Feature History 4.7.x

This chapter summarizes the new and modified features that are included in this release and tells you where they are documented in the User Guide.

- What's New in 4.7.x, on page 2

What's New in 4.7.x

Features	Description	First IoT FND Release Support	Related Document or Section
Enhanced Tunnel Reprovisioning and DHCP Addresses	The Tunnel Provisioning workflow has been modified so that DHCP addresses are released during decommissioning of the Field Area Router (FAR) device rather than during Tunnel Provisioning. To improve Tunnel Provisioning, we have introduced a new property: `optimizeTunnelProv` By default, tunnel creation and deletion will lock the Head-end Router (HER). However, if the optimizeTunnelProv property is set to 'true' either through CSV or cgms.properties, then tunnel creation and deletion will not lock the HER during the operation. **Note** Configuring the optimizeTunnelProv property in CSV is done at the Device level and configuring cgms.properties is done at the Global level. This change applies to the management of the following Cisco IOS and Cisco IOS XE Routers: • Connected Grid Routers: CGR1120 and CGR1240 • Cisco Industrial Integrated Services Routers: IR800 (IR807, IR809, and IR829) • Cisco 5900 Series Embedded Services Routers (ESR 5900) • Cisco SBR (C5921) This change applies to the management of the following Cisco IOS XE Routers: • Cisco IR1101 Integrated Services Routers	4.7.2-8	Tunnel Provisioning Configuration Process in Cisco IoT Field Network Director Post-Installation Guide - Release 4.3.x and Later - High Availability and Tunnel Provisioning

Features	Description	First IoT FND Release Support	Related Document or Section
Support Expired Cisco SUDI Certificate	The expiration date for a limited number of Cisco Secure Unique Device Identifier (SUDI) certificates for a limited number of Internet of Things (IoT) products will expire on: Date of Manufacture plus 10 years or 2029-05-14, whichever is earlier. The following Cisco devices are affected by this change: • Connected Grid Routers: CGR1120 and CGR1240 • Cisco IR1101 Integrated Services Router • Cisco Industrial Integrated Services Routers: IR807, IR809, and IR829 • Cisco Wireless Gateway for LoRaWAN: IXM **Note** A previously enrolled device will not be affected by an expired Cisco SUDI certificate. Devices with expired SUDI certificate will not have any authentication issues with FND from now on.	4.7.1-60	Support Expired Cisco SUDI Certificate
Improved Usability for File Management	You can modify the width of the Open Issues column that displays for a Field Device when two or more open issues exist by selecting the column and moving the cursor to the left to minimize the size of the column. Additionally, this feature reduces the Open Issues display to a single line of content versus multiple lines and displays three periods (...) to indicate that additional content is available to view by expanding the column to the right. **DEVICES** > **FIELD DEVICES** > **Browse Devices** > **Inventory**	4.7.1-60	Displaying Truncated Views of the OPERATIONS > Issues page
Device Search Field added to the Device File Management page to Search for a Specific Router	You can perform partial or full search for a router on the Upload File to Routers page using a router name such as: • CGR1120/K9+JAF1641648BBCT • **CONFIG** > **DEVICE FILE MANAGEMENT** > **Actions**	4.7.1-60	Device File Management for Routers

Features	Description	First IoT FND Release Support	Related Document or Section
Number of Devices that Display on the Upload File to Routers Page Increased to 200	By default, a minimum of ten routers display. You can select up to 200 devices to display. **CONFIG** > **DEVICE FILE MANAGEMENT** > **Actions**	4.7.1-60	Adding a Router Device File to IoT FND
Set Time Range and Page Preferences for Events	On the **Events** tab for a device, you can define values for Time Range and Page View settings for a device type and apply those same settings to a device of the same type. **DEVICES** > **FIELD DEVICES** > **{Router | Switch | Endpoint | Gateway}**	4.7.1-60	Set Time Range and Page View Preferences for Operations > Events
New Browser Support for FND 4.7.1	Microsoft Edge browser Microsoft EdgeHTML:88.0.705.68	4.7.1-60	—
Troubleshooting Page for On-Demand Statistics	A new Troubleshooting tab is available for CG-MESH and IR500 endpoints on the Device Details page. This new page allows you to generate the following predefined system reports for the CG-MESH and IR500 endpoints: - All TLVs, Connectivity, General, Registration, and Routing. **DEVICESFIELD DEVICES ENDPOINTTroubleshoot** tab.	4.7.0-100	Troubleshooting On-Demand Statistics for Endpoints

Features	Description	First IoT FND Release Support	Related Document or Section
Itron Bridge Meter, ITRON30 Support and Management	An Endpoint Operator can now manage Itron Bridge Meters (such as ITRON30) using IoT FND as a cg-mesh device type (METER-CGMESH). This meter was previously run in RFLAN mode. Only Root and Endpoint operators can see and perform the endpoint operations and scheduling for the channel notch feature. To manage an Itron Bridge Meter in cg-mesh node, an Endpoint Operator (RBAC) must convert the RFLAN meter to a cg-mesh device type and upgrade all CG-mesh firmware to CG-mesh 5.6.x. After successful registration, the channel notch settings (in the bootstrap config.bin file) should be pushed to all nodes by the Endpoint operator. Two new properties: • channelNotchMaxAttempts = 20: The maximum allowed attempts to try to send the configuration and schedule info to all the endpoints. • channelNotchSettingEnabled=true. Allows you to enable or disable the channel notch feature.	4.7.0-100	Managing Itron Bridge Meters
Channel Notch Settings	You can define up to four pairs of Notch Range Start and End Channels in the Channel Notch Settings page: **CONFIG > CHANNEL NOTCH SETTINGS** The above page only appears when the cgmesh.properties has the following setting: channelNotchSettingEnabled=true	4.7.0-100	Managing Itron Bridge Meters

Features	Description	First IoT FND Release Support	Related Document or Section
Channel Notch Configuration page	You can push and schedule the Channel Notch Configuration Settings in the following new page: **CONFIG** > **CHANNEL NOTCH CONFIG** You can initiate the following two actions for those routers whose endpoints have been successfully updated with the channel notch configuration: (+) button on the router group displays the router name and the corresponding cg-mesh endpoints. • **Push Channel Notch Config** button — When you select the Router group and click the Push Channel Notch Config button, FND initiates a push of the channel notch settings to the endpoints. • **Schedule Channel Config** button — This operation is only allowed for those router config groups that have routers with endpoints that have received a channel notch config successfully. When applicable, the panel allows you to set a schedule channel config date and time for the devices.	4.7.0-100	Managing Itron Bridge Meters
ITRON30, IR500 and CG-Mesh Device Configuration	On the **ENDPOINT** > **Default-cgmesh** page, you can now perform the additional actions at the Push Configuration tab page found in the right-pane: Select the **Push ENDPOINT Re-Enrollment** option in the drop-down menu on the page, along with the **Certificate Re-enrollment Type**. Supported certificate re-enrollment options are: • Get NMS Cert and NPSA/AAA Cert • LDevID Certificate • IDevID Certificate Messages are sent in unicast form. **CONFIG** > **DEVICE CONFIGURATION** > **Groups** > **ENDPOINT** > **Desired Group (Default-ir500 or Meter)** > **Push CONFIG** Select **Push Endpoint Re-enrollment**	4.7.0-100	Certificate Re-Enrollment for ITRON30 and IR500

Features	Description	First IoT FND Release Support	Related Document or Section
Endpoint Re-Enrollment Option for ITRON30 and IR500 Endpoints	You can now re-enroll a certificate for cg-mesh endpoints by selecting the Re-Enrollment tab on the Device info page of the CGMESH and IR500 endpoints. When you click the Re-enrollment button on the cgmesh or IR500 device details page, it will open a popup window with three options. Select one of the certificates and click Submit. **DEVICES** > > **FIELD DEVICES** > **Browse Devices** > **ENDPOINT** > **METER-CGMESH** (left pane). Newly added endpoint appears on the **Device Config** page	4.7.0-100	Certificate Re-Enrollment for ITRON30 and IR500
DTLS Relay and Certificate Auto Renew Settings for ITRON30 and IR500 Endpoints	New options are available on the **Edit Configuration Template** page. • You can enable or disable the DTLS Relay Settings. • You can enter the Certificate Auto Renew Settings percentage, range of 0 to 100. **CONFIG** > > **DEVICE CONFIGURATION** > **Groups** > **ENDPOINT** > **Default-CGMesh** > **Edit Configuration Template**. **CONFIG** > **DEVICE CONFIGURATION** > **Groups** > **ENDPOINT** > **Default-ir500** > **Edit Configuration Template**	4.7.0-100	Certificate Re-Enrollment for ITRON30 and IR500
Certificate Information page for Gateway IR500 Endpoints	The following certificate information is reported for IR500 endpoints managed by IoT FND on the Certificate Info page (right-pane): • Manufacturer IDevID • LDevID • NMS Cert **DEVICE** > **FIELD DEVICES** > **ENDPOINT** > **GATEWAY-IR500** > **Certificate Info**.	4.7.0-100	Certificate Re-Enrollment for ITRON30 and IR500

Features	Description	First IoT FND Release Support	Related Document or Section
New Device Events for Gateway IR500 Endpoints	Name of new events supported: • MAJOR: Authentication Failure • INFO: Authentication Success, CAcert Request, CAcert Response, Email Success, Enroll Request, Enroll Success, SSL Error **DEVICE** > **FIELD DEVICES** > **Browse Devices** > **GATEWAY-IR500** > **Events** .	4.7.0-100	New Events for IR500
Audit Trail for Re-Enrollment for Gateway-IR500 Endpoints	The following new Operation will be recorded for Re-Enrollment of the Group: • Operation: Re-Enrollment (Get NMS Cert and NPS/AAA Cert) • Status: Initiated • Details: Group default-cg-mesh, Device category: endpoint **ADMIN** > **SYSTEM MANAGEMENT** > **AUDIT TRAIL**	4.7.0-100	Audit Trail for Re-enrollment for Gateway-IR500 Endpoints
Wi-SUN Configuration for IR500 and Itron30	**Note** In Mesh software 6.1, the Wi-SUN 1.0 protocol is supported for all IR500 platforms. The mesh protocol setting between CG-Mesh or Wi-SUN 1.0 can only be set in the bootstrap configuration. **Note** In Mesh software 6.3, only the Wi-SUN 1.x protocol will be supported for all mesh endpoints. It will display Wi-SUN 1.0 from mesh 6.3 firmware onward under the Mesh Protocol heading on the **DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **Inventory page**. **Note** The Wi-SUN settings have been removed from the IR500 Config Group template. **CONFIG** > **DEVICE CONFIGURATION** > **Default-ir500** > **Edit Configuration Template**.	4.7.0-100	Wi-SUN 1.0 Support

Features	Description	First IoT FND Release Support	Related Document or Section
TLS Version Settings for Default-cgmesh Endpoints	The available settings for the TLS version are: • 1.2 • 1.0 and 1.2 • N/A **CONFIG** > > **DEVICE CONFIGURATION** > **Groups** > **Endpoint** > **default-ir500** > **Edit Configuration Template** .	4.7.0-100	Certificate Re-Enrollment for ITRON30 and IR500
Mesh Wi-SUN 1.x Power Outage Notifications (PON) and Power Restoration Notifications (PRN) for IR510	This feature is supported on IR510 from Mesh Release 6.2 and onward. IR510 can send the WiSUN Outage and Restoration notification when running in WiSUN mode. **Note** IR509, IR529 and IR530 running in WiSUN mode can **relay** the WiSUN Outage and Restoration notification message but **cannot** send the message. **OPERATIONS** > **EVENTS** **OPERATIONS** > **ISSUES**	4.7.0-100	Wi-SUN 1.0 Support
Mesh 6.3: Configure Rate Limits for LoWPAN interfaces and IR5xx Ethernet Interfaces and meters (ITRON30, CGREF3) to Defend Against Denial of Service (DoS) Attacks	You can define a Default Access Control List (ACL) Profile for each protocol (UDP, TCP, ICMP) to control the rate of the traffic sent or received. The rate limit is set in kbits/unit. A configuration push will fail if the rate exceeds the configured limit. **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles** > **ACL Profile** > **Default ACL Profile**	4.7.0-100	• Release Notes for Cisco Resilient Mesh, Release 6.3 • Create, Delete, Rename, or Clone any Profile at the Config Profiles Page
Interface ACL Settings for Lowpan in the Config Push Template	You can now define an ACL rule in the configuration profile for Lowpan interfaces as well as define rate limits for lowpan interfaces. **CONFIG** > **DEVICE CONFIGURATION** > **Config Profiles** > **ACL Profile** > **Interface ACL Settings**	4.7.0-100	Create, Delete, Rename, or Clone any Profile at the Config Profiles Page

Features	Description	First IoT FND Release Support	Related Document or Section
ACL Deny Messages	A new section on the Device Details page for IR510, IR529 and IR530, shows ITRON30 and CGREF3 meters, displays ACL Deny Message Detail for LoWPAN Interfaces. **DEVICES** > **FIELD DEVICES** > **ENDPOINT** > **GATEWAY-IR500**	4.7.0-100	Create, Delete, Rename, or Clone any Profile at the Config Profiles Page
Bandwidth Efficient Software Transfer (BEST)	When updating an existing installed software base for IR510, IR530, IR509, IR529 and CGMESH (Itron, CGEREF2, CGEREF3) devices, you have the option to upload only the new FND 4.7 software updates, rather than the full image, by using bspatch and bsdiff version 4.3. The platform image on IR510, IR509, IR530, IR529 and CGMESH (ITRON, CGEREF2, CGEREF3) must be running Mesh 6.3 or greater for this feature to work. To make use of this feature in the FND 4.7 user interface at the **CONFIG** > **FIRMWARE UPDATE** > **Firmware Management** > **Upload Image** page of your system, you must enable the feature by checking the **Install Patch** option on that page before you select the **Upload Image** button. **CONFIG** > **FIRMWARE UPDATE**	4.7.0-100	Uploading a Firmware Image to a Resilient Mesh Endpoint (RME) Group
Enforcing Wi-SUN Firmware Upgrade Rules	All endpoints in the subnet that are moved to Wi-SUN mode must have a mesh firmware software version of Mesh 6.3 or greater. IoT FND 4.7 will not allow a software upgrade to proceed if the mesh firmware software version requirement is not met. Additionally, you will not be able to downgrade endpoints from a Wi-SUN firmware version to a non-Wi-SUN version. Pop-up messages will appear when an invalid firmware upload or scheduled firmware upload is detected. **Note** The NB-API has been enhanced to handle the validation check in both the upload and reload phase. **Note** The feature is not applicable to all IR500s.	4.7.0-100	—

Features	Description	First IoT FND Release Support	Related Document or Section
Management of Cisco Wireless Gateway for LoRAWAN (IXM), Release 2.1.0.1	IoT FND now manages the following IXM components: • Plug and Play (PNP) support • Configuring the Common Packet Forwarder (CPF) • Display of CPF properties (Info and Status) in the FND Device Details page Prerequisite to managing the IXM: Add the following property to cgms.properties and set it to 'true' and restart the FND service: `trust-ixm-server-cert=true` **Note** After you enter the above command, you will need to add the Gateway Bootstrap Configuration template to LoRAWAN in the Tunnel Provisioning Page before triggering PnP on the device.	4.7.0-100	Gateway Bootstrap Configuration Template in Release Notes for IoT Field Network Director, Release 4.7.x
Oracle 19C Support	FND 4.7.0 Oracle OVA will have Oracle19C installed in the virtual machine.	4.7.0-100	Oracle Database 19c IoT Field Network Director Oracle Upgrade from 18c to 19c

Features	Description	First IoT FND Release Support	Related Document or Section
Update LDevID for Greenfield and Brownfield deployment	FND now has tcl scripts, **autorenewal_update.tcl**, which activates the CLIs, and LDevID-update.tcl, which does file manipulation to update the new certificate information in the **before-*** config files whenever the LDevID certificate is renewed. • In greenfield deployments these scripts are pushed as part of the Registration flow. • In brownfield deployments, these scripts are pushed during periodic refresh metrics. Formerly, when a FAR device renewed its LDevID certificate, the **before-*** config files were not updated with the new certificate information. As a result, if FND rolled back a FAR device because of a new tunnel or device config push, then the FAR device would reload with its previous certificate information which might have been expired at that time and break any communication with FND. **Note** By default this feature is enabled. You can manage it through the **enable_ldevid_renewal_tcl** property.	4.7.1-60	LDevID: Auto-Renewal of Certs and Saving Configuration

Features	Description	First IoT FND Release Support	Related Document or Section
Setup and Configuration for an Enrollment over Secure Transport End-to-End Solution	FND provides the capability to integrate Enrollment over Secure Transport (EST) certificate enrollment for clients over security transport within your network. EST is based on public-private key exchange. Currently, this feature is supported only on IR510 and IR530. The EST service is located between a Certification Authority (CA) and a client. EST uses Hypertext Transfer Protocol (HTTP) to provide an authenticated and authorized channel for Simple Public Key Infrastructure (PKI) Requests and Responses. EST also operates with the following protocols and authentication methods: • Constrained Application Protocol (COAP) web transfer protocol for use with constrained nodes and constrained networks such as low-power, lossy networks. • TLS/SSL Handshake between Registration Authority (RA) and CA • Datagram Transport Layer Security (DTLS) protocol is the preferred method for securing CoAP messages when the Nodes do not have any IPv6(IP) addresses configured. DTLS uses UDP. It is based on Transport Layer Security (TLS) • Constrained Application Protocol (COAP) web transfer protocol for use with constrained nodes and constrained networks such as low-power, lossy networks. • Trust Anchor is explicitly configured on the client or server for use during EST TLS authentication.	4.7.0-100	Configuring Enrollment over Secure Transport