Bar appears above the network diagram, at the top right of the page with the following options: Layer, Refresh, Save and Discover Topology Operate > Topology	IND Online Help

Table 1 New Platforms and Features Supported in IND 1.7.0

Feature	Description	Related Documentation
Precision Time Protocol (PTP) support	PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead. PTP is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. The following PTP related information is collected on IND: ■ PTP local clock, Master clock and Grandmaster clocks. ■ PTP port states ■ PTP mode, domain and system time For licensed devices, when the Grandmaster is licensed, the PTP timing distribution tree is available on the Topology page as a layer on top of physical topology. The following alarms are generated when there are changes in the PTP domain that affect the system time of a device ■ Grandmaster changed – This alarm will help identify Grandmaster changes and the affected devices in the PTP domain ■ Steps removed from grandmaster changed – This alarm helps identify if the number of hops from the grandmaster has increased, thereby changing latency. ■ Grandmaster not found – This alarm occurs on a device when it is not getting system time from another entity. Supported devices: ■ All Devices supporting CIP Object 43 ■ All Devices supporting CISCO-PTP-MIB Operate > Alarm Settings > Time Services Operate > Inventory Operate > Topology	Precision Time Protocol Software Configuration Guide for IE 4000, IE 4010, and IE 5000 Switches IND Online Help

Table 1 New Platforms and Features Supported in IND 1.7.0

Feature	Description	Related Documentation
Asset Discovery Enhancement: Discover Related Devices Toggle	When you enable the Discover Related Devices toggle, the following occurs: ■ When an IP Scan discovers a device, it also discovers all of its neighbors. ■ When Link-Layer Discovery performs, the hop count of the neighbors discovered, will be one higher than the specified hop count ■ When a scan discovers an enabled DLR device (node or supervisor), then all the DLR ring members will also be discovered. **Note:** The toggle options are Yes or No. The default setting is No. Operate > Discovery	IND Online Help
DLR Alarm Support	DLR Alarms are generated for licensed DLR Active Supervisors when a fault occurs on the DLR ring. This alarm is generated after every metrics status poller cycle. The following alarms are supported: ■ DLR Partial Network Fault ■ DLR Rapid Fault Restore Cycle ■ DLR Ring Fault ■ DLR Unexpected Loop Detected	IND Online Help
SETTINGS menu change		
CCO User Account Delete Option	You can delete a CCO User Account within IND. You **cannot** delete the CCO User account when a Software download is in progress.	IND Online Help
SMTP Settings Page	A new SMTP Settings Page allows you to: ■ Add a Primary and an optional Secondary server. ■ Test server settings by generating a test email You will need to define the hostname or IP address, username and password on both a Primary and Secondary SMTP Server. SMTP server setup allows IND to send users email alerts for alarms. SMTP > System Settings	IND Online Help
MAINTAIN menu changes		
Configuration Archive Updates page	Updates to the look and feel of the Configuration Archives page. (No operational changes)	IND Online Help

Table 1 New Platforms and Features Supported in IND 1.7.0

Feature	Description	Related Documentation
IND Device Pack 1.7	■ Cisco Releases 1.6, 1.7, 1.8 (IE 1000 only) Cisco Universal IOS images supported: ■ Cisco IOS Release 15.2(7)E ■ Cisco IOS Release 15.2(6)E2A, Cisco IOS Release 15.2(6)E2, Cisco IOS Release 15.2(6)E1, Cisco IOS Release 15.2(6)E0a ■ Cisco IOS Release 15.2(5)E2,Cisco IOS Release 15.2(5)E1, Cisco IOS Release 15.2(5)E ■ Cisco IOS Release 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 Cisco Universal IOS XE images supported: ■ Cisco IOS 16.10 XE, Cisco IOS 16.11a XE **Note:** See Limitations and Restrictions, page 14 for image limitations. The device pack supports the following Cisco and Rockwell Automation/Allen-Bradley platforms: ■ Cisco IOS platforms supported: CGS 2520, IE 2000, IE 2000U, IE 3000, IE 3010, IE 4000, IE 4010 and IE 5000 ■ Cisco IOS XE platforms supported: IE3200, IE 3300, IE 3400	IND Online Help
IND Device Pack 1.7, continued	Rockwell Automation/Allen-Bradley platforms: ■ Stratix 8000/8300 Modular Managed Ethernet Switches ■ Stratix 5800 Industrial Managed Ethernet Switches ■ Stratix 5400 and 5700 Industrial Ethernet Switches ■ Stratix 5410 Industrial Distribution Switches ■ Stratix 2500 Lightly Managed Switches	

IND Licenses and PIDs

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 and PIDs for ordering purposes, refer to the: Cisco Industrial Network Director Data Sheet.

System Requirements

Table 2 System Requirements

Desktop Requirements	Minimum Requirement
Windows Operating System (OS)	Windows 7 Enterprise or Professional with Service Pack 2 Windows 10 Windows 2012 R2 Server Windows 2016 Server (64-bit version)
Browser	Chrome: Version 50.0.2661.75, 53.0.2785.116 or above Firefox: 55.0.3, 57.0.4, 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 and transition the device from UNLICENSED to LICENSED state in secure mode.

- For IE switches running Cisco IOS, refer to Prerequisite Configuration Required for ALL IE Switches Running Cisco IOS
- For IE1000 switches, refer to Device Manager Configuration Required for Discovery and Management of IE 1000 Switches

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

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.

1. Enter global configuration mode:

   configure terminal

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”.

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 configured 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.

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*

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*

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

7. Configure the Secure Shell (SSH) server:

   ip ssh version 2

8. Configure the HTTP/HTTPS server:

   ip http server

   ip http secure-server

   ip http authentication aaa login-authentication default

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

10. Return to privileged EXEC mode:

    end

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

1. Login to the IE 1000 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)

   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.
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
```

Installation Notes

IND Application Installation

Update link

The installation procedure for IND is described in the Installation Guide for Industrial Network Director for Release 1.7.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 1.7.x, 1.7 is the version number and x is the release number.

A new Device Pack must be version 1.7.0 and the release must be 0 value or higher.

Installation Steps

For Device Pack installation steps, refer to the Installation Guide for Cisco Industrial Network Director, Release 1.7.x.

Important Notes

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

Supported IND Release Upgrades

You can perform the following IND upgrades:

- Upgrade from 1.6.1 to 1.7.x
- Upgrade from 1.5.x to 1.6.x
- Upgrade from 1.4.x to 1.5.1
- Upgrade from 1.4.x to 1.5.0
- Upgrade from 1.3.1 to 1.4.0
- Upgrade from 1.3.0 to 1.3.1
- Upgrade from 1.2.x to 1.3.0
- 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.

- 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 AAA command not working (CSCvg64039)-Caveat currently marked Unreproduceable in CDETs.
- IE 5000: Horizontal Stacking is not supported. Stacked devices can be discovered on IND but cannot be licensed.
- PTP Limitations:
  - **PTP Support limitation for Cisco IE/Rockwell Stratix devices without CIP**: Because of platform bugs noted in Table 5 on page 15, PTP is supported only for Clock Mode as Boundary Clock with PTP Profile as Default Profile if CIP is not enabled on the management interface and PTP information is collected over SNMP. IND will show that PTP is disabled if switch clock type is anything other than Boundary Clock with PTP Profile as Default Profile.
  - PTP capable devices discovered In IND 1.6 will not support PTP after upgrade to IND 1.7. Device has to be re-discovered on IND 1.7 to enable PTP support.
  - IE2000, IE3200, IE3300 and IE3400 do not support CISCO-PTP-MIB for supported PIDs. For these PIDs, PTP is only supported over CIP.

Caveats

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

Resolved Caveats

Table 3 IND 1.7.1 Resolved Caveats

Bug ID	Headline
CSCvp78350	Show running config output processing error
CSCvq24142	MAC address is not being collected for IOS devices for some devices

Open Caveats

Table 4 displays open caveats for IND 1.7.0

Table 5 displays open caveats for Industrial Ethernet switches that may affect the functionality of IND 1.7.x.

Table 4 IND 1.7.0 Open Caveats

Bug ID	Headline
CSCvp78350	Show running config output processing error

Table 5 Platform-related Open Caveats

Bug ID	Headline
CSCvm36711	IE1000 devices do not return hostname in PnP work response.
CSCvq00721	CISCO-PTP-MIB supports only default PTP profile. (Platforms: IE4000, IE5000, IE4010, IE2000U)
CSCvq22373	entPhysicalSoftwareRev doesn't return the software
CSCvq23714	IE1k PnP fails with CA signed certificate

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://bst.cloudapps.cisco.com/bugsearch/?referring_site=shp

Related Documentation

Installation Guide for Industrial Network Director Application for Release 1.7.x

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