Performing Tasks on the IR500

This chapter explains how to use the Device Manager to perform tasks on the Cisco 500 WPAN Industrial Router (IR500).

Connecting to the IR500

You can use Device Manager in the following ways:

- Operating with IoT-FND—When you have IoT-FND operating in the network, you can connect to that system with Device Manager to download and update work orders. Work orders allow Device Manager to view status and perform tasks on the IR500. To operate in conjunction with IoT-FND, follow the steps in Setting Up the IoT-FND Connection.

- Operating without IoT-FND—When you do not have IoT-FND operating in the network or do not want to connect to that system, use Device Manager to connect directly to an IR500 to view status.

Note When connecting to the IR500 without a work order, you cannot change the device configuration or send data to IoT-FND.

Note The laptop running Device Manager must be directly connected to the IR500.

For more information about the IR500 guides, see http://www.cisco.com/go/ir500 .

Connecting the Laptop to the IR500

To connect the laptop to the IR500, first ensure that you meet these prerequisites:

- You have installed the Device Manager software as described in Installation.
- You are familiar with the information in Managing Work Orders.
- You have a valid work order if you plan on changing any IR500 settings.

To connect the laptop to the IR500:

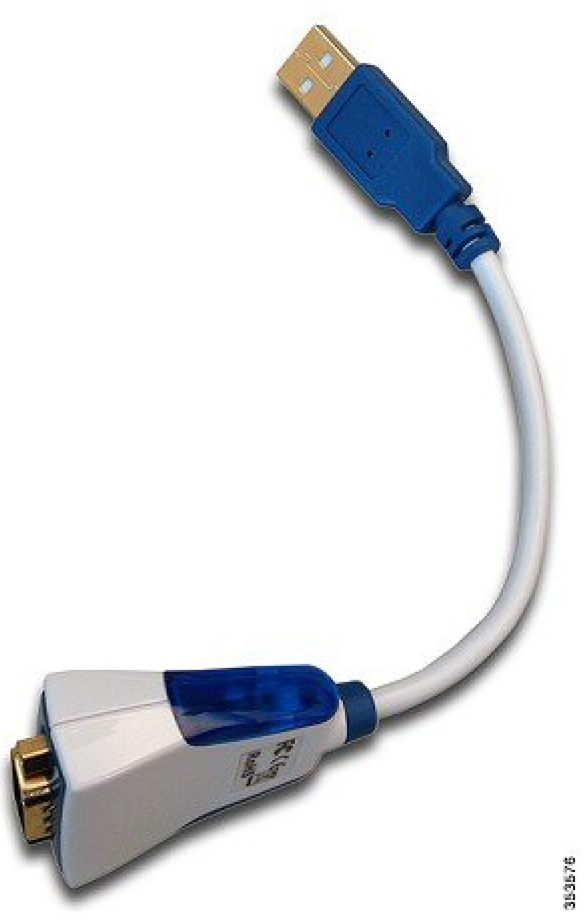
SUMMARY STEPS

1. Attach a serial-to-USB adapter to a serial cable. The serial-to-USB adapter and serial cable are not supplied with the IR500.
2. Connect the serial cable to the IR500 console port.
3. Connect the serial-to-USB adapter to the Windows 7 USB port on the laptop.
4. Launch IoT-Device Manager 5.0.
5. Connect to the IR500 as described in Connecting to the IR500 with a Work Order, on page 4 or Connecting to the IR500 Without a Work Order, on page 4.

DETAILED STEPS

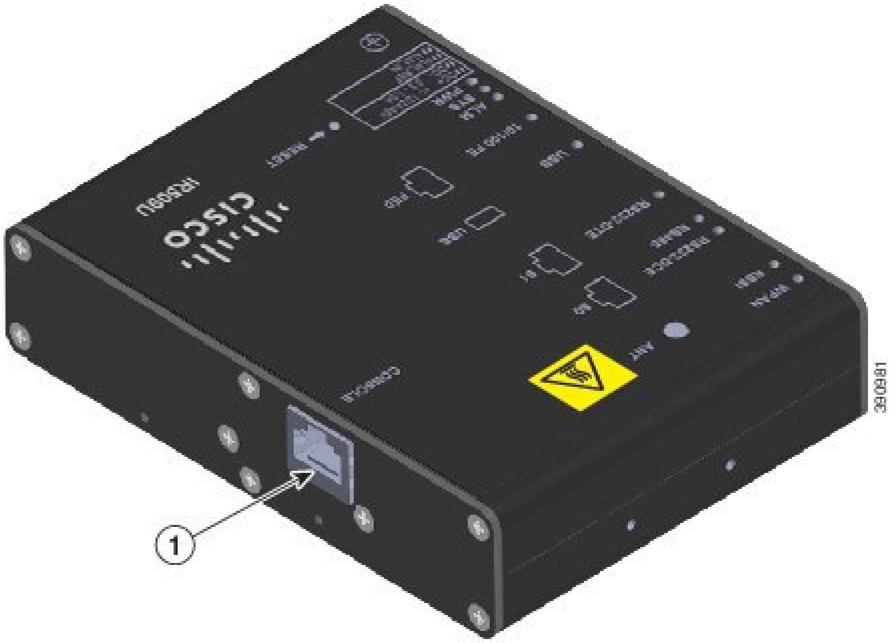
Step 1 Attach a serial-to-USB adapter to a serial cable. The serial-to-USB adapter and serial cable are not supplied with the IR500.

Figure 1: Serial-to-USB Adapter Cable



Step 2 Connect the serial cable to the IR500 console port.

Figure 2: IR500 Rear Panel



1	console port

Step 3 Connect the serial-to-USB adapter to the Windows 7 USB port on the laptop.

Step 4 Launch IoT-Device Manager 5.0.

Step 5 Connect to the IR500 as described in Connecting to the IR500 with a Work Order, on page 4 or Connecting to the IR500 Without a Work Order, on page 4.

For details about IR500 hardware, see the Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide .

Connecting to the IR500 with a Work Order

Before connecting to the router with a work order, you should be familiar with the information in Managing Work Orders.

To connect to the router with a work order, select a work order from the list on the Device Manager opening page and click **Connect**.

Connecting to the IR500 Without a Work Order

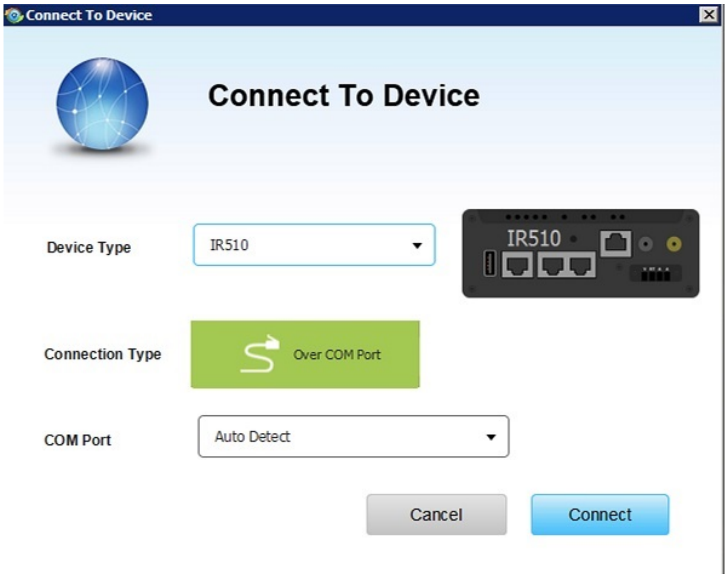
SUMMARY STEPS

1. On the Device Manager opening page, click **Connect Without Work Order**.
2. In the Connect to Device dialog box, select the Device Type: **IR500**.

3. Select the **Over COM port** or **Over Ethernet**.
4. Click **Connect**. The Device Manager main page appears.

DETAILED STEPS

Step 1 On the Device Manager opening page, click **Connect Without Work Order**.



Connect To Device

Device Type: IR510

Connection Type: Over COM Port

COM Port: Auto Detect

Step 2 In the Connect to Device dialog box, select the Device Type: **IR500**.

Step 3 Select the **Over COM port** or **Over Ethernet**.

Step 4 Click **Connect**. The Device Manager main page appears.

Viewing Settings and Status

You can view details about IR500 settings and status from the subtabs of the Dashboard.

General Details

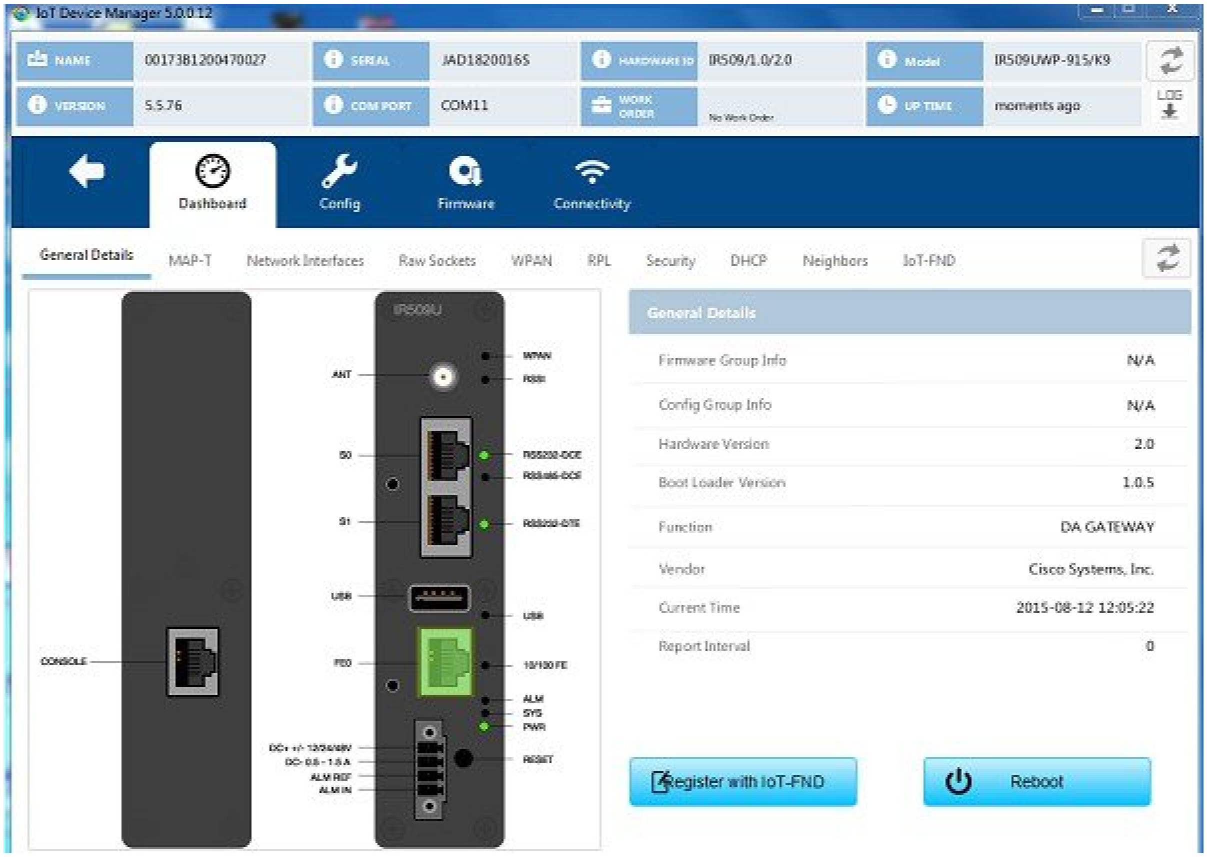
To view General Details:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **General Details** sub-tab.
2. View the General Details:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **General Details** sub-tab.



IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details

Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

Step 2 View the General Details:

- Firmware Group Info: The name of the firmware group that IoT-FND uses to upload and install firmware images on member devices.
- Config Group Info: The configuration group that IoT-FND uses to manage devices in bulk. The default config group for the DA Gateway is **default-ir500**.
- Hardware Version: The hardware version of the device.
- Boot Loader Version: The boot loader image version.
- Function: The function of the device in the Resilient Mesh network. The function of the IR500 is DA Gateway.
- Vendor: The manufacturer of this device.
- Current Time: The current date and time. The IR500 has a real-time clock that maintains the current time.
- Report Interval: The number of seconds between data updates. By default, Mesh Endpoints (MEs) send a new set of metrics to IoT-FND every 28,800 seconds (8 hours).

MAP-T

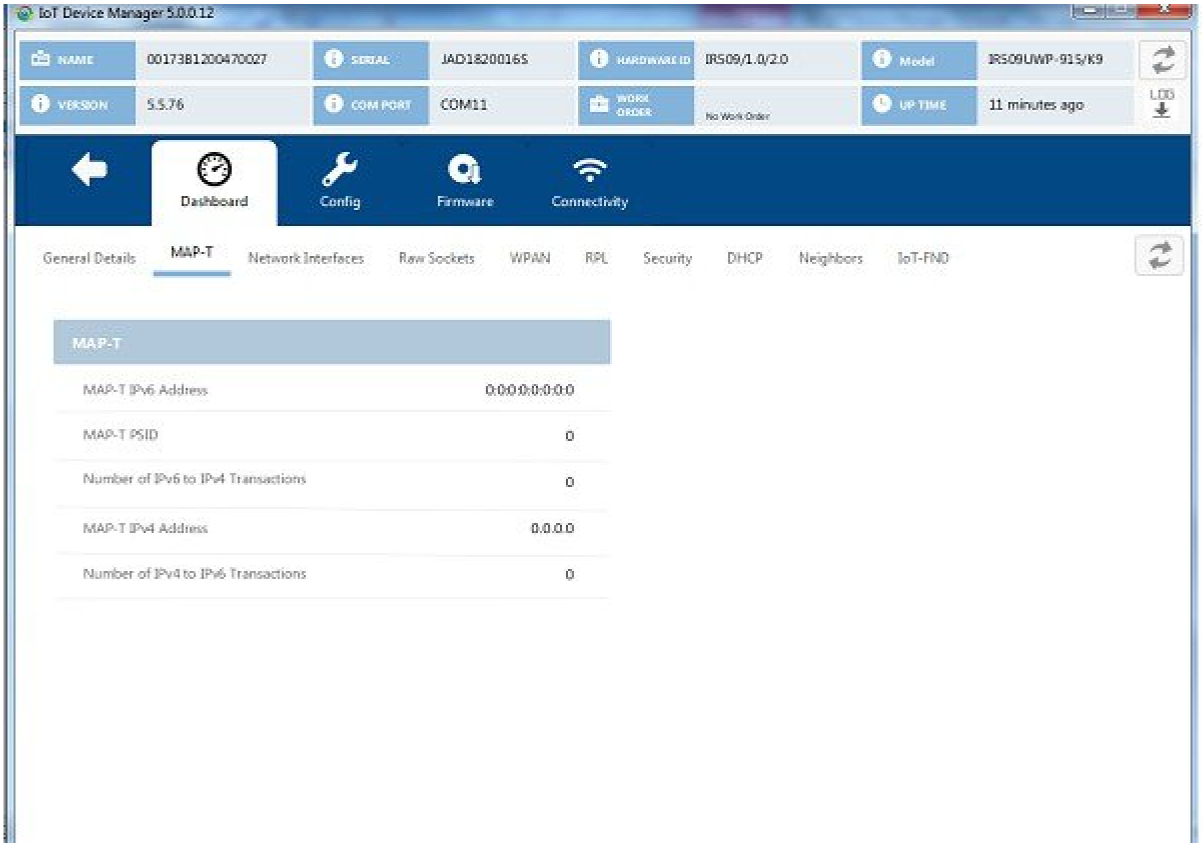
To view MAP-T information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **MAP-T** sub-tab.
2. View the MAP-T settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **MAP-T** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

MAP-T	
MAP-T IPv6 Address	0:0:0:0:0:0:0:0
MAP-T PSID	0
Number of IPv6 to IPv4 Transactions	0
MAP-T IPv4 Address	0.0.0.0
Number of IPv4 to IPv6 Transactions	0

Step 2 View the MAP-T settings and statistics:

- MAP-T IPv6 Address: Contains the IPv4 address used by devices external to the MAP-T domain to communicate with the IR500 Raw Socket over Serial and Ethernet ports.
- MAP-T PSID: The port-set ID (PSID) that algorithmically identifies a set of ports exclusively assigned to the IR500.
- Number of IPv6 to IPv4 Transactions: The number of IPv6 to IPv4 address translations.
- MAP-T IPv4 Address: IPv4 address used by IPv4 devices and applications outside the MAP-T domain to communicate with Raw Socket over Serial and Ethernet attached devices.

- Number of IPv4 to IPv6 Transactions: The number of IPv4 to IPv6 address translations.

Network Interfaces

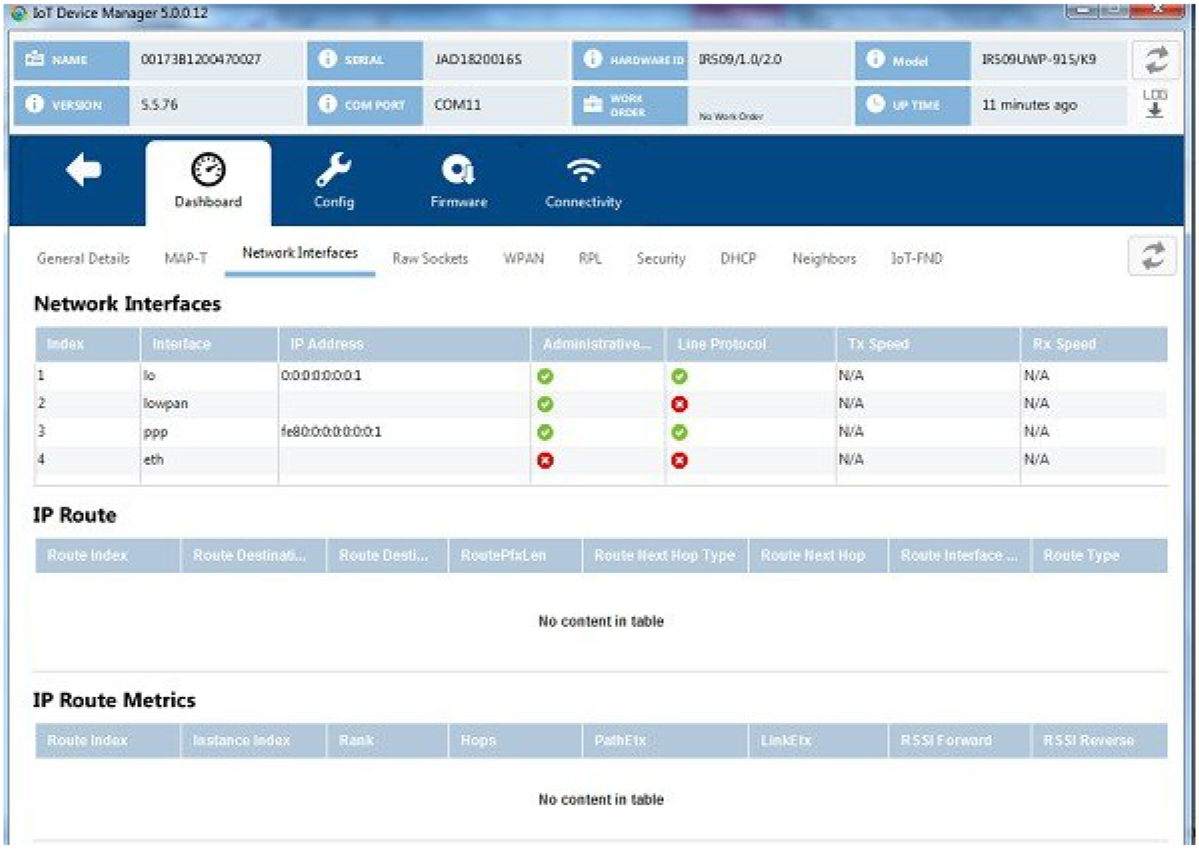
To view information for Network Interfaces:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Network Interfaces** sub-tab.
2. In the Network Interfaces area, view the settings and status for the IR500 interfaces:
3. In the IP Route area, view the IP route information. This table describes a particular IP route (identified by the index) attached to an interface.
4. In the IP Route Metrics area, view the IP Route IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) metrics. The Route Index corresponds to the same index in the IP Route table.

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Network Interfaces** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

Network Interfaces

Index	Interface	IP Address	Administrative...	Line Protocol	Tx Speed	Rx Speed
1	lo	0:0:0:0:0:0:0:1	✓	✓	N/A	N/A
2	lowpan		✓	✗	N/A	N/A
3	ppp	fe80:0:0:0:0:0:0:1	✓	✓	N/A	N/A
4	eth		✗	✗	N/A	N/A

IP Route

Route Index	Route Destinati...	Route Desti...	RoutePfxLen	Route Next Hop Type	Route Next Hop	Route Interface ...	Route Type

No content in table

IP Route Metrics

Route Index	Instance Index	Rank	Hops	PathEtx	LinkEtx	RSSI Forward	RSSI Reverse

No content in table

Step 2 In the Network Interfaces area, view the settings and status for the IR500 interfaces:

- Index: Identifies the interface.
- Interface: Name of the IR500 interface.
- IP Address: IP address assigned to the interface.
- Administrative Status: When the administrative status for an interface is administratively *up* , the interface was brought up by the administrator. When the administrative status for an interface is *down* , the interface was taken down by the administrator.
- Line Protocol: When the line protocol for an interface is *up* , the line protocol is currently active. When the line protocol for an interface is *down* , it means the line protocol is not active.
- Tx Speed: Transmit speed.
- Rx Speed: Receive speed.

Step 3 In the IP Route area, view the IP route information. This table describes a particular IP route (identified by the index) attached to an interface.

- Route Index
- Route Destination Type
- Route Destination
- Route PfxLen: Route Prefix Length
- Route Next Hop Type
- Route Next Hop
- Route Interface Index
- Route Type
- Route Proto
- Route Age

Step 4 In the IP Route Metrics area, view the IP Route IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) metrics. The Route Index corresponds to the same index in the IP Route table.

- Route Index: Identifies the route.
- Instance Index: Identifies the instance.
- Rank: The node's individual position relative to other nodes with respect to a DODAG root. Rank is computed based on the Objective Function (OF) of the Directed Acyclic Graph (DAG). The Rank may analogously track a simple topological distance, be calculated as a function of link metrics, and consider other properties such as constraints. [rfc6550]
- Hops: Hop count.
- PathEtx: Expected transmission count of the path. [rfc6550 and rfc6719]
- LinkEtx: Expected transmission count of the link. [rfc6550 and rfc6719]
- RSSI Forward: Forward Received Signal Strength Indicator (RSSI) value.

- RSSI Reverse: Reverse RSSI value.
- LQI Forward: Forward Link Quality Indicator (LQI) value.
- LQI Reverse: Reverse LQI value.
- Dag Size: Size of the DAG. [rfc6550]
- Phase: Electric power phase.

Raw Sockets

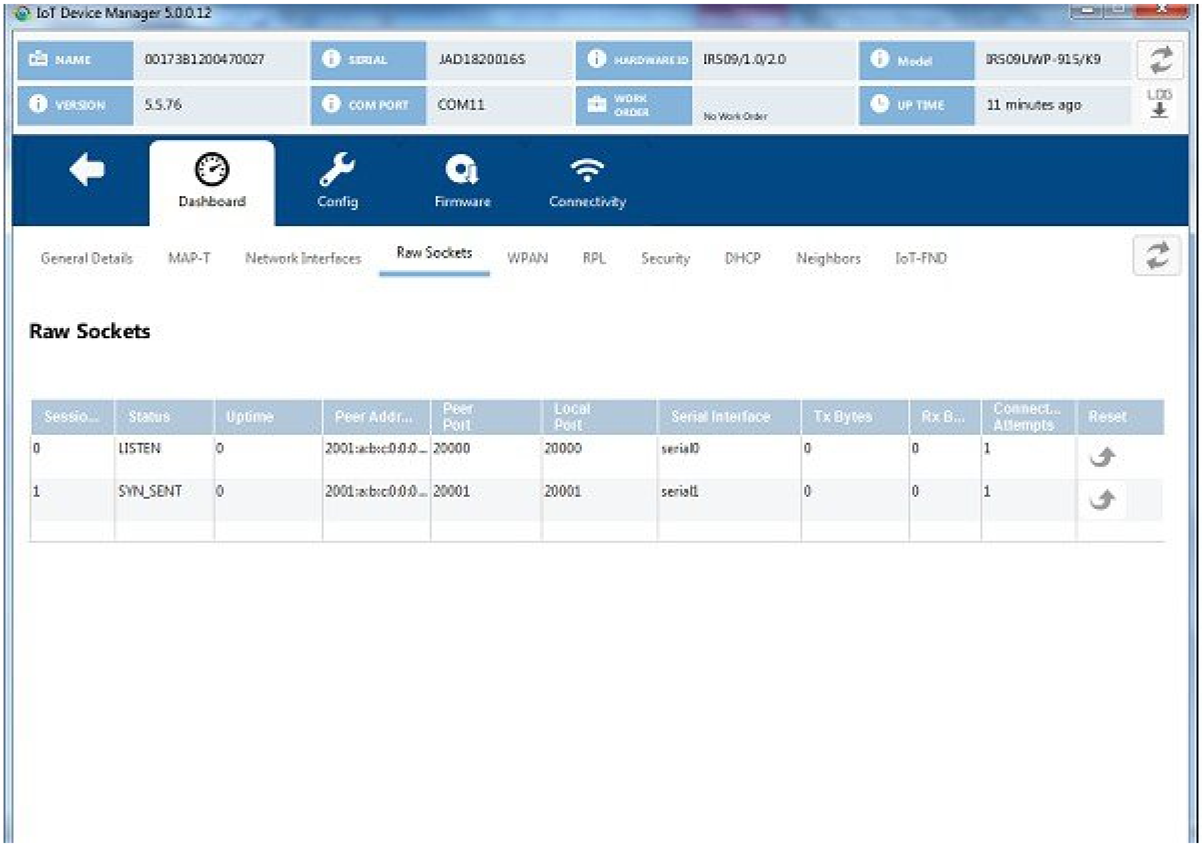
To view information about Raw Sockets:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Raw Sockets** sub-tab.
2. View the raw socket settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Raw Sockets** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

Raw Sockets

Sessio...	Status	Uptime	Peer Addr...	Peer Port	Local Port	Serial Interface	Tx Bytes	Rx B...	Connect... Attempts	Reset
0	LISTEN	0	2001:a:b:c:0:0:0...	20000	20000	serial0	0	0	1	
1	SYN_SENT	0	2001:a:b:c:0:0:0...	20001	20001	serial1	0	0	1	

Step 2 View the raw socket settings and statistics:

- Session Index: Identifies the session.
- Status: The status of the raw socket connection.
- Uptime: The length of time that the connection has been up.
- Peer Address: IP address of the host connected to the device.
- Peer Port: The port number of the client/server connected to the device.
- Local Port: The port that either the server listens to for connections (in Server Socket Mode), or to which the client binds to initiate connections to the server (in Client Socket Mode).
- Serial Interface: The name of the serial interface configured for raw socket encapsulation.
- Tx Bytes: Number of bytes sent over the raw socket connection.
- Rx Bytes: Number of bytes received over the raw socket connection.
- Connection Attempts: Number of times that a raw socket client attempted a connection.

Click **Reset** to reset counters to zero.

WPAN

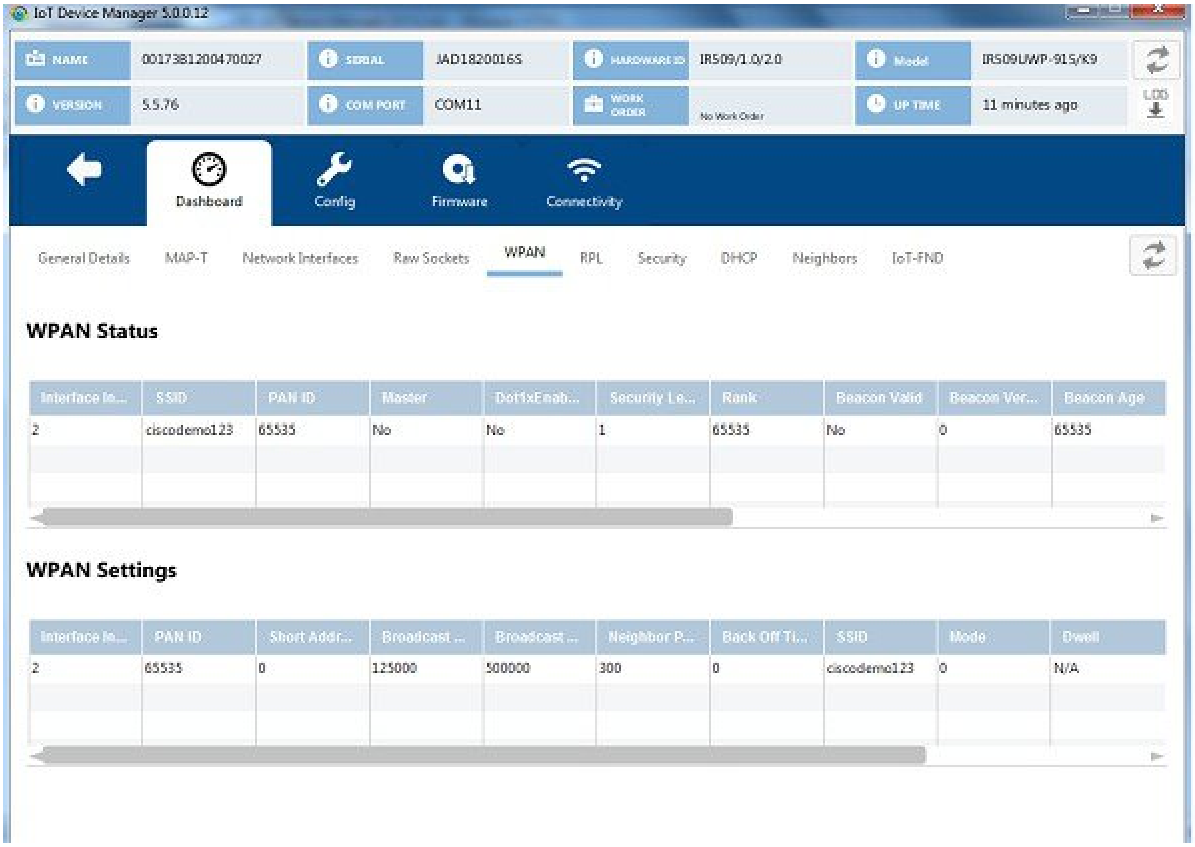
To view information about WPAN:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **WPAN** sub-tab.
2. View the following information in the WPAN Status area:
3. View the following information in the WPAN Settings area:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **WPAN** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

WPAN Status

Interface In...	SSID	PAN ID	Master	Dot1xEnab...	Security Le...	Rank	Beacon Valid	Beacon Ver...	Beacon Age
2	ciscodemo123	65535	No	No	1	65535	No	0	65535

WPAN Settings

Interface In...	PAN ID	Short Addr...	Broadcast ...	Broadcast ...	Neighbor P...	Back Off Ti...	SSID	Mode	Dwell
2	65535	0	125000	500000	300	0	ciscodemo123	0	N/A

Step 2 View the following information in the WPAN Status area:

- Interface Index: Identifies the WPAN interface.
- SSID: Service Set Identifier (SSID) used to differentiate networks.
- PAN ID: Personal Area Network Identifier (PAN ID) used to differentiate WPANs.
- Master: Whether the endpoint is master (yes/no).
- Dot1xEnabled: Whether the 802.1x protocol is enabled.

- Security Level: Level of security corresponding to the protection offered (0–2).
- Rank: The node's individual position relative to other nodes with respect to a DODAG root. Rank is computed based on the DAG's Objective Function (OF). The Rank may analogously track a simple topological distance, be calculated as a function of link metrics, and consider other properties such as constraints. [RFC6550]
- Beacon Valid: The validity of the beacon according to the beacon's age.
- Beacon Version: The beacon's version from the FAR.
- Beacon Age: Parameter related to the time interval received beacon.
- Tx Power: The device current transmission power.
- Metric: The value calculated by rank / the weight value of the rank + size / the weight value of the PAN size.
- Last Changed: The time (in hundredths of a second) since the device changed the PAN.
- LastChangedReason: The reason that the device updated the PAN.
- Demo Mode Enabled: Whether enable demo mode is enabled.
- TxFec: Whether forward error correction (FEC) is enabled.

Step 3 View the following information in the WPAN Settings area:

- Interface Index: Identifies the WPAN interface.
- PAN ID: Personal Area Network Identifier (PAN ID) used to differentiate WPANs.
- Short Address: 16-bit node identifier.
- Broadcast Slot Size: Slot size of the broadcast.
- Broadcast Period: Period of the broadcast.
- Neighbor Probe Rate:
- Back Off Timer: Timer for back off algorithm.
- SSID: Service Set Identifier (SSID) used to differentiate networks.
- Mode: Security mode. 0=no security, 1=802.1x security.
- Dwell: Dwell window in IEEE802.15.4g protocol.
- Notch: List of disabled channels.

RPL

To view information about RPL:

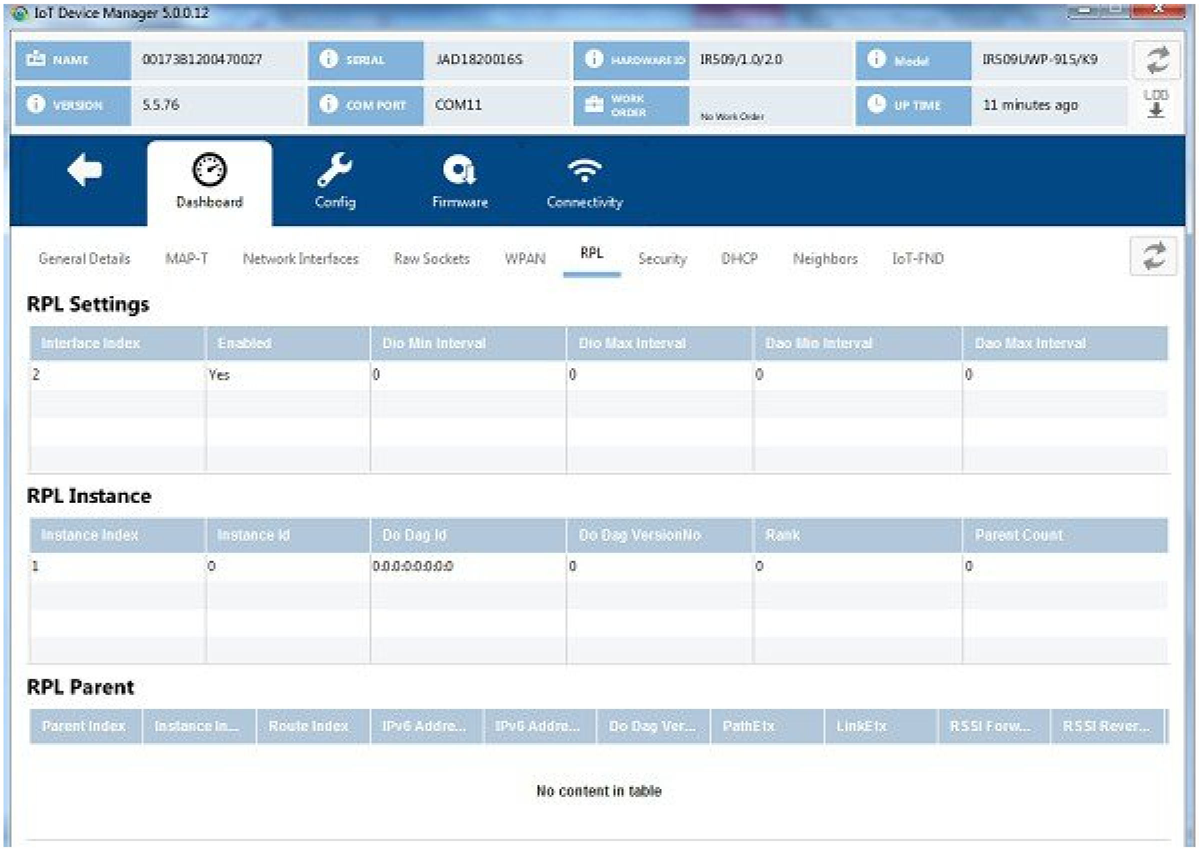
SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **RPL** sub-tab.
2. View the following information in the RPL Settings area:

3. View the following information in the RPL Instance area:
4. View the following information in the RPL Parent area:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **RPL** sub-tab.



IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

RPL Settings

Interface Index	Enabled	Dio Min Interval	Dio Max Interval	Dao Min Interval	Dao Max Interval
2	Yes	0	0	0	0

RPL Instance

Instance Index	Instance Id	Do Dag Id	Do Dag VersionNo	Rank	Parent Count
1	0	0:0:0:0:0:0:0:0	0	0	0

RPL Parent

Parent Index	Instance In...	Route Index	IPv6 Addre...	IPv6 Addre...	Do Dag Ver...	PathEtx	LinkEtx	RSSI Forw...	RSSI Rever...

No content in table

Step 2 View the following information in the RPL Settings area:

- Interface Index: Identifies the interface.
- Enabled: Whether the RPL protocol is enabled.
- Dio Min Interval: Minimum DODAG Information Object (DIO) interval in RPL protocol.
- Dio Max Interval: Maximum DIO interval in RPL protocol.
- Dao Min Interval: Minimum Destination Advertisement Object (DAO) interval in RPL protocol.
- Dao Max Interval: Maximum DAO interval in RPL protocol.

Step 3 View the following information in the RPL Instance area:

- Instance Index: Identifies the RPL instance.
- Instance Id: Identifies an RPL instance, which is a set of one or more DODAGS. [RFC6550]

- Dodag Id: Identifies the DODAG root. The DODAGID is unique within the scope of a RPL instance in the LLN.
- Dodag VersionNo: A sequential counter that is incremented by the root to form a new DODAG version.
- Rank: The node's individual position relative to other nodes with respect to a DODAG root. Rank is computed based on the DAG's Objective Function (OF). The Rank may analogously track a simple topological distance, be calculated as a function of link metrics, and consider other properties such as constraints. [RFC6550]
- Parent Count:

Step 4 View the following information in the RPL Parent area:

- Parent Index: Identifies the parent.
- Instance Index: Identifies the instance.
- Route Index: Identifies the route.
- IPv6 Address Local: Unique local IPv6 address of the parent.
- IPv6 Address Global: IPv6 global unicast address of the parent.
- Dodag VersionNo: A sequential counter that is incremented by the root to form a new DODAG version.
- PathEtx: Expected transmission count of the path. [rfc6550]
- LinkEtx: Expected transmission count of the link. [rfc6550]
- RSSI Forward: Forward Received Signal Strength Indicator (RSSI) value.
- RSSI Reverse: Reverse RSSI value.
- LQI Forward: Forward Link Quality Indicator (LQI) value.
- LQI Reverse: Reverse LQI value.
- Hops: Hop count.

Security

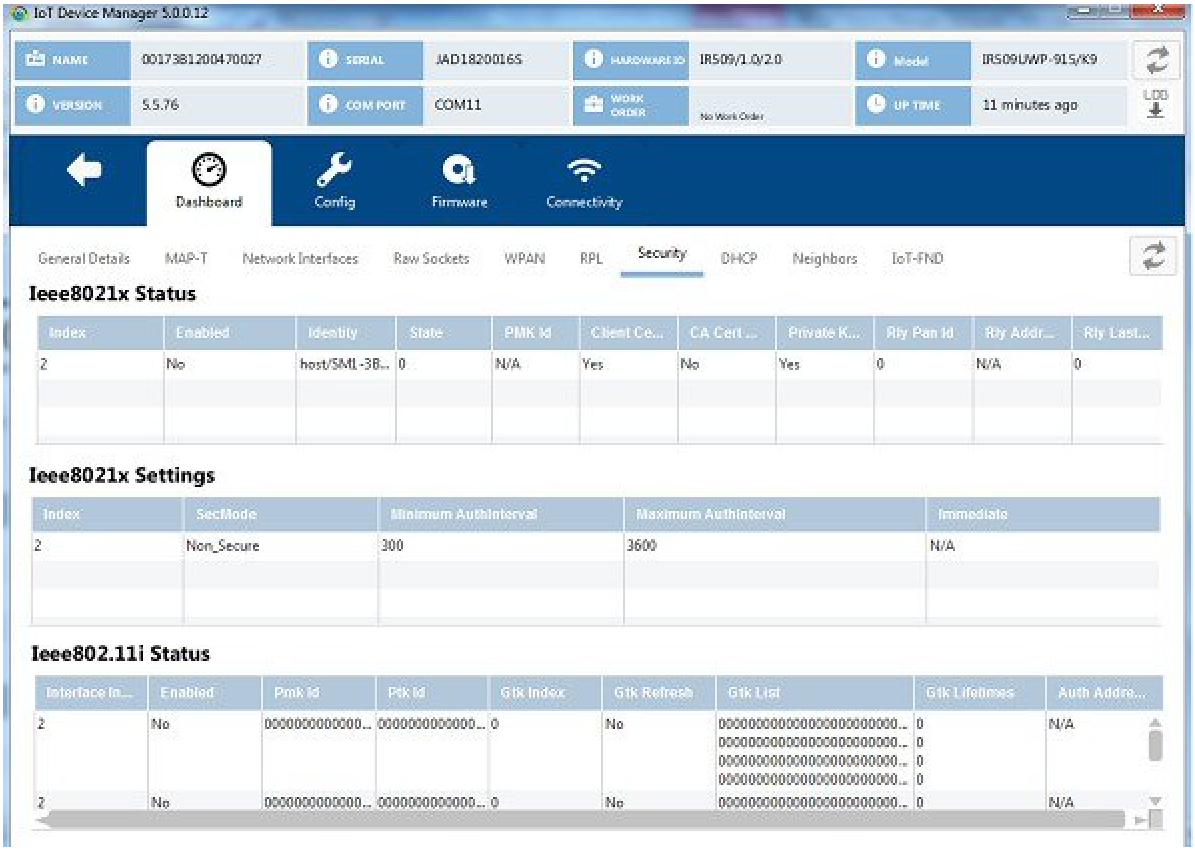
To view information about IEEE 802.1x for WPAN authentication and encryption:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Security** sub-tab.
2. View the information in the Ieee8021x Status area:
3. View the information in the Ieee8021x Settings area:
4. View the information in the Ieee80211i Status area:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Security** sub-tab.



NAME	0017381200470027	SERIAL	JAD1820016S	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

Ieee8021x Status

Index	Enabled	Identity	State	PMK Id	Client Ce...	CA Cert ...	Private K...	Rly Pan Id	Rly Addr...	Rly Last...
2	No	host/SML-3B...	0	N/A	Yes	No	Yes	0	N/A	0

Ieee8021x Settings

Index	SecMode	Minimum AuthInterval	Maximum AuthInterval	Immediate
2	Non_Secure	300	3600	N/A

Ieee802.11i Status

Interface In...	Enabled	Pmk Id	Ptk Id	Gtk Index	Gtk Refresh	Gtk List	Gtk Lifetimes	Auth Addre...
2	No	0000000000000...	0000000000000...	0	No	000000000000000000000000... 000000000000000000000000... 000000000000000000000000... 000000000000000000000000...	0 0 0 0	N/A
2	No	0000000000000...	0000000000000...	0	No	000000000000000000000000...	0	N/A

Step 2 View the information in the Ieee8021x Status area:

- Index: Identifies the network.
- Enabled: Whether 802.1x authentication is enabled.
- Identity: Subject of the X.509 digital certificate.
- State: Current state of Transport Layer Security (TLS).
- PMK Id: Pairwise Master Key identifier.
- Client Certificate:
- CA Certificate: Certificate Authority (CA) certificate
- Private Key: Encryption/decryption key.
- Rly Pan Id: Reply PAN ID.
- Rly Address: Reply address.
- Rly Last Heard: Time of last heard reply.

Step 3 View the information in the Ieee8021x Settings area:

- Index: Identifies the network.
- SecMode: The security mode in use.

- Minimum Auth Interval: The minimum authentication interval.
- Maximum Auth Interval: The maximum authentication interval.
- Immediate: Request authentication immediately.

Step 4 View the information in the Ieee80211i Status area:

- Interface Index: Identifies the interface.
- Enabled: Whether the 80211i protocol is enabled.
- Pmk Id: Pairwise Master Key identifier.
- Ptk Id: Pairwise Transient Key identifier.
- Gtk Index: Identifies the Group Temporal Key.
- Gtk Refresh:
- Gtk List: Group Temporal Key list.
- Gtk Lifetimes:
- Auth Address: Authenticator server address.

DHCP

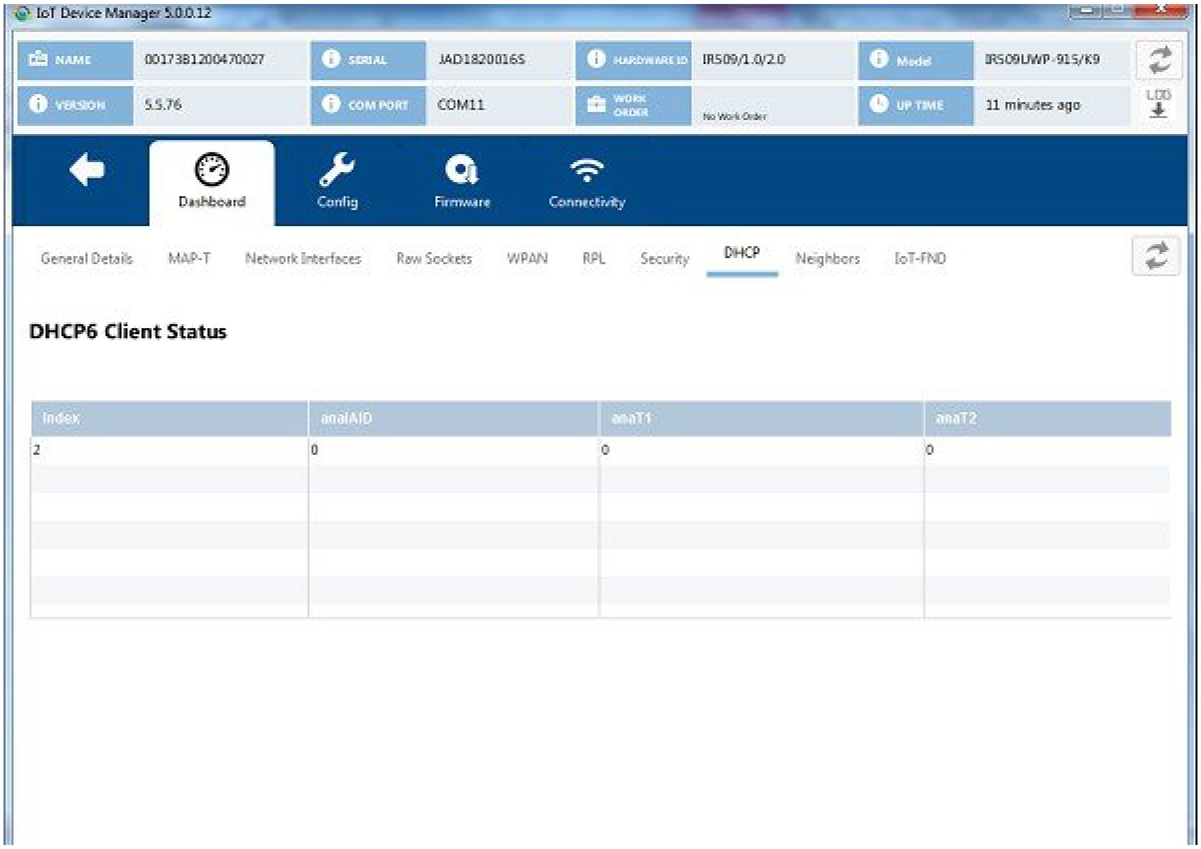
To view information about DHCPv6 for IPv6 address allocation:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **DHCP** sub-tab.
2. View the DHCP Client Status:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **DHCP** sub-tab.



NAME	00173B1200470027	SERIAL	JAD1820016S	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

DHCP6 Client Status

Index	anaIAID	anaT1	anaT2
2	0	0	0

Step 2 View the DHCP Client Status:

- Index: Identifies the network.
- anaIAID: Interface Association Identifier.
- anaT1: Preferred-lifetime.
- anaT2: Valid-lifetime.

Neighbors

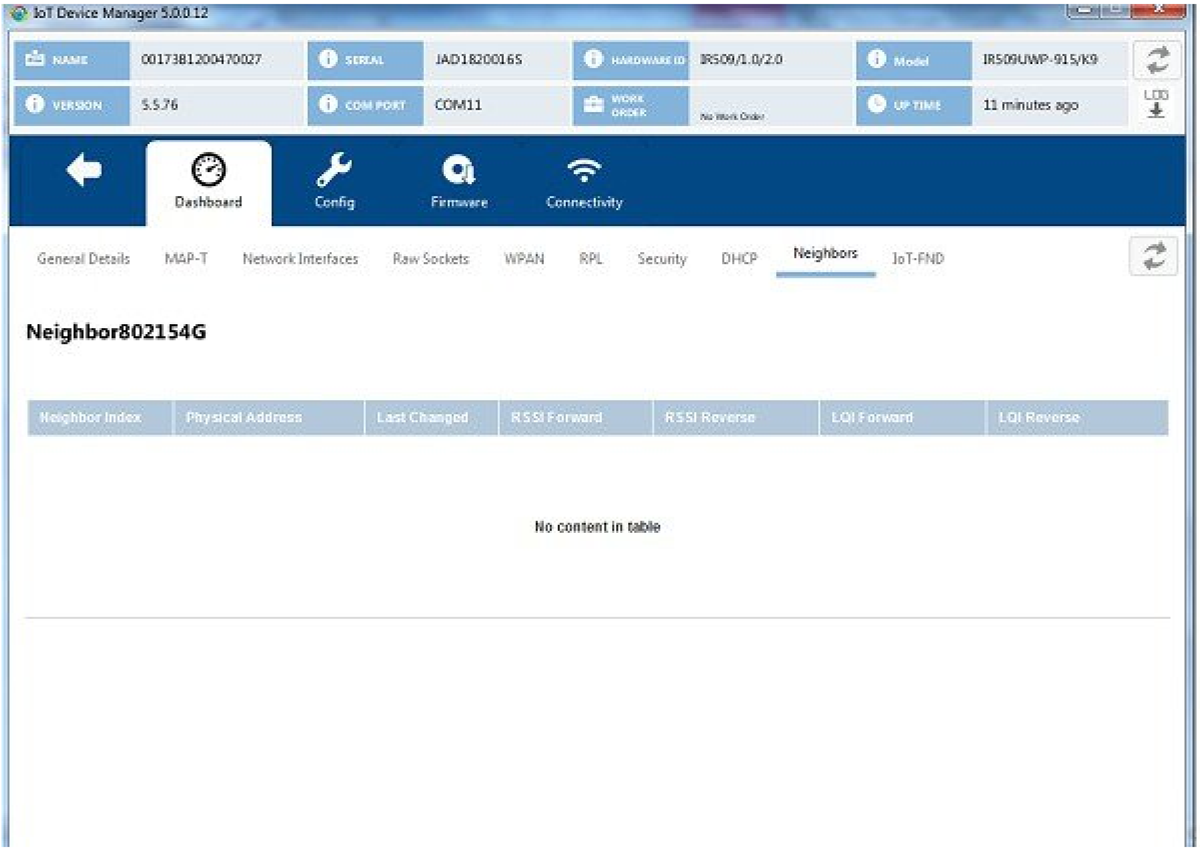
To view 802.15.4g neighbor information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **Neighbors** sub-tab.
2. View the neighbors settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **Neighbors** sub-tab.



NAME 00173B1200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME 11 minutes ago

Neighbor802154G

Neighbor Index	Physical Address	Last Changed	RSSI Forward	RSSI Reverse	LQI Forward	LQI Reverse

No content in table

Step 2 View the neighbors settings and statistics:

- Neighbor Index: Identifies the neighbor
- Physical Address: The 64-bit Extended Unique Identifier (EUI-64) of the device.
- Last Changed: The time (in hundredths of a second) since hearing from the neighbor.
- RSSI Forward: Forward Received Signal Strength Indicator (RSSI) value.
- RSSI Reverse: Reverse RSSI value.
- LQI Forward: Forward Link Quality Indicator (LQI) value.
- LQI Reverse: Reverse LQI value.

IoT-FND

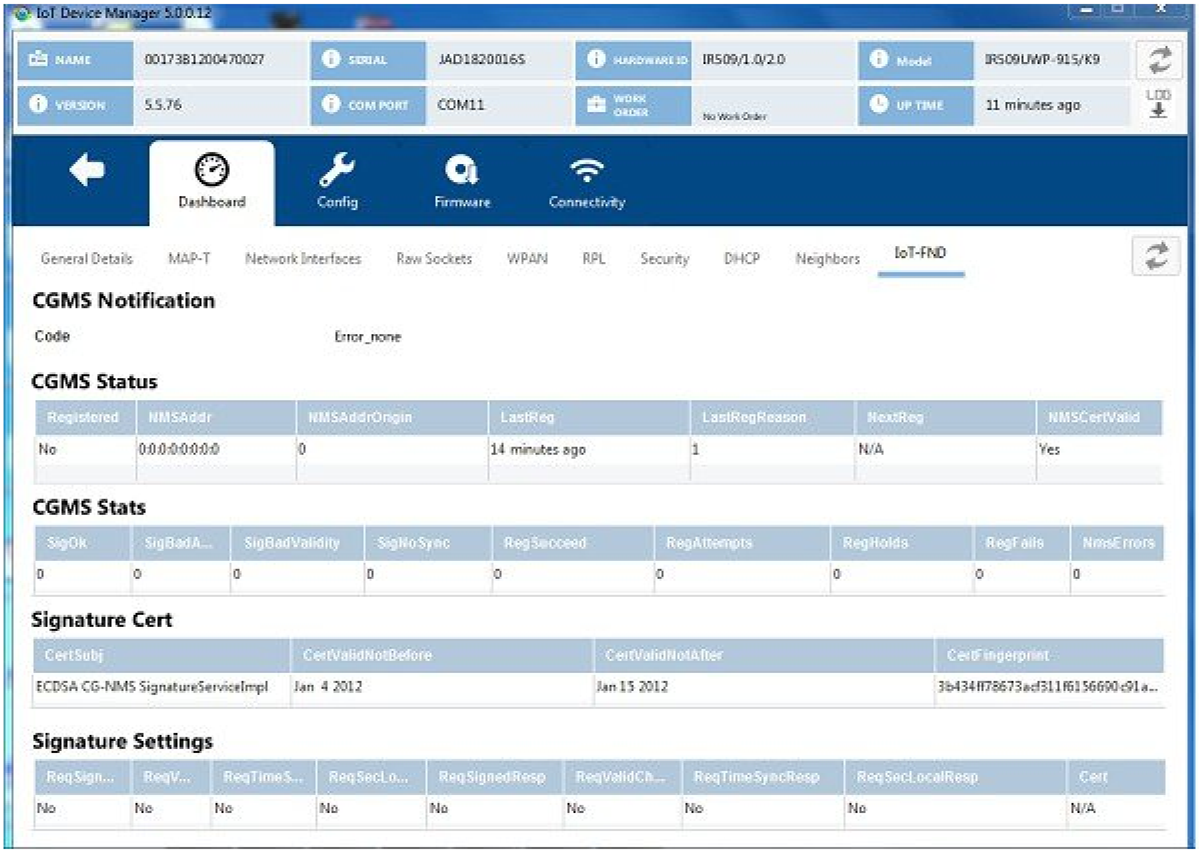
To view information about IoT-FND:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **IoT-FND** sub-tab.
2. View the information in the CGMS notification area:
3. View CGMS Status information:
4. View CGMS Stats:
5. View Signature Cert information:
6. View the Signature Settings information:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **IoT-FND** sub-tab.



NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	11 minutes ago

CGMS Notification

Code Error_none

CGMS Status

Registered	NMSAddr	NMSAddrOrigin	LastReg	LastRegReason	NextReg	NMSCertValid
No	0:0:0:0:0:0:0:0	0	14 minutes ago	1	N/A	Yes

CGMS Stats

SigOk	SigBadA...	SigBadValidity	SigNoSync	RegSucceed	RegAttempts	RegHolds	RegFails	NmsErrors
0	0	0	0	0	0	0	0	0

Signature Cert

CertSubj	CertValidNotBefore	CertValidNotAfter	CertFingerprint
ECDSA CG-NMS SignatureServiceImpl	Jan 4 2012	Jan 15 2012	3b434ff78673acf311f6156690c91a...

Signature Settings

ReqSign...	ReqV...	ReqTimeS...	ReqSecLo...	ReqSignedResp	ReqValidCh...	ReqTimeSyncResp	ReqSecLocalResp	Cert
No	No	No	No	No	No	No	No	N/A

Step 2 View the information in the CGMS notification area:

Code Values:

- 1 = COAP Error
- 2 = Signature Error
- 3 = Registration Processing Error

Step 3 View CGMS Status information:

- Registered: Whether the end point is registered with NMS.
- NMSAddr: Address of NMS.
- NMSAddrOrigin: Origin of NMS address.
- LastReg: Last registration time.
- LastRegReason: Reason for last registration.
- NextReg: Time of next registration.
- NMSCertValid: Whether the certificate is valid.

Step 4 View CGMS Stats:

- SigOk: Count of verified signatures.
- SigBadAuth: Count of bad authorized signatures.
- SigBadValidity: Count of bad validity signatures.
- SigNoSync: Count of signatures that are not synchronized.
- RegSucceed: Count of successful registrations.
- RegAttempts: Count of registration attempts.
- RegHolds: Count of registration holds.
- RegFails: Count of registration failures.
- NmsErrors: Count of NMS errors.

Step 5 View Signature Cert information:

- CertSubj: Certificate subject.
- CertValidNotBefore: Certificate valid.
- CertValidNotAfter: Certificate not valid.
- CertFingerprint: Fingerprint of the certificate.

Step 6 View the Signature Settings information:

- ReqSignedPost: Whether request signed post.
- ReqValidCheckPost: Whether request valid check post.
- ReqTimeSyncPost: Whether request time synchronization post.
- ReqSecLocalPost: Whether request security local post.
- ReqSignedResp: Whether request signed response.
- ReqValidCheckResp: Whether valid check response.
- ReqTimeSyncResp: Whether time synchronization response.

- ReqSecLocalResp: Whether request security local response.

ACL

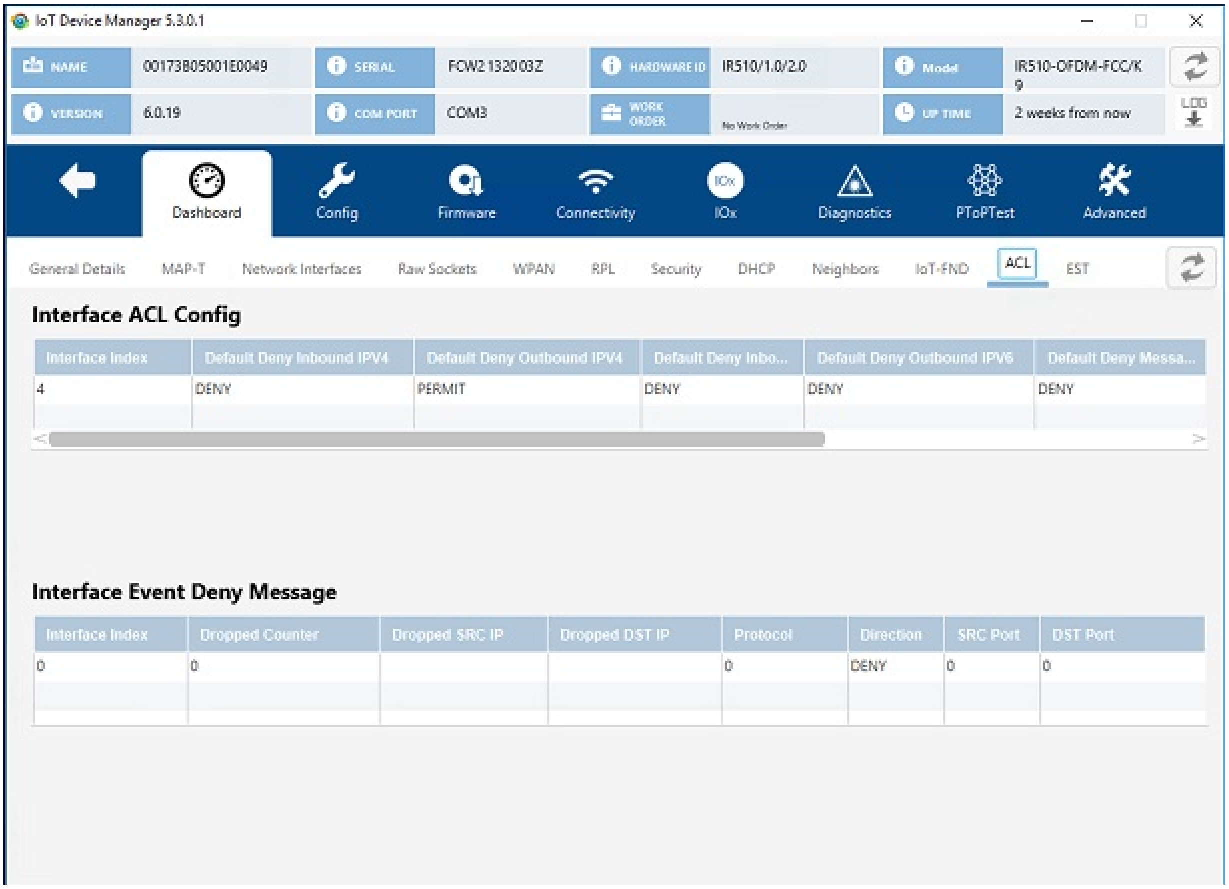
To view Access Control List (ACL) information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **ACL** sub-tab.
2. View the ACL settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **ACL** sub-tab.



NAME 00173B05001E0049
SERIAL FCW2132003Z
HARDWARE ID IR510/1.0/2.0
Model IR510-OFDM-FCC/K9
VERSION 6.0.19
COM PORT COM3
WORK ORDER No Work Order
UP TIME 2 weeks from now

Interface ACL Config

Interface Index	Default Deny Inbound IPV4	Default Deny Outbound IPV4	Default Deny Inbo...	Default Deny Outbound IPV6	Default Deny Messa...
4	DENY	PERMIT	DENY	DENY	DENY

Interface Event Deny Message

Interface Index	Dropped Counter	Dropped SRC IP	Dropped DST IP	Protocol	Direction	SRC Port	DST Port
0	0			0	DENY	0	0

Step 2 View the ACL settings and statistics:

- Interface ACL Config

- Interface Event Deny Message

EST

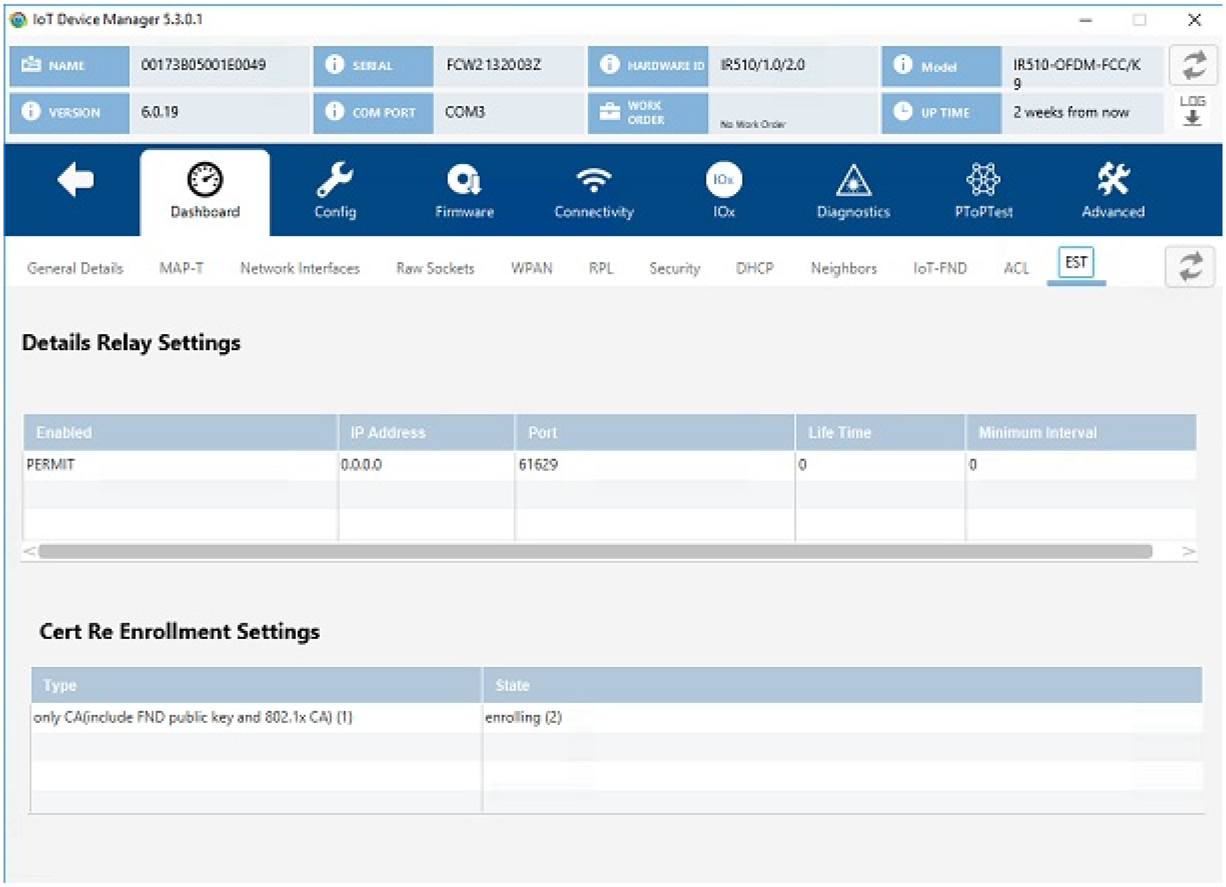
To view Enrollment settings (EST) information:

SUMMARY STEPS

1. On the Device Manager main page (Dashboard), click the **EST** sub-tab.
2. View the EST settings and statistics:

DETAILED STEPS

Step 1 On the Device Manager main page (Dashboard), click the **EST** sub-tab.



NAME 00173B05001E0049

SERIAL FCW2132008Z

HARDWARE ID IR510/1.0/2.0

Model IR510-OFDM-FCC/K9

VERSION 6.0.19

COM PORT COM3

WORK ORDER No Work Order

UP TIME 2 weeks from now

Details Relay Settings

Enabled	IP Address	Port	Life Time	Minimum Interval
PERMIT	0.0.0.0	61629	0	0

Cert Re Enrollment Settings

Type	State
only CA(include FND public key and 802.1x CA) (1)	enrolling (2)

Step 2 View the EST settings and statistics:

- Details Relay Settings

- Cert Re Enrollment Settings

Viewing Interface Details

You can view details for the Ethernet and the two serial interfaces from the Device Manager main page (Dashboard).

Ethernet Interface Details

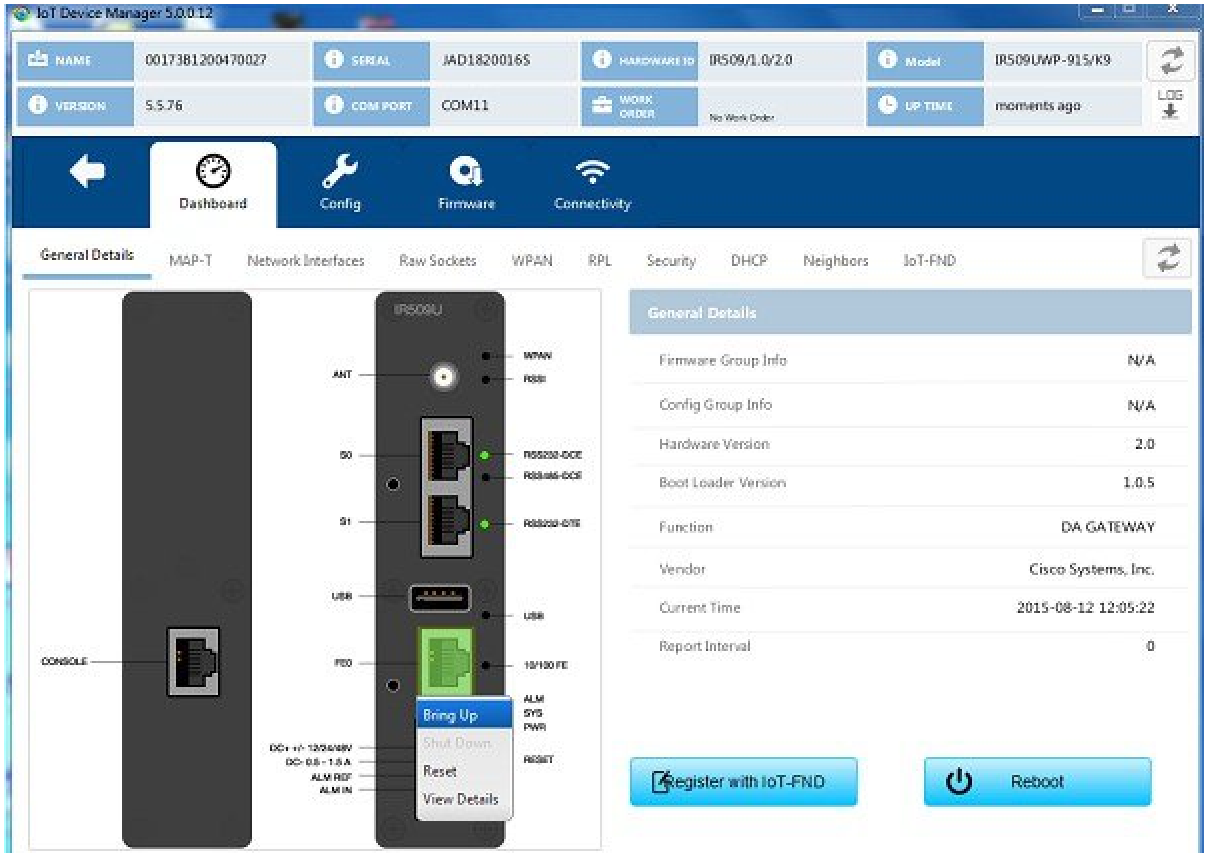
To view details for the Ethernet interface:

SUMMARY STEPS

1. On the Device Manager main page, click the Ethernet port to display the popup menu and select **View Details**.
2. To refresh the display, click the refresh icon in the upper right corner of the View Details window.

DETAILED STEPS

Step 1 On the Device Manager main page, click the Ethernet port to display the popup menu and select **View Details**.



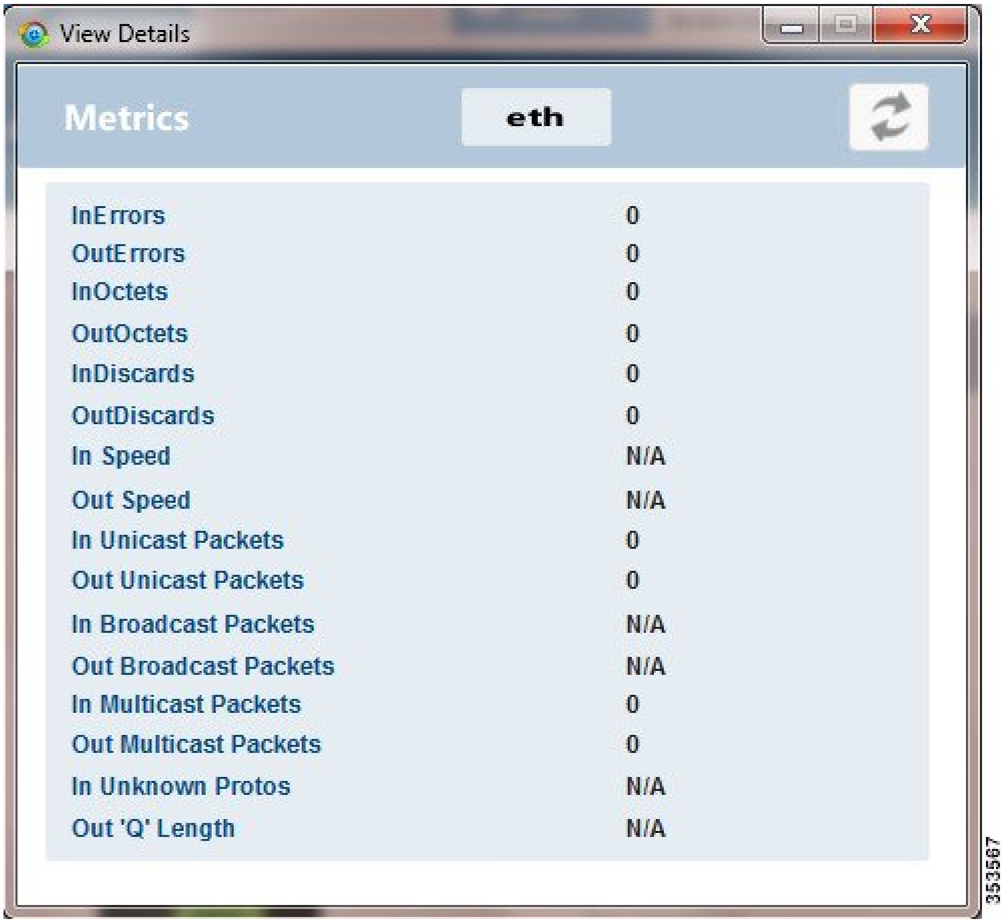
IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details

Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

The View Details window displays the Ethernet metrics.



InErrors	0
OutErrors	0
InOctets	0
OutOctets	0
InDiscards	0
OutDiscards	0
In Speed	N/A
Out Speed	N/A
In Unicast Packets	0
Out Unicast Packets	0
In Broadcast Packets	N/A
Out Broadcast Packets	N/A
In Multicast Packets	0
Out Multicast Packets	0
In Unknown Protos	N/A
Out 'Q' Length	N/A

Step 2 To refresh the display, click the refresh icon in the upper right corner of the View Details window.

Serial Interface Details

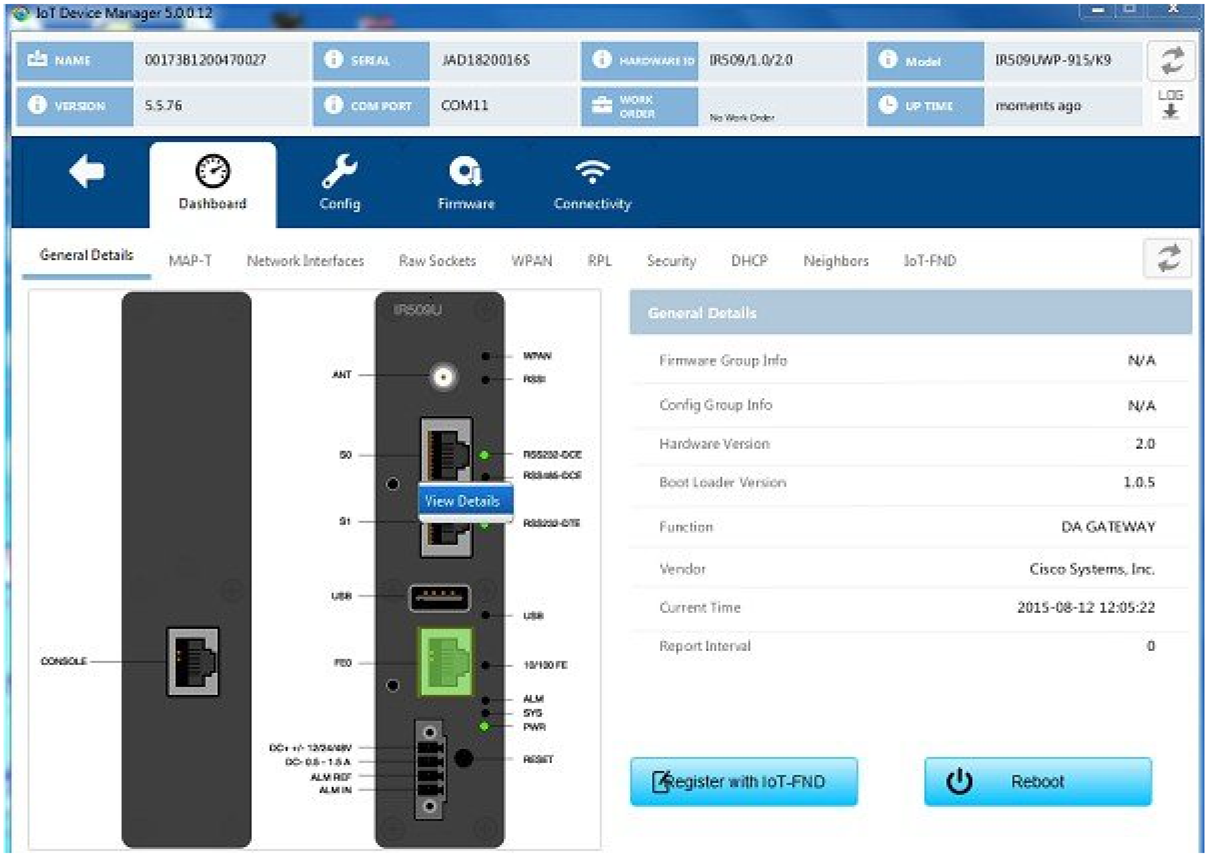
To view details for serial interface 0 (DCE) or serial interface 1 (DTE):

SUMMARY STEPS

1. On the On the Device Manager main page, click a serial port to display the popup menu and select **View Details**.
2. To refresh the display, click the refresh icon in the upper right corner of the View Details window.

DETAILED STEPS

Step 1 On the On the Device Manager main page, click a serial port to display the popup menu and select **View Details**.

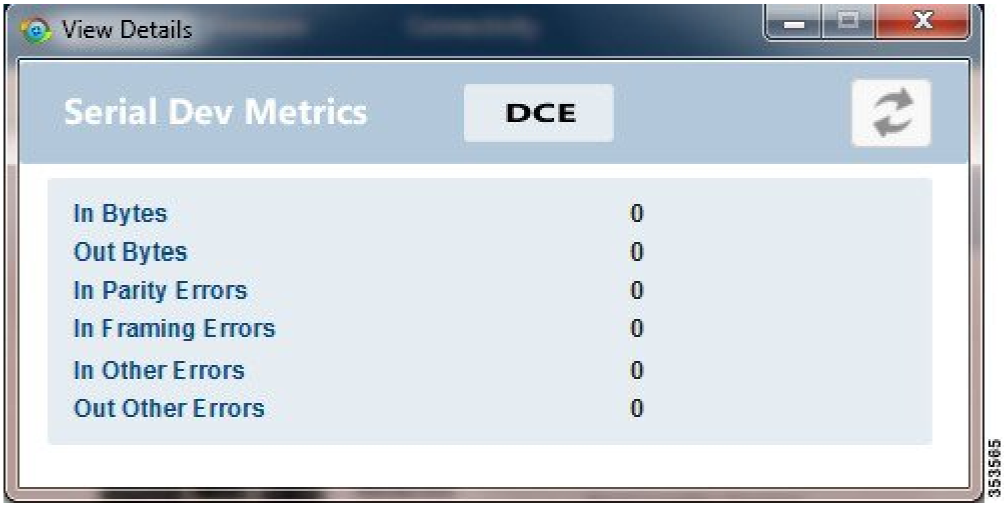


NAME	0017381200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

General Details

Firmware Group Info	N/A
Config Group Info	N/A
Hardware Version	2.0
Boot Loader Version	1.0.5
Function	DA GATEWAY
Vendor	Cisco Systems, Inc.
Current Time	2015-08-12 12:05:22
Report Interval	0

The View Details window displays the DCE or DTE metrics.



Serial Dev Metrics DCE

In Bytes	0
Out Bytes	0
In Parity Errors	0
In Framing Errors	0
In Other Errors	0
Out Other Errors	0

Step 2 To refresh the display, click the refresh icon in the upper right corner of the View Details window.

Managing the Ethernet Interface

To bring up, shut down, or reset the Ethernet interface:

SUMMARY STEPS

1. On the Device Manager main page, click the Ethernet port to display the popup menu and select the operation you want to perform on the interface: **Bring Up**, **Shut Down**, or **Reset**.
2. In the confirmation dialog box that appears, click **Yes** to continue the operation.

DETAILED STEPS

Step 1 On the Device Manager main page, click the Ethernet port to display the popup menu and select the operation you want to perform on the interface: **Bring Up**, **Shut Down**, or **Reset**.

Step 2 In the confirmation dialog box that appears, click **Yes** to continue the operation.

Registering with IoT-FND

When you connect to the IR500 with a work order, the IR500 registers with IoT-FND. Registration notifies IoT-FND that the device is on the network and provides a mechanism for pushing management configuration information to the device.

You can also manually cause the IR500 to re-register with IoT-FND for load balancing or delegation to specific sites. In this case, IoT-FND redirects the IR500 to re-register with an alternate IoT-FND.

To register with IoT-FND, on the Device Manager main page (Dashboard), click **Register with IoT-FND**. Device Manager displays messages to inform you of the redirection status.

Rebooting the IR500

To immediately reboot the IR500, on the Device Manager main page (Dashboard), click **Reboot**. Device Manager displays messages to inform you of the reboot status.

Changing the Configuration

You can view or change the following IR500 settings from the Config page:

Note For detailed information about IR500 operation and configuration, including Raw Socket and MAP-T information, refer to the Cisco IR 500 Series WPAN Gateway and Range Extender Installation and Configuration Guide .

Changing General Settings

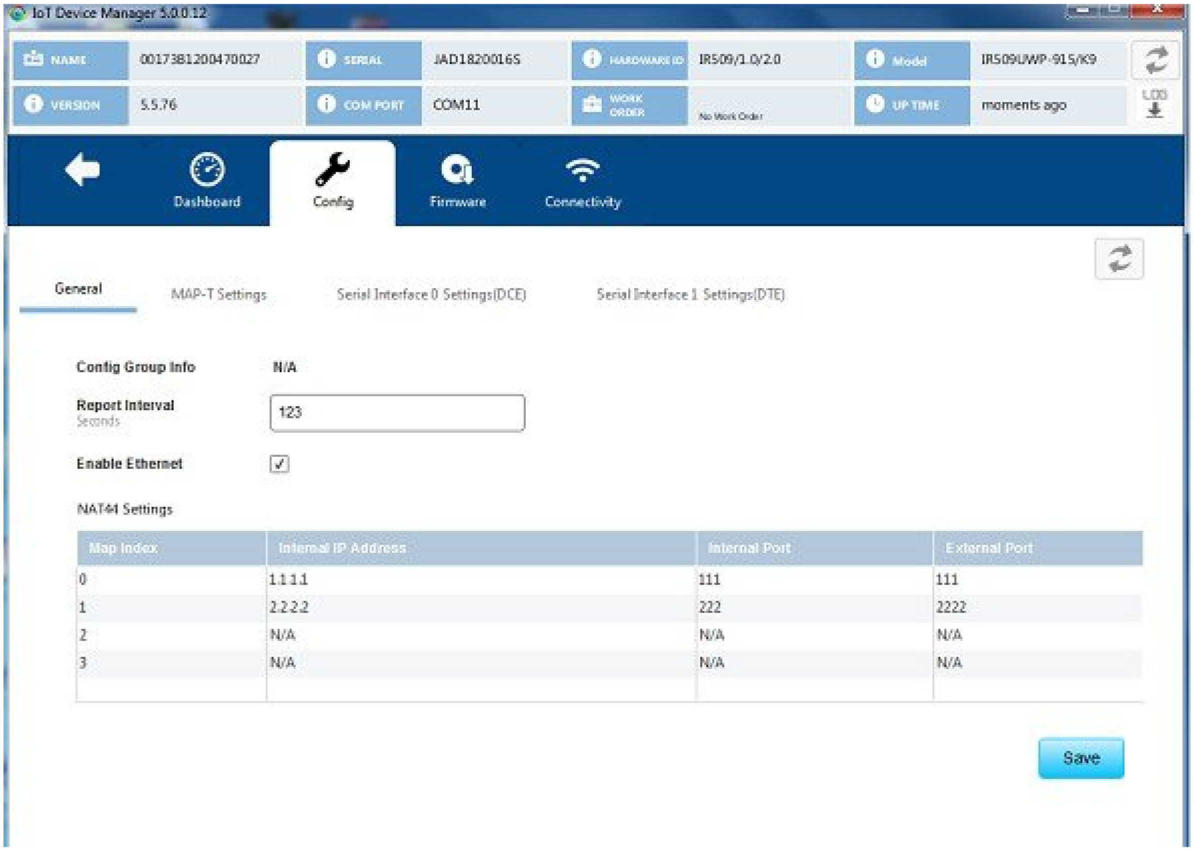
To view or change general IR500 configuration settings:

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. View or modify General settings:
3. Click Save.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
LOG
Save

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

Config Group Info N/A

Report Interval Seconds 123

Enable Ethernet ☑

NAT44 Settings

Map Index	Internal IP Address	Internal Port	External Port
0	1.1.1.1	111	111
1	2.2.2.2	222	2222
2	N/A	N/A	N/A
3	N/A	N/A	N/A

Step 2 View or modify General settings:

- **Config Group Info**: The configuration group that IoT-FND uses to manage devices in bulk. The default config group for the DA Gateway is **default-ir500**.
- **Report Interval**: The number of seconds between data updates. By default, Mesh Endpoints (MEs) send a new set of metrics to IoT-FND every 28,800 seconds (8 hours).
- **Enable Ethernet**: Select this check box for IPv4 connectivity to devices and to enable NAT44 configuration.

- **NAT44 Settings**:
  - Map Index: Identifies the map.
  - Internal IP Address: The internal address of the NAT 44 configured device.
  - Internal Port: The internal port number of the NAT 44 configured device.
  - External Port: The external port number of the NAT 44 configured device.

Step 3 Click Save.

Changing MAP-T Settings

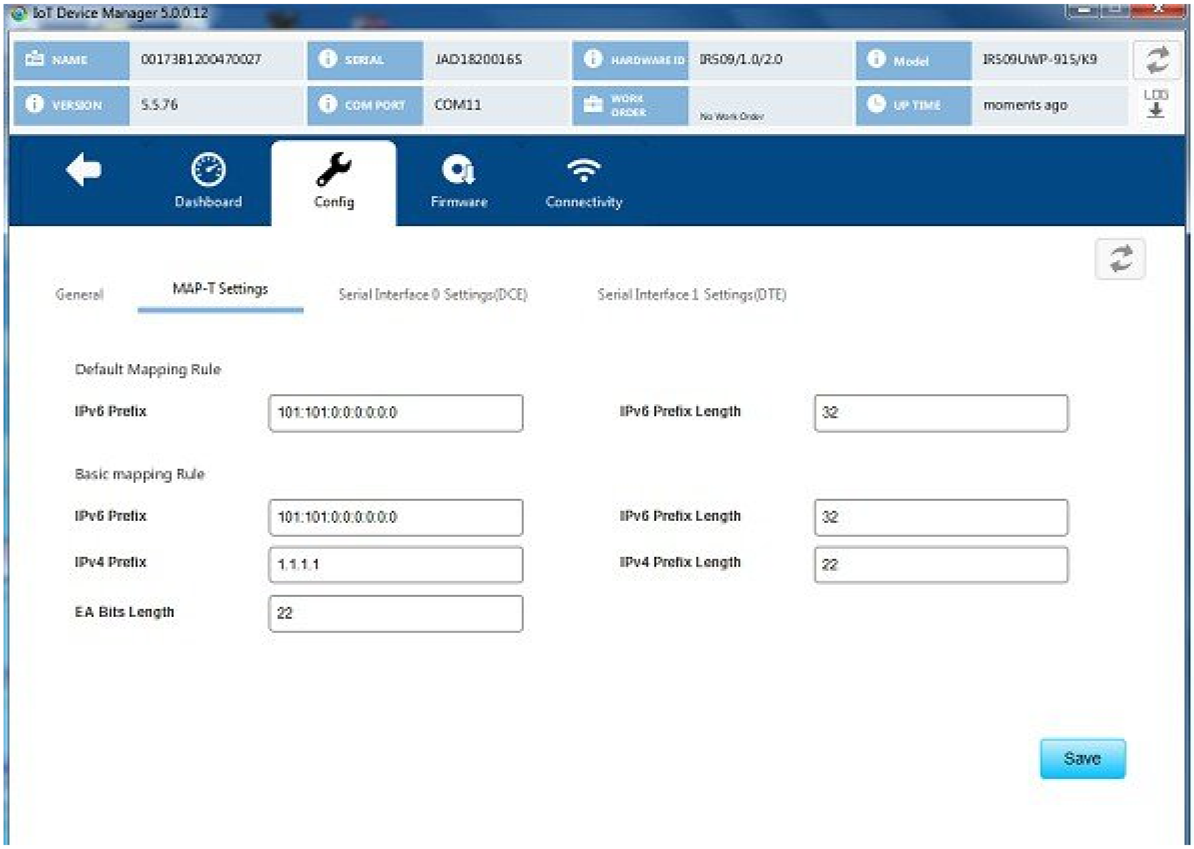
To view or change MAP-T configuration settings:

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **MAP-T Settings** and view or modify these settings:
3. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.



NAME 00173B1200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME moments ago

General | MAP-T Settings | Serial Interface 0 Settings(DCE) | Serial Interface 1 Settings(DTE)

Default Mapping Rule

IPv6 Prefix: 101:101:0:0:0:0:0:0
IPv6 Prefix Length: 32

Basic mapping Rule

IPv6 Prefix: 101:101:0:0:0:0:0:0
IPv6 Prefix Length: 32
IPv4 Prefix: 1.1.1.1
IPv4 Prefix Length: 22
EA Bits Length: 22

Step 2 Click **MAP-T Settings** and view or modify these settings:

- Default Mapping Rule: These fields specify an IPv6 prefix used to address all destinations outside the MAP-T domain.
  - **IPV6 Prefix**: IPv6 prefix used to embed any IPv4 addresses outside the MAP-T domain.
  - **IPV6 Prefix Length**: Length of the IPv6 prefix used to embed any IPv4 addresses outside the MAP-T domain.
- Basic Mapping Rule: These fields specify the IPv6 and IPv4 prefixes used to address MAP-T nodes inside the MAP-T domain.
  - **IPV6 Prefix**: MAP-T IPv6 End-user prefix, which contains the MAP-T Basic Mapping Rule or MAP-T IPv6 prefix + the IPv4 suffix of the assigned IPv4 address.
  - **IPV4 Prefix**: IPv4 prefix that specifies the IPv4 subnet selected to address all IPv4 nodes in a MAP-T domain.
  - **EA Bits Length**: Length of the IPv4 Embedded Address (EA) bits that indicates the length of the IPv4 suffix embedded in the MAP-T IPv6 End-user IPv6 prefix.
  - **IPV6 Prefix Length**: Length of the IPv6 prefix used to embed the IPv4 address of nodes inside the MAP-T domain.
  - **IPV4 Prefix Length**: Length of the IPv4 prefix that specifies the IPv4 subnet selected to address all IPv4 nodes in a MAP-T domain.

Step 3 Click **Save**.

Changing Serial Interface 0 Settings (DCE)

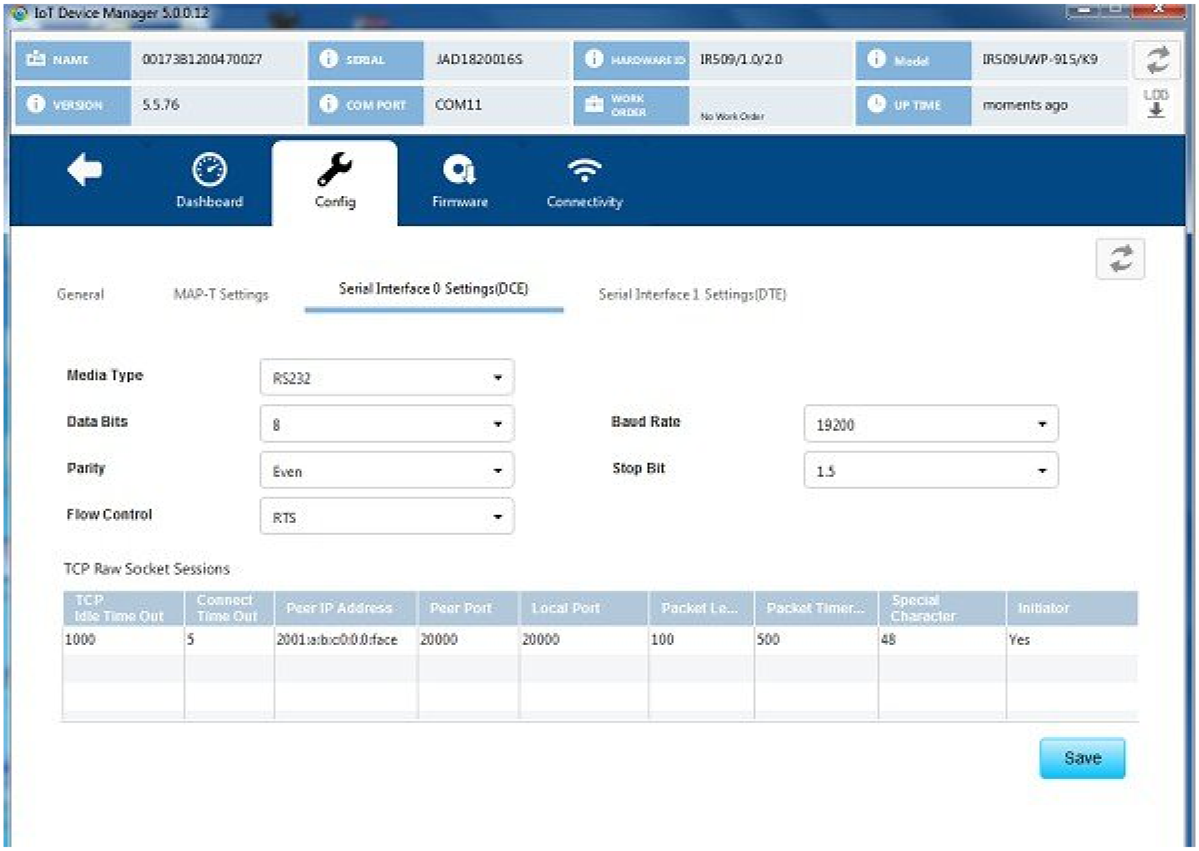
To view or change the configuration for Serial Interface 0 (DCE):

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Serial Interface 0 Settings (DCE)** and view or modify these settings:
3. View or modify settings for TCP Raw Socket Sessions:
4. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
Save

NAME 00173B1200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME moments ago

Media Type: RS232
Data Bits: 8
Parity: Even
Flow Control: RTS
Baud Rate: 19200
Stop Bit: 1.5

TCP Raw Socket Sessions

TCP Idle Time Out	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Le...	Packet Timer...	Special Character	Initiator
1000	5	2001:a:b:c0:0:0:face	20000	20000	100	500	48	Yes

Step 2 Click **Serial Interface 0 Settings (DCE)** and view or modify these settings:

- **Media Type**: The serial interface type.
  - Disable

- LoopBack
- RS232
- RS485 Full Duplex
- RS485 Half Duplex

- **Data Bits**: Number of data bits per character. Default value is 8.
- **Parity**: Odd or even parity for error detection. Default value is None.
- **Flow Control**: The use of flow control on the line. Default value is None.
- **Baud Rate**: Data transmission rate in bits per second. Default value is 115200.
- **Stop Bit**: The asynchronous line stop bit. Default value is 1.

Step 3 View or modify settings for TCP Raw Socket Sessions:

- **TCP Idle Time Out**: The time to maintain an idle connection.
- **Connect Time Out**: TCP client connect timeout for Initiator DA Gateway devices.
- **Peer IP Address**: IP address of the host connected to the device.
- **Peer Port**: Port number of the client/server connected to the device.
- **Local Port**: Port number of the device.
- **Packet Length**: Maximum length of serial data to convert into the TCP packet.
- **Packet Timer (ms)**: The time interval between each TCP packet creation.
- Special Character: The delimiter for TCP packet creation.
- **Initiator**: Designates the device as the client/server.

Step 4 Click **Save**.

Changing Serial Interface 1 Settings (DTE)

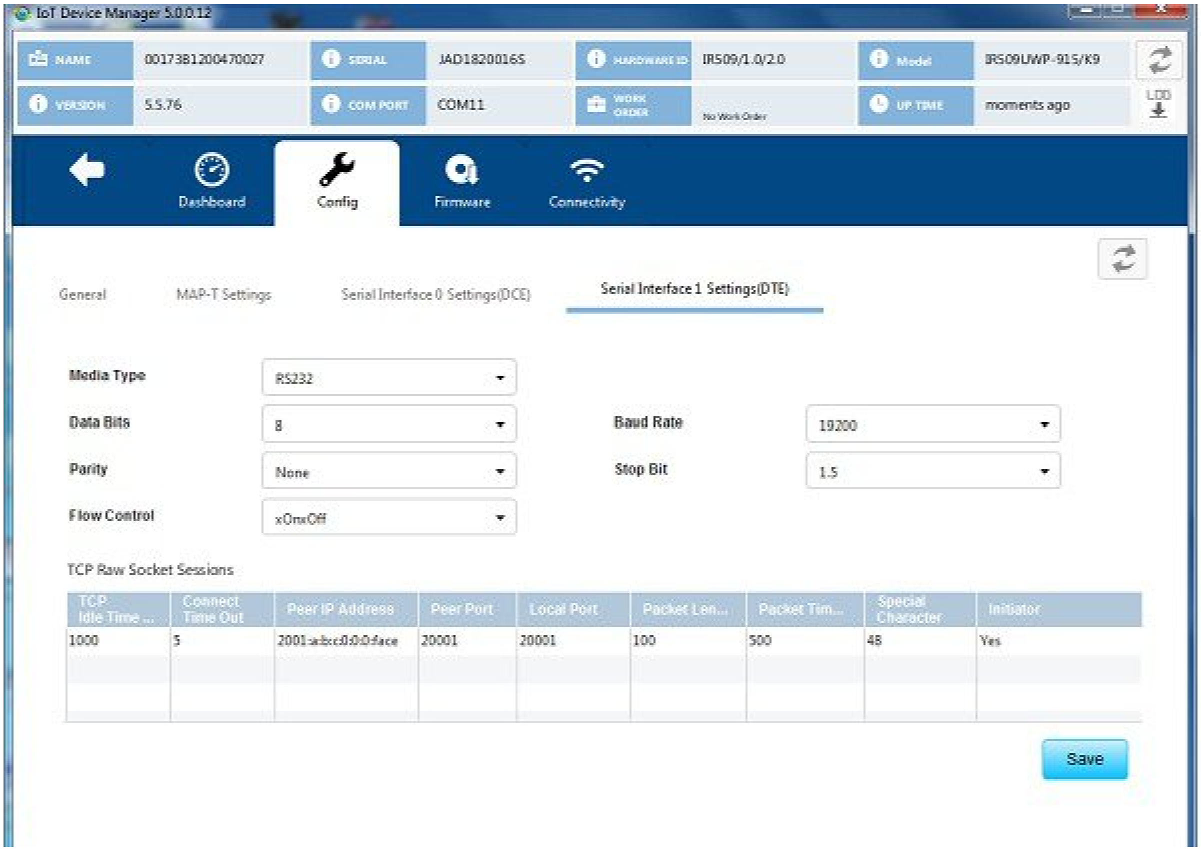
To view or change the configuration for Serial Interface 1 (DTE):

SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click **Serial Interface 1 Settings (DTE)** and view or modify these settings:
3. View or modify settings for TCP Raw Socket Sessions.
4. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.


IoT Device Manager 5.0.0.12
Dashboard
Config
Firmware
Connectivity
General
MAP-T Settings
Serial Interface 0 Settings(DCE)
Serial Interface 1 Settings(DTE)
Save

NAME 00173B1200470027
SERIAL JAD18200165
HARDWARE ID IR509/1.0/2.0
Model IR509UWP-915/K9
VERSION 5.5.76
COM PORT COM11
WORK ORDER No Work Order
UP TIME moments ago

Media Type: RS232
Data Bits: 8
Parity: None
Flow Control: xOnxOff
Baud Rate: 19200
Stop Bit: 1.5

TCP Raw Socket Sessions

TCP Idle Time ...	Connect Time Out	Peer IP Address	Peer Port	Local Port	Packet Len...	Packet Tim...	Special Character	Initiator
1000	5	2001:a:b:c:0:0:0:face	20001	20001	100	500	48	Yes

Step 2 Click **Serial Interface 1 Settings (DTE)** and view or modify these settings:

- **Medial Type**: The serial interface type.
  - Disable
  - LoopBack
  - RS232
  - RS485 Full Duplex
  - RS485 Half Duplex
- **Data bits**: The number of data bits per character. Default value is 8.
- **Parity**: Odd or even parity for error detection. Default value is None.
- **Flow Control**: The use of flow control on the line. Default value is None.
- **Baud Rate**: The data transmission rate in bits per second. Default value is 115200.
- **Stop Bit**: The asynchronous line stop bit. Default value is 1.

Step 3 View or modify settings for TCP Raw Socket Sessions.

- **TCP Idle Time Out**: The time to maintain an idle connection.
- **Connect Time Out**: TCP client connect timeout for Initiator DA Gateway devices.
- **Peer IP Address**: IP address of the host connected to the device.
- **Peer Port**: Port number of the client/server connected to the device.
- **Local Port**: Port number of the device.
- **Packet Length**: Maximum length of serial data to convert into the TCP packet.
- **Packet Timer (ms)**: The time interval between each TCP packet creation.
- Special Character: The delimiter for TCP packet creation.
- **Initiator**: Designates the device as the client/server.

Step 4 Click **Save**.

Changing ACL Settings

To view or change ACL configuration settings:

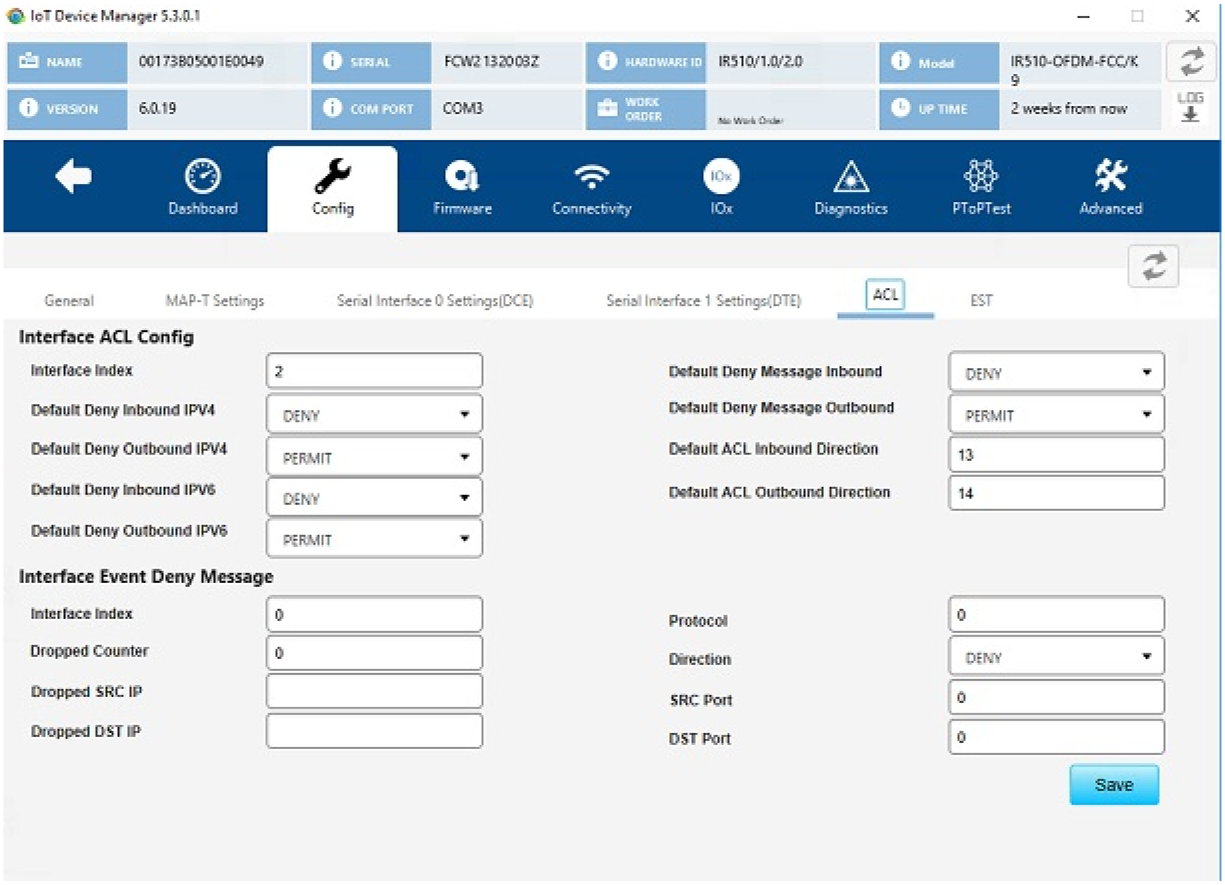
SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click the **ACL** tab and view or modify the settings.
3. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click the **ACL** tab and view or modify the settings.



NAME	00173805001E0049	SERIAL	FCW2132003Z	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.0.19	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	2 weeks from now

Interface ACL Config

Interface Index: 2

Default Deny Inbound IPV4: DENY

Default Deny Outbound IPV4: PERMIT

Default Deny Inbound IPV6: DENY

Default Deny Outbound IPV6: PERMIT

Default Deny Message Inbound: DENY

Default Deny Message Outbound: PERMIT

Default ACL Inbound Direction: 13

Default ACL Outbound Direction: 14

Interface Event Deny Message

Interface Index: 0

Dropped Counter: 0

Dropped SRC IP:

Dropped DST IP:

Protocol: 0

Direction: DENY

SRC Port: 0

DST Port: 0

Step 3 Click **Save**.

Changing EST Settings

To view or change EST settings:

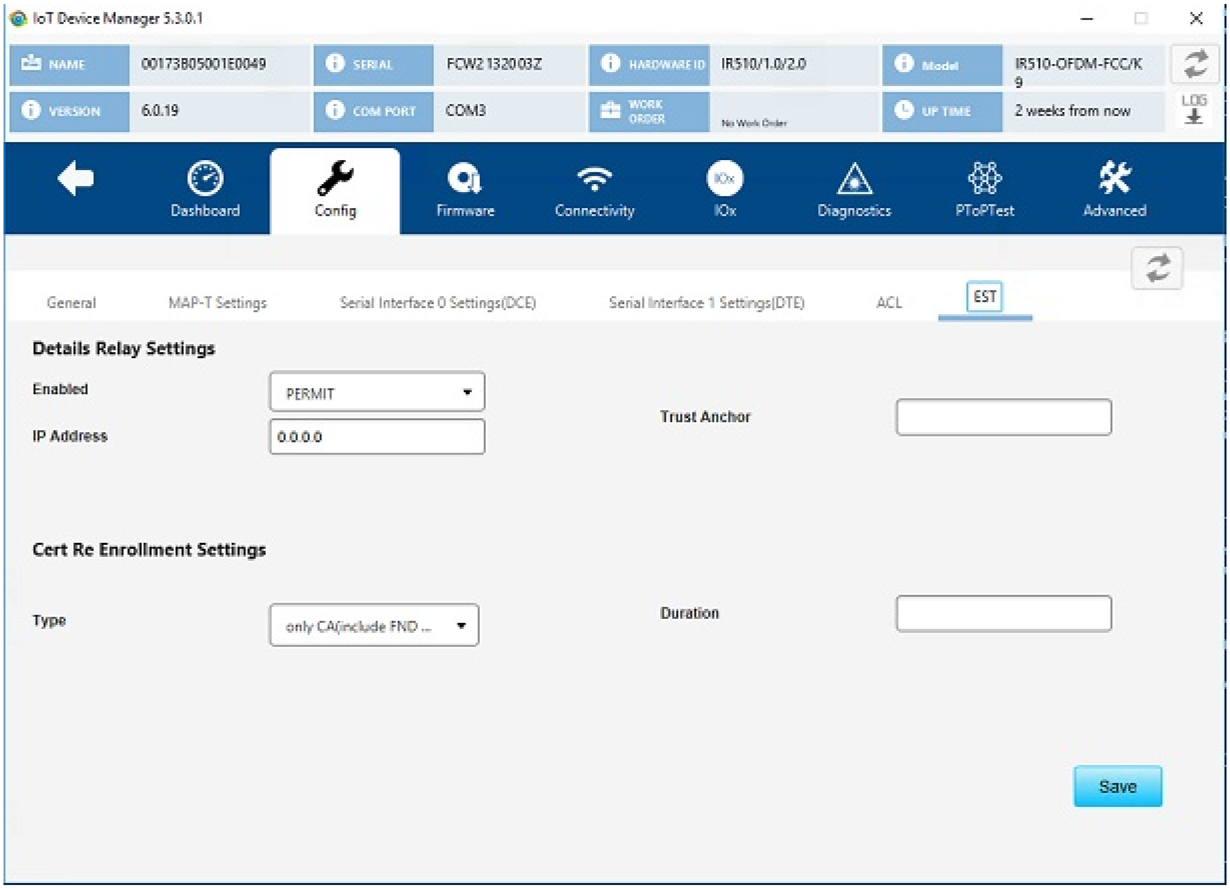
SUMMARY STEPS

1. On the Device Manager main page, click the **Config** tab.
2. Click the **EST** tab and view or modify the settings.
3. Click **Save**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click the **EST** tab and view or modify the settings.



NAME 00173B05001E0049
SERIAL FCW2132003Z
HARDWARE ID IR510/1.0/2.0
Model IR510-OFDM-FCC/K9
VERSION 6.0.19
COM PORT COM3
WORK ORDER No Work Order
UP TIME 2 weeks from now

Details Relay Settings

Enabled: PERMIT

IP Address: 0.0.0.0

Trust Anchor:

Cert Re Enrollment Settings

Type: only CA(include FND ...

Duration:

Step 3 Click **Save**.

Generating and Uploading Bootstrap Configuration

To generate and upload bootstrap configuration files, follow these steps:

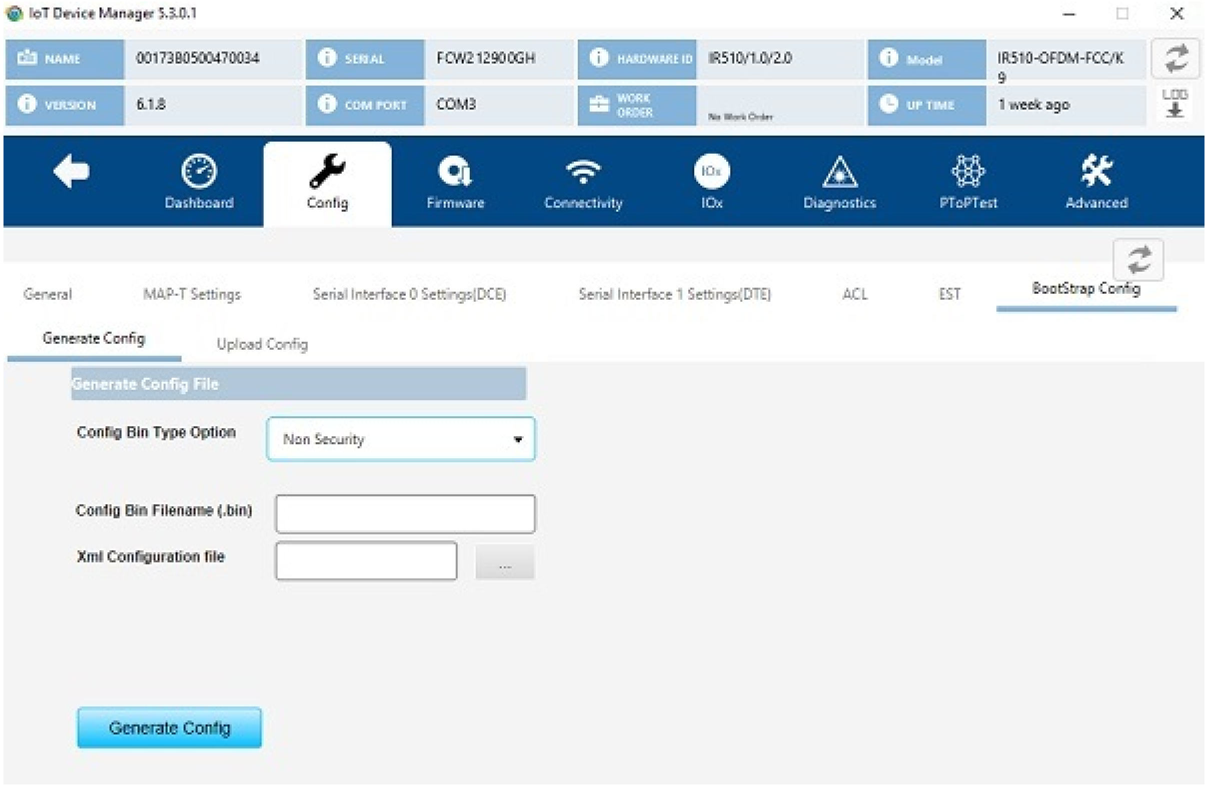
Before you begin

From IoT Device Manager Release 5.5, you can generate and upload bootstrap configuration files to one or more IR510 devices with Cisco Resilient Mesh Release 6.0 and later.

Step 1 On the Device Manager main page, click the **Config** tab.

Step 2 Click the **BootStrap Config** tab and then click the **Generate Config** subtab.

a) To generate non security bootstrap configurations, choose **Non Security** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, and browse to choose the XML configuration file to be provided as input, as shown in the following figure.



IoT Device Manager 5.3.0.1

NAME: 00173B0500470034
SERIAL: FCW212900GH
HARDWARE ID: IR510/1.0/2.0
Model: IR510-OFDM-FCC/K9
VERSION: 6.1.8
COM PORT: COM3
WORK ORDER: No Work Order
UP TIME: 1 week ago

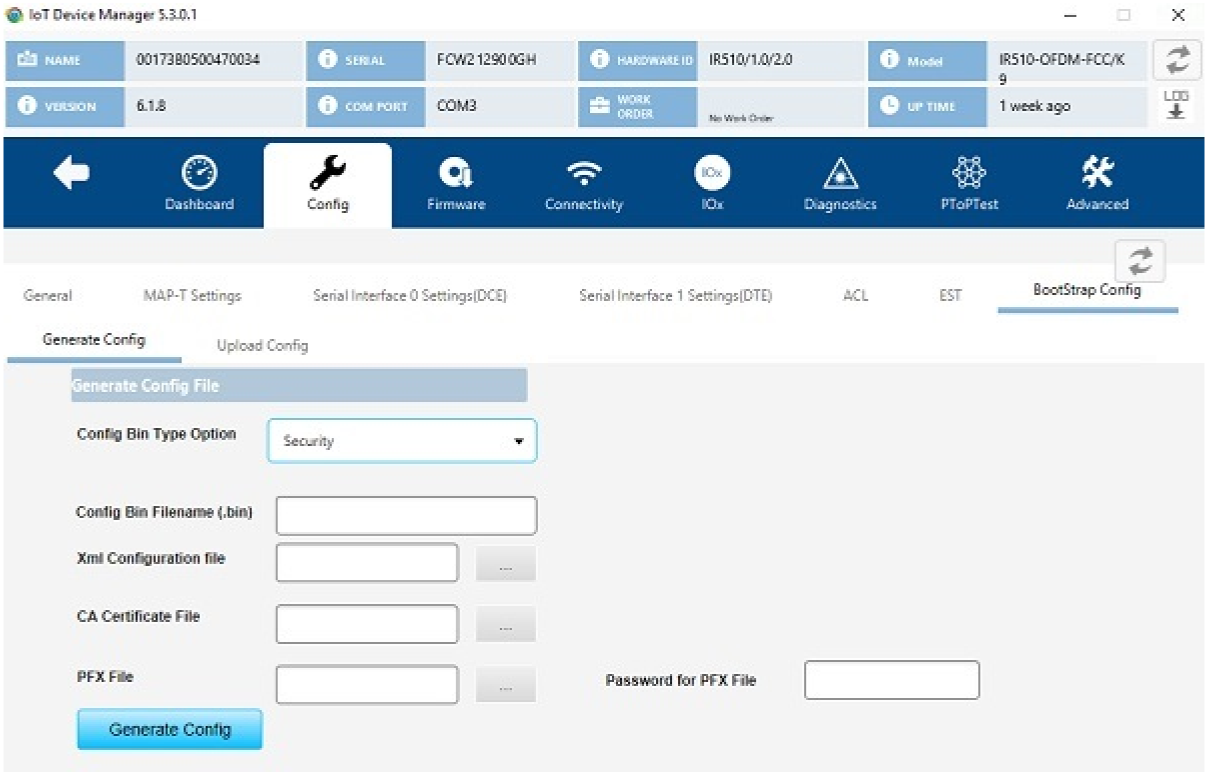
Generate Config File

Config Bin Type Option: Non Security

Config Bin Filename (.bin)

Xml Configuration file

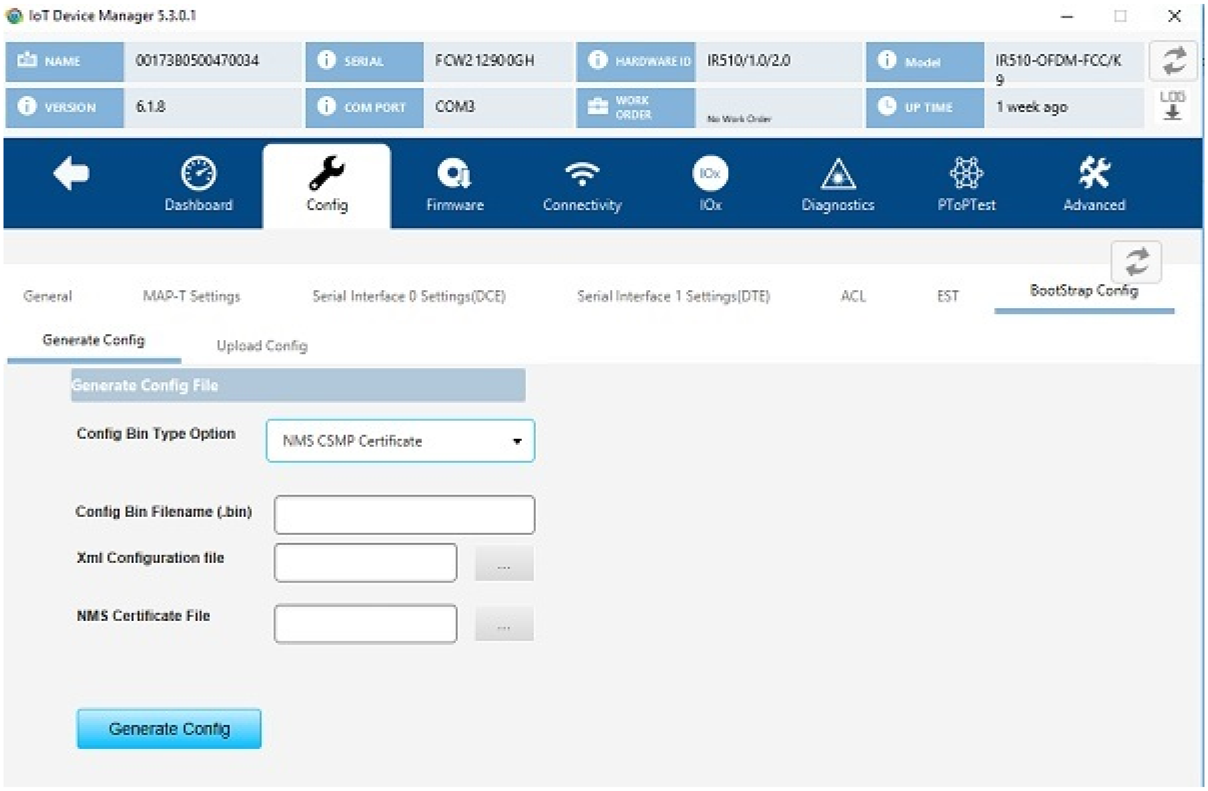
b) To generate security bootstrap configurations, choose **Security** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, browse to choose the XML configuration file to be provided as input, the CA certificate file and PFX file, and enter the password for the PFX file, as shown in the following figure.



NAME: 00173B0500470034
SERIAL: FCW2129000GH
HARDWARE ID: IR510/1.0/2.0
Model: IR510-OFDM-FCC/K9
VERSION: 6.1.8
COM PORT: COM3
WORK ORDER: No Work Order
UP TIME: 1 week ago

Config Bin Type Option: Security
Config Bin Filename (.bin):
Xml Configuration file:
CA Certificate File:
PFX File:
Password for PFX File:

c) To generate bootstrap configuration with NMS CSMP certificate, choose **NMS CSMP Certificate** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, browse to choose the XML configuration file to be provided as input and the NMS certificate file for connecting to FND, as shown in the following figure.



NAME 00173B0500470034
SERIAL FCW21290GH
HARDWARE ID IR510/1.0/2.0
Model IR510-OFDM-FCC/K9
VERSION 6.1.8
COM PORT COM3
WORK ORDER No Work Order
UP TIME 1 week ago

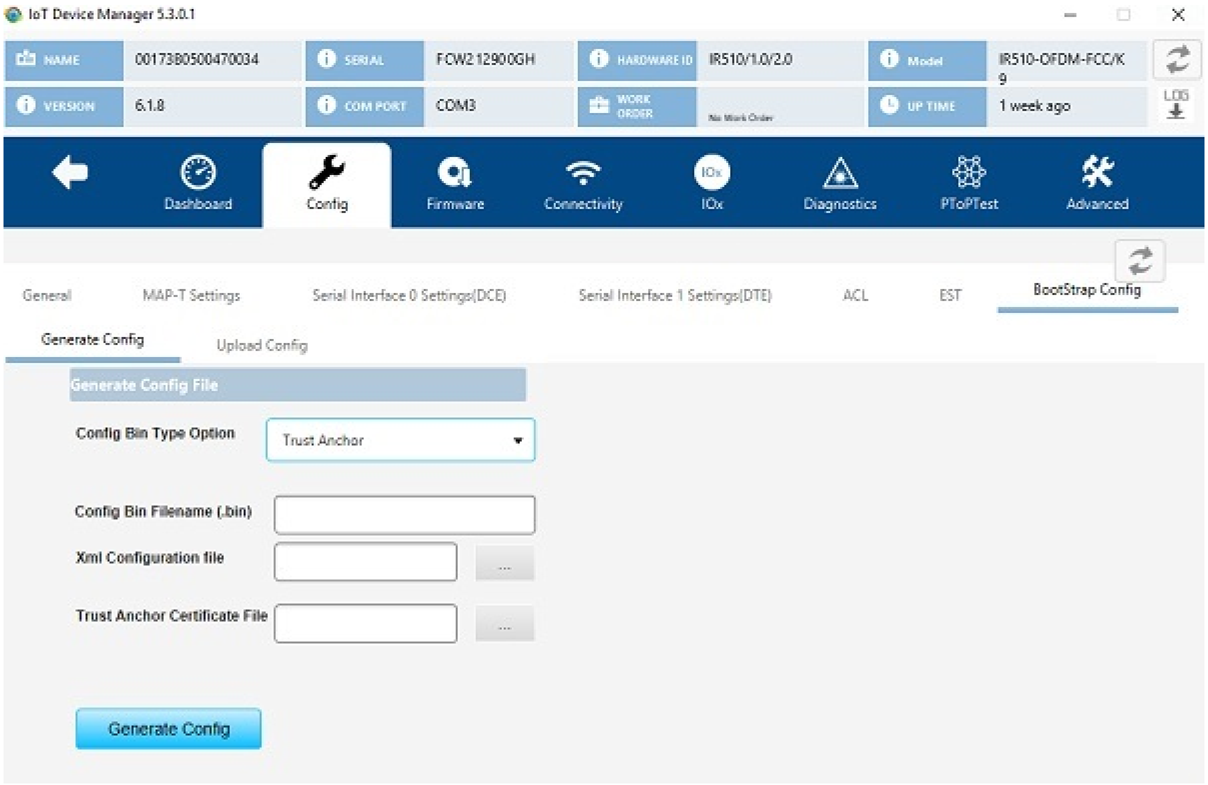
Config Bin Type Option: NMS CSMP Certificate

Config Bin Filename (.bin):

Xml Configuration file:

NMS Certificate File:

d) To generate bootstrap configuration with trustanchor for EST, choose **Trust Anchor** from the **Config Bin Type Option** drop-down list, enter the filename of the configuration bin to be generated, browse to choose the XML configuration file to be provided as input and the Trust Anchor certificate file for EST, as shown in the following figure.

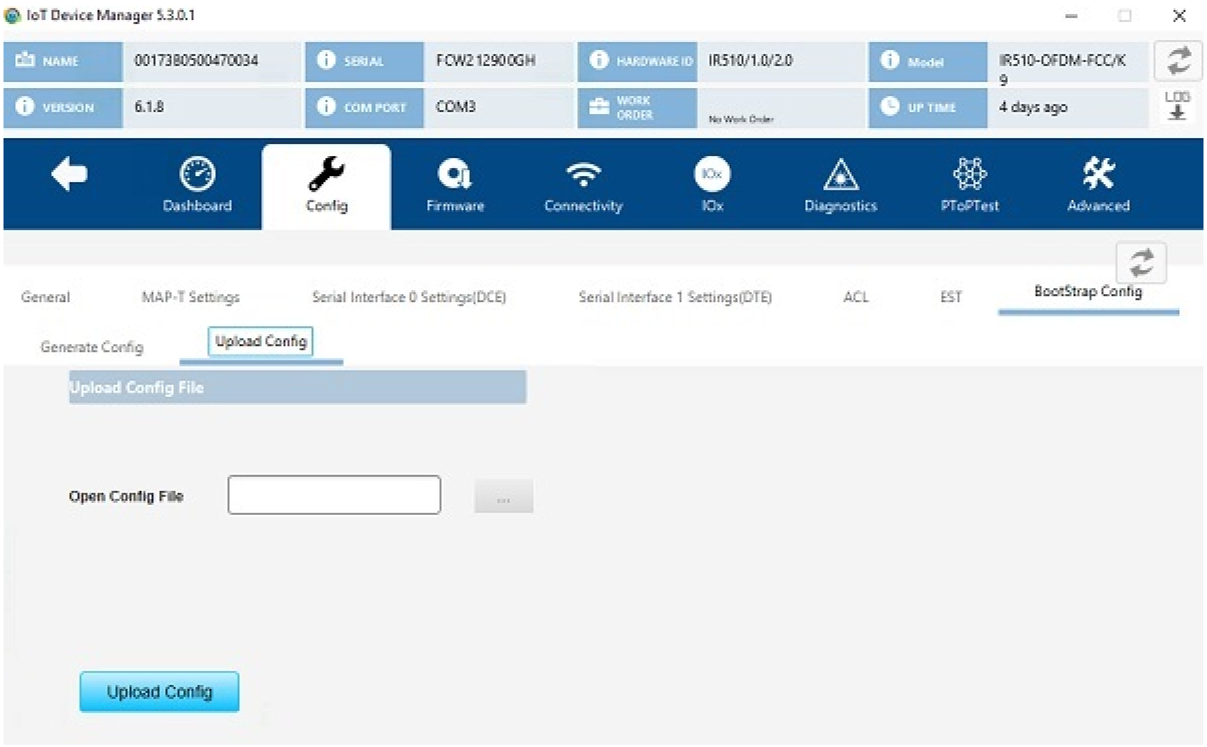


NAME 0017380500470034
SERIAL FCW21290OGH
HARDWARE ID IR510/1.0/2.0
Model IR510-OFDM-FCC/K9
VERSION 6.1.8
COM PORT COM3
WORK ORDER No Work Order
UP TIME 1 week ago

Config Bin Type Option: Trust Anchor
Config Bin Filename (.bin)
Xml Configuration file
Trust Anchor Certificate File

Step 3 Click the Generating Config button. The configuration bin file is created and a dialog box appears showing the location of the created configuration bin file. If there are errors while creating the configuration bin file, the error is shown in the dialog box.

Step 4 Click the **Uplooad Config** subtab.



IoT Device Manager 5.3.0.1

NAME	0017380500470034	SERIAL	FCW212900GH	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.1.8	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	4 days ago

Open Config File

Step 5 Browse to choose the location of the config bin file in the **Open Config File** field.

Step 6 Click the Upload Config button. The configuration bin file is executed in the device and a dialog box appears with a success message. If there are any errors while executing the configuration bin file, the error is shown to in the dialog box.

Updating the Firmware Image

Use the Firmware page to perform these tasks: upload an image, install an image, and set the backup.

Uploading an Image

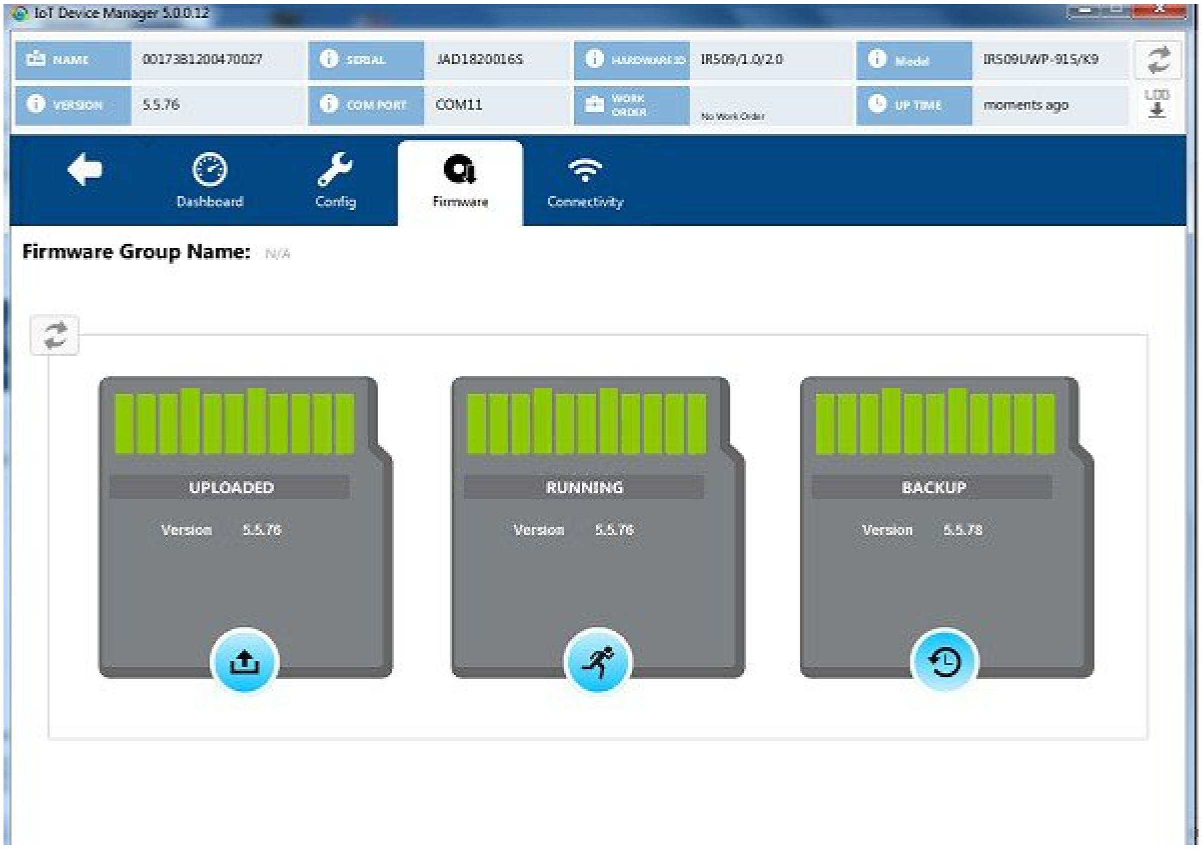
To upload an image to the IR500:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. On the left of the Firmware page, click the Upload icon and select an image to upload. The new image is stored on the IR500 until you are ready to install the image on the IR500. (See Installing an Image, on page 43.)
3. In the dialog box that appears, click **Yes** to upload the selected image.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.



IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

Firmware Group Name: N/A

UPLOADED	RUNNING	BACKUP
Version 5.5.76	Version 5.5.76	Version 5.5.78

Step 2 On the left of the Firmware page, click the Upload icon and select an image to upload. The new image is stored on the IR500 until you are ready to install the image on the IR500. (See Installing an Image, on page 43.)

Step 3 In the dialog box that appears, click **Yes** to upload the selected image.

Installing an Image

To install an uploaded image on the IR500:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. In the middle of the Firmware page, click the Install icon.
3. In the dialog box that appears, click **Yes** to install the image on the IR500.
4. In the dialog box that appears after the installation is completed, click **Save Results** or **OK**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 In the middle of the Firmware page, click the Install icon.

Step 3 In the dialog box that appears, click **Yes** to install the image on the IR500.

If you did not previously upload an image to install, Device Manager displays the Upload to Device dialog box for you to upload an image.

After you confirm the installation, the image installs automatically on the device. No manual reboot is required.

Step 4 In the dialog box that appears after the installation is completed, click **Save Results** or **OK**.

Setting the Backup

To set the running image as the backup image:

SUMMARY STEPS

1. On the Device Manager main page, click the **Firmware** tab.
2. On the right of the Firmware page, click the Set Backup icon.
3. In the dialog box that appears, click **Yes**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Firmware** tab.

Step 2 On the right of the Firmware page, click the Set Backup icon.

Step 3 In the dialog box that appears, click **Yes**.

Testing Connectivity

Use the Connectivity page to test connectivity to a target with an IPv6 address. You can test connectivity of the Ethernet or 6LoWPAN interface.

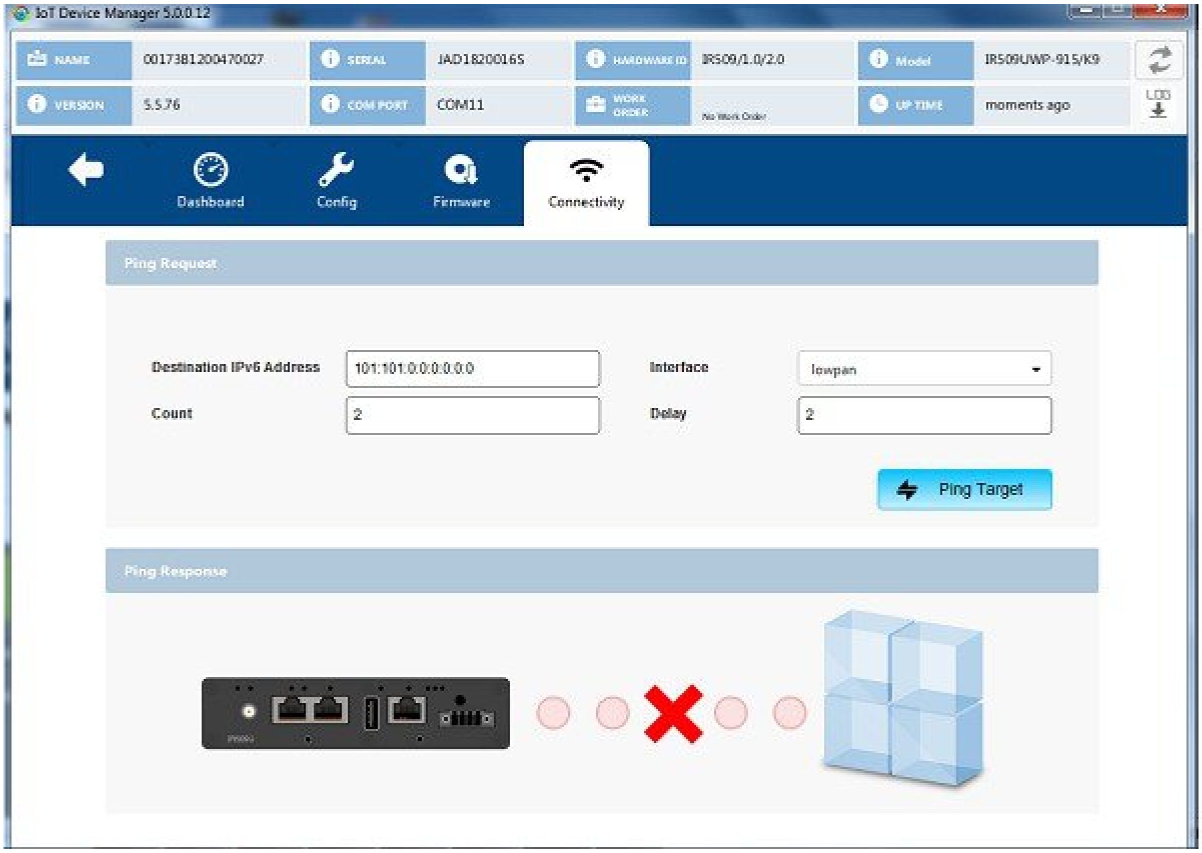
To test connectivity:

SUMMARY STEPS

1. On the Device Manager main page, click the **Connectivity** tab.
2. Configure the Ping Request settings:
3. Click **Ping Target**.

DETAILED STEPS

Step 1 On the Device Manager main page, click the **Connectivity** tab.



IoT Device Manager 5.0.0.12

NAME	00173B1200470027	SERIAL	JAD18200165	HARDWARE ID	IR509/1.0/2.0	Model	IR509UWP-915/K9
VERSION	5.5.76	COM PORT	COM11	WORK ORDER	No Work Order	UP TIME	moments ago

Ping Request

Destination IPv6 Address: 101:101:0:0:0:0:0:0
Interface: lowpan
Count: 2
Delay: 2

Step 2 Configure the Ping Request settings:

- **Destination IPv6 Address:** IPv6 address of the ping target
- **Interface**:
  - **eth**: Ethernet.
  - **lowpan:** 6LoWPAN.
- **Count**: Number of ping requests to send (0 to 9).
- **Delay**: Number of seconds to wait between sending each request (0 to 9).

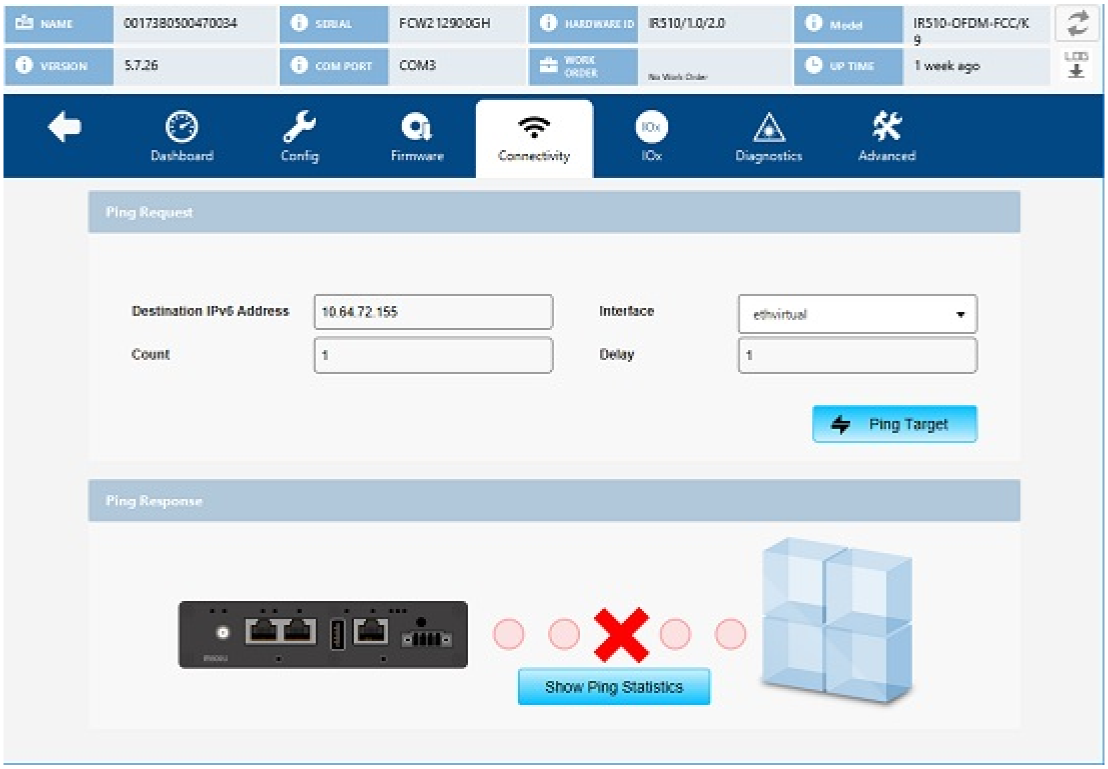
Step 3 Click **Ping Target**.

A dialog box appears indicating that the IR500 is attempting to ping the target IPv6 address. When the IR500 successfully pings the target, the Ping Response area of the Connectivity page displays a green check mark. If the ping is unsuccessful, the response area displays a red X.

To see the contents of the ping response message as a tooltip, hover over the icon for the target device.

Ping Test Enhancement on IR510

Under Connectivity tab, **Show Ping Statistics** is supported for IR510. On clicking this button, a dialog box will be displayed to show the details of the ping operation performed. This function is disabled by default. Once the Ping operation is completed, the **Show Ping Statistics** button will be enabled.



NAME	00173805004700034	SERIAL	FCW212900GH	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	5.7.26	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	1 week ago

Ping Request

Destination IPv6 Address: 10.64.72.155
Interface: ethvirtual
Count: 1
Delay: 1

Ping Response

Offline Authorization—FTT Secured Wireless Console for IR510

In IoT-Device Manager Release 5.6, an authorization security procedure is introduced between IoT-DM FTT wireless console and target node (IR510) by using wireless console authorize TLV 342. Currently, FTT wireless console session with target nodes from IoT-DM is validating the connection by following an authentication procedure through DTLS certificates. However, DTLS channel is suspectable for various security attacks (man-in-the-middle, Denial of Service attacks, and so on) as well as security vulnerabilities. This feature will ensure the target node to connect and process the request from a legible source. As part of this feature, IoT-DM will receive signed authorization TLV 342 message byte array from FND through work order. IoT-DM will send the authorization message to target after the successful post operation of TLV 341 to the neighboring target node and DTLS secure channel establishment. Based on the authorization response received from target node, IoT-DM will process the same and start the wireless console session with supported authorized TLV's. This way the device node will execute only the communicated authorize TLV commands.

Note

- This feature cannot work when IR510 is connected to COM port or connected without work order option.
- IPV4 connectivity from IoT-DM to relay node is not supported.
- Management command is not supported.

As shown in the following figures, the FND admin creates the work order with authorization message which contains wireless authorize console TLV and FND signature TLV and the same will be assigned to IoT-DM. You need to connect to the device through the respective work order. While starting the wireless console, IoT-DM will transfer the authorization message to the target after establishing the DTLS channel. Target node validates the same and send the response to the IoT-DM and IoT-DM process the response. If it is a successful response, IoT-DM will perform a get TLV 342 operation and based on the get response TLV command execution session start with supported TLV's list received as part of TLV 342 get request.

Figure 3: Authorization TLV Message Procedure

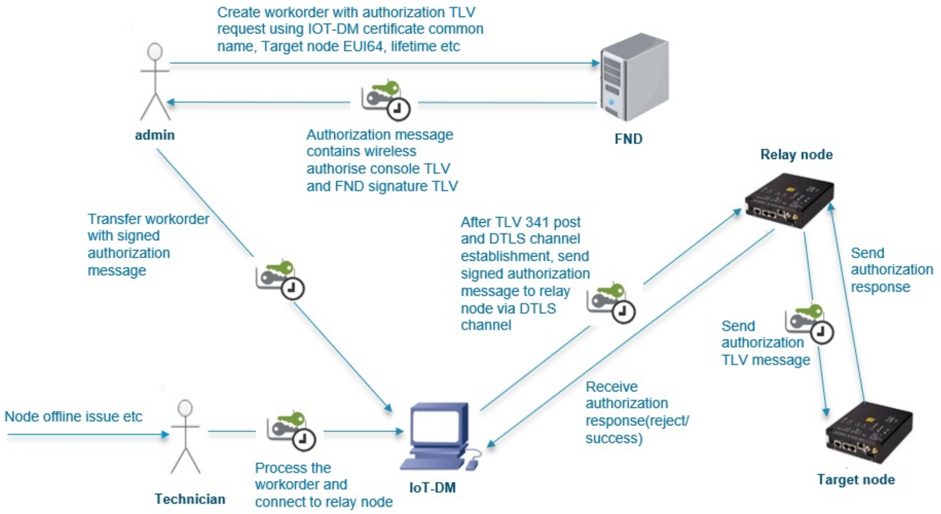
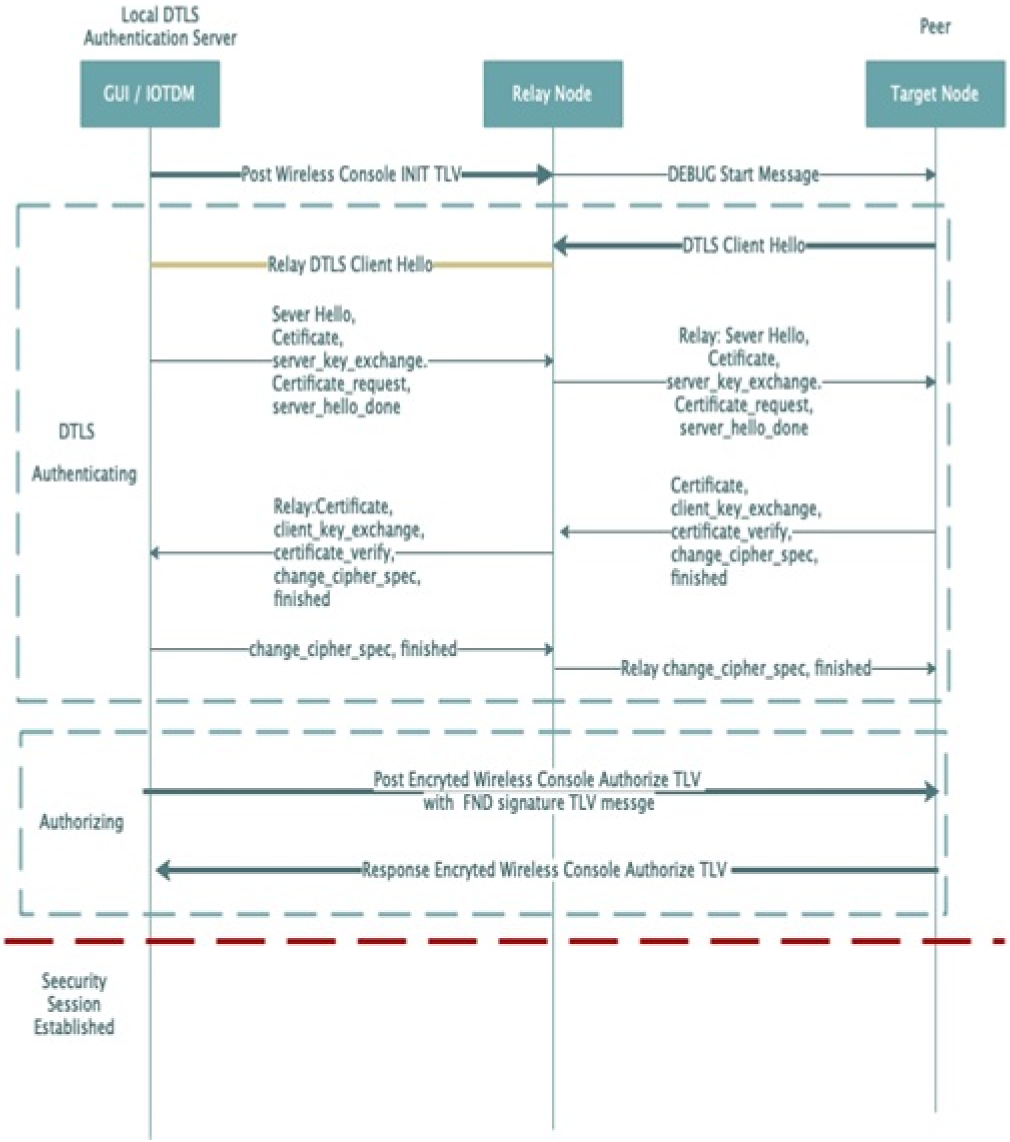

Create workorder with authorization TLV request using IOT-DM certificate common name, Target node EUI64, lifetime etc
admin
Authorization message contains wireless authorise console TLV and FND signature TLV
FND
Relay node
Transfer workorder with signed authorization message
After TLV 341 post and DTLS channel establishment, send signed authorization message to relay node via DTLS channel
Send authorization response
Send authorization TLV message
Receive authorization response(reject/ success)
Node offline issue etc
Technician
Process the workorder and connect to relay node
IoT-DM
Target node

Figure 4: Authorization Message Request Procedure Between IoT-DM and Target Node


Local DTLS Authentication Server
Peer
GUI / IOTDM
Relay Node
Target Node
Post Wireless Console INIT TLV
DEBUG Start Message
DTLS Client Hello
Relay DTLS Client Hello
Sever Hello, Cetificate, server_key_exchange. Certificate_request, server_hello_done
Relay: Sever Hello, Cetificate, server_key_exchange. Certificate_request, server_hello_done
DTLS
Authenticating
Relay:Certificate, client_key_exchange, certificate_verify, change_cipher_spec, finished
Certificate, client_key_exchange, certificate_verify, change_cipher_spec, finished
change_cipher_spec, finished
Relay change_cipher_spec, finished
Post Encryted Wireless Console Authorize TLV with FND signature TLV messge
Authorizing
Response Encryted Wireless Console Authorize TLV
Seecurity Session Established

FND will send a work order with its type, whether it is FTT or Non-FTT work order. After Sync up with FND, IoT-DM will list the work order with the type parameter in the work order table. If you want to enable the FTT feature, you need to choose the respective work order type.

Prerequisites

- SSM[CSMP] service should be up and running in FND. You should be able to download CSMP certificate from UI [Admin -> certificates -> certificate for CSMP].
- Target node EID should be present in the FND endpoint.
- Configure IPv6 address on relay node ethernet interface and then program it with security mode enabled.
- Sample Relay node configuration: **decxu_sec.xml**

Import **FTT.keystore** into IOT-DM which contains the following three certificates with alias of ca_cert, server_cert, server.key:

1. root_ca_ec.crt—Root CA's public key, for verifying the client certificate.

2. server_ec.crt—DTLS server's certificate signed by root CA's private key for TLS handshake. Client will use the root CA's public key to verify it.

3. server_pk8.key—DTLS server's private key, for representing himself in TLS handshake.

- Program the Target node with following certificates, keys and config.xml:

  1. root_ca_ec.der—Root CA's public key. (Same Root CA certificate is used, but it is converted in to der format.)

  2. client_ec.der —Generate CSR in any linux and get it signed by root CA's private key and convert into der format.

  3. client_pk8.der—Generate private key in pkcs8 standard and convert into der format.

  4. nms_ec.der— Export the CSMP certificate (SSM cert) from FND and convert into der format.

  5. decxu_sec.xml—Same as relay node enable security mode and config.xml properties should be the same as relay xml config SSID, phy-mode, TX power ReqSignedPost, and ReqValidCheckPost

  6. Sample Target node configuration: decxu_sec.xml

- From Relay node to target node, RSSI strength should be good. To verify this, you can use TLV - 52 [Neighbor802154G].

  1. -90 <= -60 - Good

  2. -100 <= -90 - Fair

  3. -110 <= -100 - Poor

- FND should be release 4.6.115 and later

- IOT-DM should be Release 5.6.0.25 and later

- Mesh (IR510) should be Release 6.2.19 and later. Target and Relay should have the same firmware.

Note FTT is not supported when IR510 is connected to COM Port. IPV4 connectivity from IoT-DM to relay node is not supported.

Steps to Install Custom Certificates (jboss) in the Browser Client for FND

- Export the custom certificate from CA server in *.pfx format and keep in below directory,

  ```
  cd /opt/cgms/server/cgms/conf/
  ```

- Rename the following files to keep as backup jbossas.keystore, vault.keystore and VAULT.dat

  Delete existing jbossas.keystore, vault.keystore and VAULT.dat

- To view the certificate in pfx format:

  ```
  keytool -list -v -keystore <BGL_CA.pfx> -storetype pkcs12
  ```

  Copy the alias <**lab-win-bhl6pvc7ngu-ca**> to import it into the new jbossas.keystore file.

- Import the certificate into jbossas.keystore with the alias name of jboss:

  ```
  keytool -importkeystore -v -srckeystore <BGL_CA.pfx> -srcstoretype pkcs12 -destkeystore
   /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks -srcalias
  <lab-win-bhl6pvc7ngu-ca> -destalias jboss -destkeypass <your_keystore_password>
  ```

  Enter destination keystore password: <keystore>

  Enter source keystore password: <keystore>

  [Storing /opt/cgms/server/cgms/conf/jbossas.keystore]

- Create a new vault.keystore file:

  ```
  keytool -genseckey -alias vault -storetype jceks -keyalg AES -keysize 128 -storepass
  <your_keystore_password> -keypass <your_keystore_password> -keystore
  /opt/cgms/server/cgms/conf/vault.keystore
  ```

- Update the VAULT.dat file with the new password: [/opt/cgms/server/cgms/conf/VAULT.dat file - Keystore password is stored]

  ```
  /opt/cgms/bin/vault.sh -k /opt/cgms/server/cgms/conf/vault.keystore -p
  <your_keystore_password> -e /opt/cgms/server/cgms/conf -i 50 -s 12345678 -v vault -b
  keystore_pass -a password -x <your_keystore_password>
  ```

  Example:

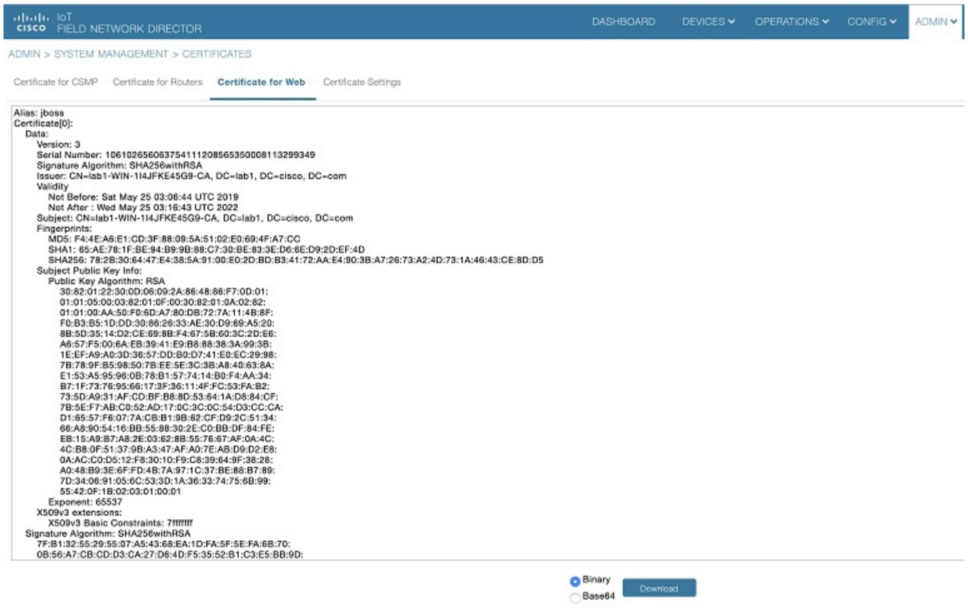
  ```
  Vault Configuration in AS7 config file:
  *******************************************
  </extensions>
  <vault>
  <vault-option name="KEYSTORE_URL" value="/opt/cgms/server/cgms/conf/vault.keystore"/>
  <vault-option name="KEYSTORE_PASSWORD" value="MASK-VKsAwH928fwt.3H2qUwOG"/>
  <vault-option name="KEYSTORE_ALIAS" value="vault"/>
  <vault-option name="SALT" value="12345678"/>
  <vault-option name="ITERATION_COUNT" value="50"/>
  <vault-option name="ENC_FILE_DIR" value="/opt/cgms/server/cgms/conf/"/>
  </vault><management> ...
  ```

- Take backup of following two files: /opt/cgms/standalone/configuration/standalone.xml and standalone-cluster.xml

  Update the generated vault tags in /opt/cgms/standalone/configuration/standalone.xml or standalone-cluster.xml file.

- service cgms restart

- When FND comes up, check for the updated custom certificate either through browser view certificate or through login to FND and choose Admin → Certificate → Certificate For Web.



```
Alias: jboss
Certificate[0]:
  Data:
    Version: 3
    Serial Number: 106102656063754111208565350008113299349
    Signature Algorithm: SHA256withRSA
    Issuer: CN=lab1-WIN-1I4JFKE45G9-CA, DC=lab1, DC=cisco, DC=com
    Validity
      Not Before: Sat May 25 03:06:44 UTC 2019
      Not After : Wed May 25 03:16:43 UTC 2022
    Subject: CN=lab1-WIN-1I4JFKE45G9-CA, DC=lab1, DC=cisco, DC=com
    Fingerprints:
      MD5: F4:4E:A6:E1:CD:3F:88:09:5A:51:02:E0:69:4F:A7:CC
      SHA1: 65:AE:78:1F:BE:94:B9:9B:88:C7:30:BE:83:3E:D6:6E:D9:2D:EF:4D
      SHA256: 78:2B:30:64:47:E4:38:5A:91:00:E0:2D:BD:B3:41:72:AA:E4:90:3B:A7:26:73:A2:4D:73:1A:46:43:CE:8D:D5
    Subject Public Key Info:
      Public Key Algorithm: RSA
        30:82:01:22:30:0D:06:09:2A:86:48:86:F7:0D:01:
        01:01:05:00:03:82:01:0F:00:30:82:01:0A:02:82:
        01:01:00:AA:50:F0:6D:A7:80:DB:72:7A:11:4B:8F:
        F0:B3:B5:1D:DD:30:86:26:33:AE:30:D9:69:A5:20:
        8B:5D:35:14:D2:CE:69:8B:F4:67:5B:60:3C:2D:E6:
        A6:57:F5:00:6A:EB:39:41:E9:B8:88:38:3A:99:3B:
        1E:EF:A9:A0:3D:36:57:DD:B0:D7:41:E0:EC:29:98:
        7B:78:9F:B5:98:50:7B:EE:5E:3C:3B:A8:40:63:8A:
        E1:53:A5:95:96:0B:78:B1:57:74:14:B0:F4:AA:34:
        B7:1F:73:76:95:66:17:3F:36:11:4F:FC:53:FA:B2:
        73:5D:A9:31:AF:CD:BF:B8:8D:53:64:1A:D8:84:CF:
        7B:5E:F7:AB:C0:52:AD:17:0C:3C:0C:54:D3:CC:CA:
        D1:65:57:F6:07:7A:CB:B1:9B:62:CF:D9:2C:51:34:
        66:A8:90:54:16:BB:55:88:30:2E:C0:BB:DF:84:FE:
        EB:15:A9:B7:A8:2E:03:62:8B:55:76:67:AF:0A:4C:
        4C:B8:0F:51:37:9B:A3:47:AF:A0:7E:AB:D9:D2:E8:
        0A:AC:C0:D5:12:F8:30:10:F9:C8:39:64:9F:38:28:
        A0:48:B9:3E:6F:FD:4B:7A:97:1C:37:BE:88:B7:89:
        7D:34:06:91:05:6C:53:3D:1A:36:33:74:75:6B:99:
        55:42:0F:1B:02:03:01:00:01
      Exponent: 65537
    X509v3 extensions:
      X509v3 Basic Constraints: 7fffffff
  Signature Algorithm: SHA256withRSA
    7F:B1:32:55:29:55:07:A5:43:68:EA:1D:FA:5F:5E:FA:6B:70:
    0B:56:A7:CB:CD:D3:CA:27:D6:4D:F5:35:52:B1:C3:E5:BB:9D:
```

SSM Certificate Installation Steps for FND (Import jboss Certificate Into SSM Web Keystore)

```
#################################################
Default SSM Passwords and alias name:-
ssm_csmp_keystore password : ciscossm
csmp alias name : ssm_csmp
key password : ciscossm
ssm_web_keystore password: ssmweb
#################################################
```

- Download and install the ssm rpm in your FND server:

  ```
  rpm -ivh <cgms-ssm-4.6.0-*.x86_64.rpm>
  ```

- Login to FND GUI:

  ```
  Admin -> certificates -> certificate for web
  ```

  Download the Binary version of "Certificate for Web" from the FND GUI. Save the downloaded file in CGMS under the following path /opt/certForWeb.bin.

- Stop the CGMS and SSM service:

  ```
  service ssm stop
  service cgms stop
  ```

- Copy the ssm port and password in cgms.properties:

  ```
  cd /opt/cgms-ssm/bin/
  ./ssm_setup.sh
  Enter your choice : 5.    [Print CG-NMS configuration for SSM]
  Enter current ssm_csmp_keystore password : <ciscossm>
  Enter alias name : <ssm_csmp>
  Enter key password : <ciscossm>
  ```

  Example:

  ```
  security-module=ssm
  ssm-host=<Replace with IPv4 address of SSM server>
  ssm-port=8445
  ```

```
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

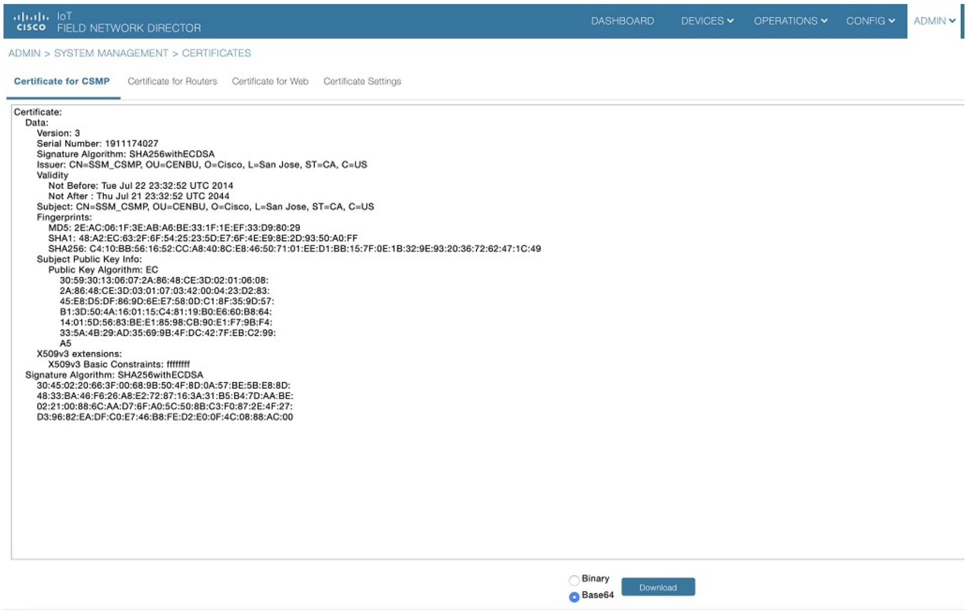
- Update the generated ssm properties in vim /opt/cgms/server/cgms/conf/cgms.properties.
- Add the FND jboss certificate (Certificate for Web) in to ssm_web_keystore.

```
cd /opt/cgms-ssm/bin/
./ssm_setup.sh
Enter your choice : 8
Enter current ssm_web_keystore password : <ssmweb>
Enter the alias for import: fnd
Certificate file name: /opt/certForWeb.bin
Trust this certificate? [no]: yes
Certificate was added to keystore
```

- Start the SSM and CGMS service.

```
service ssm start
service cgms start
```

- Login to FND and choose Admin -> certificates -> Certificate for CSMP. The CSMP certificate will be displayed.



```
Certificate:
   Data:
      Version: 3
      Serial Number: 1911174027
      Signature Algorithm: SHA256withECDSA
      Issuer: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
      Validity
         Not Before: Tue Jul 22 23:32:52 UTC 2014
         Not After : Thu Jul 21 23:32:52 UTC 2044
      Subject: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
      Fingerprints:
         MD5: 2E:AC:06:1F:3E:AB:A6:BE:33:1F:1E:EF:33:D9:80:29
         SHA1: 48:A2:EC:63:2F:6F:54:25:23:5D:E7:6F:4E:E9:8E:2D:93:50:A0:FF
         SHA256: C4:10:BB:56:16:52:CC:A8:40:8C:E8:46:50:71:01:EE:D1:BB:15:7F:0E:1B:32:9E:93:20:36:72:62:47:1C:49
      Subject Public Key Info:
         Public Key Algorithm: EC
            30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:
            2A:86:48:CE:3D:03:01:07:03:42:00:04:23:D2:83:
            45:E8:D5:DF:86:9D:6E:E7:58:0D:C1:8F:35:9D:57:
            B1:3D:50:4A:16:01:15:C4:81:19:B0:E6:60:B8:64:
            14:01:5D:56:83:BE:E1:85:98:CB:90:E1:F7:9B:F4:
            33:5A:4B:29:AD:35:69:9B:4F:DC:42:7F:EB:C2:99:
            A5
      X509v3 extensions:
         X509v3 Basic Constraints: ffffffff
   Signature Algorithm: SHA256withECDSA
      30:45:02:20:66:3F:00:68:9B:50:4F:8D:0A:57:BE:5B:E8:8D:
      48:33:BA:46:F6:26:A8:E2:72:87:16:3A:31:B5:B4:7D:AA:BE:
      02:21:00:88:6C:AA:D7:6F:A0:5C:50:8B:C3:F0:87:2E:4F:27:
      D3:96:82:EA:DF:C0:E7:46:B8:FE:D2:E0:0F:4C:08:88:AC:00
```

SSM debug log: /opt/cgms-ssm/log/ssm.log - SSM logs

Steps to Generate Certificates and Keys for Relay and Target Node

To use FTT wireless console, you need to import CA certificate and IOT-DM certificate into ftt.keystore.

Before you generate certificates and keys for relay and target node, make sure you have the following prerequisites met:

1. Openssl is installed
2. Java JDK is installed for Keytool
3. openssl.cnf

4. fwubl_win732bit_x.x.x.exe
5. cfgwriter-x.x.xx.jar
6. decxu_sec.xml

Follow these steps to generate certificates and keys for relay and target node:

1. On Linux1, generate Root_CA and key with self-signed certificate, using the following commands:

   ```
   mkdir CA
   mkdir CA/{newcerts,certreqs,crl,private}
   touch CA/index.txt
   touch CA/serial
   echo 01 > serial
   cd CA
   ```

   Then copy the openssl.cnf file into the CA directory.

   - Generate root CA ECC private key.

     ```
     openssl ecparam -genkey -name prime256v1 -out root_ca_ec.key
     ```

   - Use root CA private key to generate Self-signed SHA-256 root_ca.crt.

     ```
     openssl req -new -sha256 -x509 -days 1095 -config openssl.cnf -extensions v3_ca -key

     root_ca_ec.key -out root_ca_ec.crt   >>>  DTLS server Root_certificate
     Domain Component []:cisco
     Domain Component []:com
     Common Name (e.g. server FQDN or YOUR name) []:root_ca_cert
     ```

   - Convert root_ca cert from PEM to DER.

     ```
     openssl x509 -in root_ca_ec.crt -outform der -out root_ca_ec.der >>> Target Node
     Root_certificate
     ```

2. On Linux2, the IoT-DM DTLS server,

   - Generate DTLS server ECC private key.

     ```
     openssl ecparam -genkey -name prime256v1 -out server_ec.key
     ```

   - Generate CSR from DTLS server.

     ```
     openssl req -new -sha256 -key server_ec.key -out server.csr -extensions v3_req -config
      openssl.cnf
     Domain Component []:cisco
     Domain Component []:com
     Common Name (e.g. server FQDN or YOUR name) []:server_cert
     ```

     Copy the above **server_ec.key** and **server.csr** files to Linux1 CA directory, then execute the following commands from Linux1:

   - Use the Root_CA cert, Root_CA key, and Server CSR to give the signed certificate of root_CA[server.crt].

     ```
     openssl ca -days 365 -cert root_ca_ec.crt -keyfile root_ca_ec.key -md sha256
     -extensions v3_req
     -config openssl.cnf -in server.csr -out server_ec.crt    >>>      DTLS server
     certificate
     ```

   - Convert the DTLS server ECC key to PKCS8 standard.

```
openssl pkcs8 -topk8 -nocrypt -in server_ec.key -outform PEM -out server_pk8.key >>>
 DTLS server Private key
```

3. On Linux3, the target node IR510,

   - Generate ECC private key for the target node.

     ```
     openssl ecparam -genkey -name prime256v1 -out client_ec.key
     ```

   - Generate CSR from the target node.

     ```
     openssl req -new -sha256 -key client_ec.key -out client.csr -extensions v3_req -config
      openssl.cnf
     Domain Component []:cisco
     Domain Component []:com
     Common Name (e.g. server FQDN or YOUR name) []:client_cert
     ```

     Copy the above **client_ec.key** and **client.csr** files to Linux1 CA directory, then execute the following commands from Linux1:

   - Use the Root_CA cert, Root_CA key and Server CSR to give the signed certificate of root_CA[client.crt].

     ```
     openssl ca -days 365 -cert root_ca_ec.crt -keyfile root_ca_ec.key -md sha256
     -extensions v3_req
     -config openssl.cnf -in client.csr -out client_ec.crt
     ```

   - Convert the target node ECC key to PKCS8 standard.

     ```
     openssl pkcs8 -topk8 -nocrypt -in client_ec.key -outform PEM -out client_pk8.key
     ```

   - Convert the PKCS8 PEM to DER.

     ```
     openssl pkcs8 -topk8 -nocrypt -in client_pk8.key -outform DER
     -out client_pk8.der    >>>  Target Node Private key
     ```

   - Convert client cert from PEM to DER.

     ```
     openssl x509 -in client_ec.crt -outform der -out client_ec.der    >>>   Target Node
      certificate
     ```

4. Download CSMP certificate from FND

   - Login to FND and navigate to Admin -> certificates -> certificate for CSMP. Download the Base64 version of "Certificate for CSMP" from the FND GUI.

   - Convert CSMP cert from PEM to DER.

     ```
     openssl x509 -inform PEM -in certForCsmp.pem -outform DER -out cert_ssm.der  >>>
       Target Node CSMP certificate
     ```

Generate ftt.keystore for IoT-DM

Before you generate ftt.keystore for IoT-DM, copy the following 3 files in a directory:

- root_ca_ec.crt
- server_ec.crt
- server_pk8.key

In that directory where you copied the above files, follow these steps to generate ftt.keystore for IoT-DM:

1. Import server private key into server.crt and generate ftt.keystore:

   ```
   openssl pkcs12 -export -in server_ec.crt -inkey server_pk8.key -out ftt.keystore
   -name server.key
   ```

2. Import server_ec.crt in to ftt.keystore:

   ```
   keytool -import -alias server_cert -keystore ftt.keystore -file server_ec.crt
   ```

3. Import root_ca.crt in to ftt.keystore:

   ```
   keytool -import -alias ca_cert -keystore ftt.keystore -file root_ca_ec.crt
   >>>     ftt.keystore for IOT-DM
   ```

Configuring Target Node with Generated Certificates and Keys

1. Create a folder and keep the following 7 files in Target node windows machine.
   a. root_ca_ec.der
   b. client_pk8.der
   c. client_ec.der
   d. cert_ssm.der
   e. fwubl_win732bit_x.x.x.exe
   f. cfgwriter-x.x.xx.jar
   g. decxu_sec.xml

2. Open cmd prompt and go to the folder where all 7 files were copied:
   - Execute the below command to generate bin file for target IR510

     ```
     java -jar cfgwriter-6.1.24.jar -v --ca root_ca_ec.der -c client_ec.der -k
     client_pk8.der -nc cert_ssm.der -w decxu_sec.xml target_node.bin
     ```

   - Connect to IR510 with below command:

     ```
     fwubl_win732bit_1.0.5.exe com1
     ```

   - Hard reboot the IR510.
   - Push the generated bin into IR510 with following command:

     ```
     fwubl_win732bit_1.0.5.exe -w target_node.bin -a 0x80e0000 com1
     ```

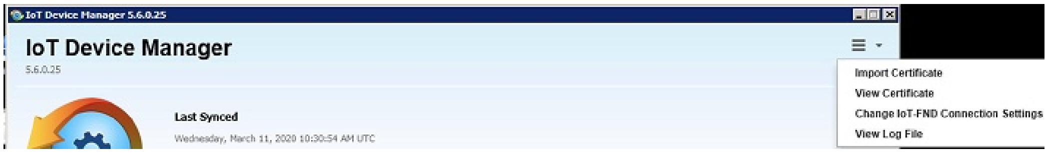
   - Hard reboot the IR510 again.

To verify the applied configuration:

- TLV - 35 WPANStatus
- TLV - 33 Ieee802.1xStatus

Secured Wireless Connection to Target Node

To import the keystore containing these certificates, on the Device Manager opening page, select **Import Certificate** from the drop-down menu on the upper right.



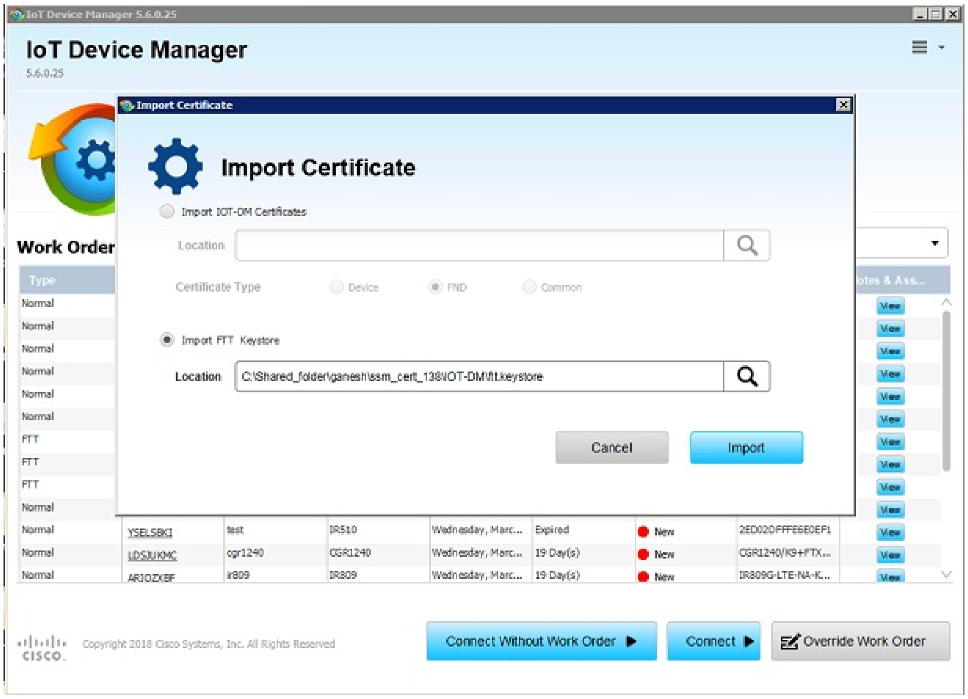
[redacted]

Last Synced

Wednesday, March 11, 2020 10:30:54 AM UTC

In the Import Certificate dialog box, browse to the location of the certificate file on your laptop.

Select Import FTT keystore radio button. Then choose the ftt.keystore file and click on Import.



○ Import IOT-DM Certificates

Location

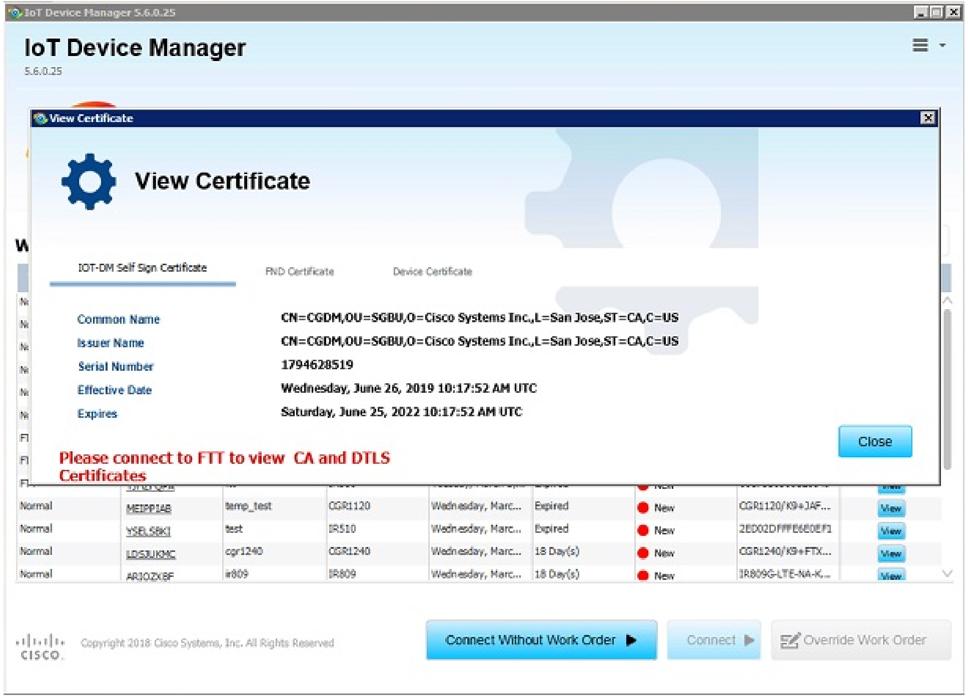
Certificate Type ○ Device ● FND ○ Common

● Import FTT Keystore

Location C:\Shared_folder\ganesh\ssm_cert_138\IOT-DM\ftt.keystore

Type								otes & Ass...
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
FTT								View
FTT								View
FTT								View
Normal								View
Normal	YSELSBKI	test	IR510	Wednesday, Marc...	Expired	● New	2ED02DFFFE6E0EF1	View
Normal	LDSJUKMC	cgr1240	CGR1240	Wednesday, Marc...	19 Day(s)	● New	CGR1240/K9+FTX...	View
Normal	ARIOZXBF	ir809	IR809	Wednesday, Marc...	19 Day(s)	● New	IR809G-LTE-NA-K...	View

Note After importing ftt.keystore, you need to connect to FTT to view the certificates; otherwise you will see the warning message to connect to FTT in the View Certificate page as shown below.


IoT Device Manager 5.6.0.25
IoT Device Manager
5.6.0.25
View Certificate
IOT-DM Self Sign Certificate
FND Certificate
Device Certificate
Close
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

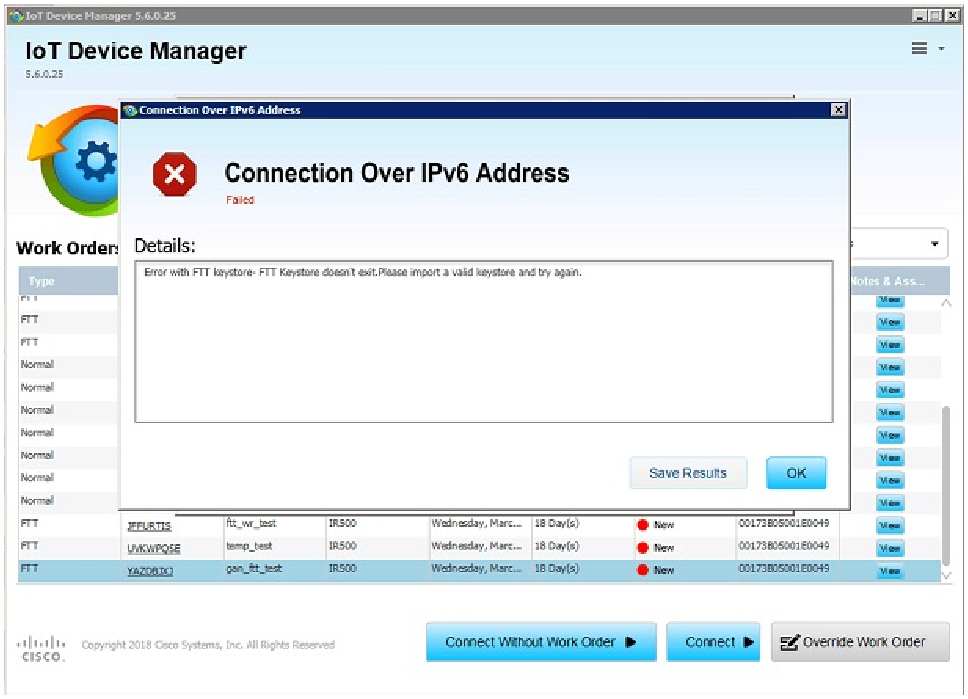
View Certificate

Common Name	CN=CGDM,OU=SGBU,O=Cisco Systems Inc.,L=San Jose,ST=CA,C=US
Issuer Name	CN=CGDM,OU=SGBU,O=Cisco Systems Inc.,L=San Jose,ST=CA,C=US
Serial Number	1794628519
Effective Date	Wednesday, June 26, 2019 10:17:52 AM UTC
Expires	Saturday, June 25, 2022 10:17:52 AM UTC

Please connect to FTT to view CA and DTLS Certificates

Normal	MEIPP1AB	temp_test	CGR1120	Wednesday, Marc...	Expired	● New	CGR1120/K9+JAF...	View
Normal	YSELS8KI	test	IR510	Wednesday, Marc...	Expired	● New	2ED02DFFFE6E0EF1	View
Normal	LDSJUKMC	cgr1240	CGR1240	Wednesday, Marc...	18 Day(s)	● New	CGR1240/K9+FTX...	View
Normal	ARJOZXBF	ir809	IR809	Wednesday, Marc...	18 Day(s)	● New	IR809G-LTE-NA-K...	View

- If ftt.keystore is not imported while connecting to FTT, you will get an error as shown below.


IoT Device Manager 5.6.0.25
IoT Device Manager
5.6.0.25
Work Orders
Type
Notes & Ass...
Connection Over IPv6 Address
Save Results
OK
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Connection Over IPv6 Address

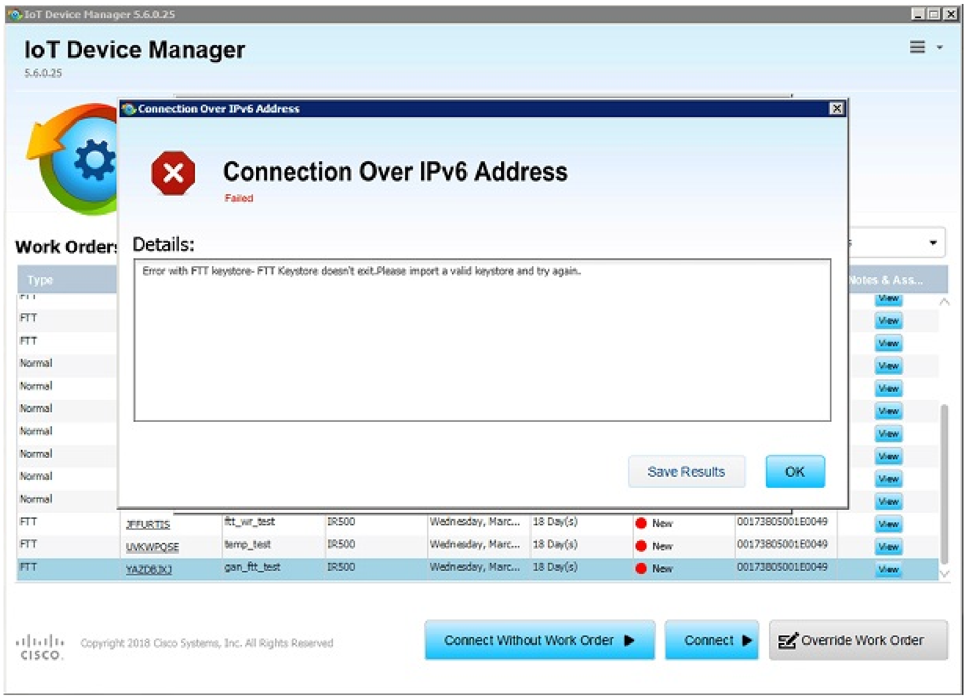
Failed

Details:

Error with FTT keystore- FTT Keystore doesn't exit.Please import a valid keystore and try again.

FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	UVKWPQSE	temp_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173B05001E0049	View

- If a wrong password is provided while connecting to FTT, you will get an error as shown below.



IoT Device Manager 5.6.0.25
IoT Device Manager
5.6.0.25
Work Orders
Type
Notes & Ass...
View
Save Results
OK
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Connection Over IPv6 Address

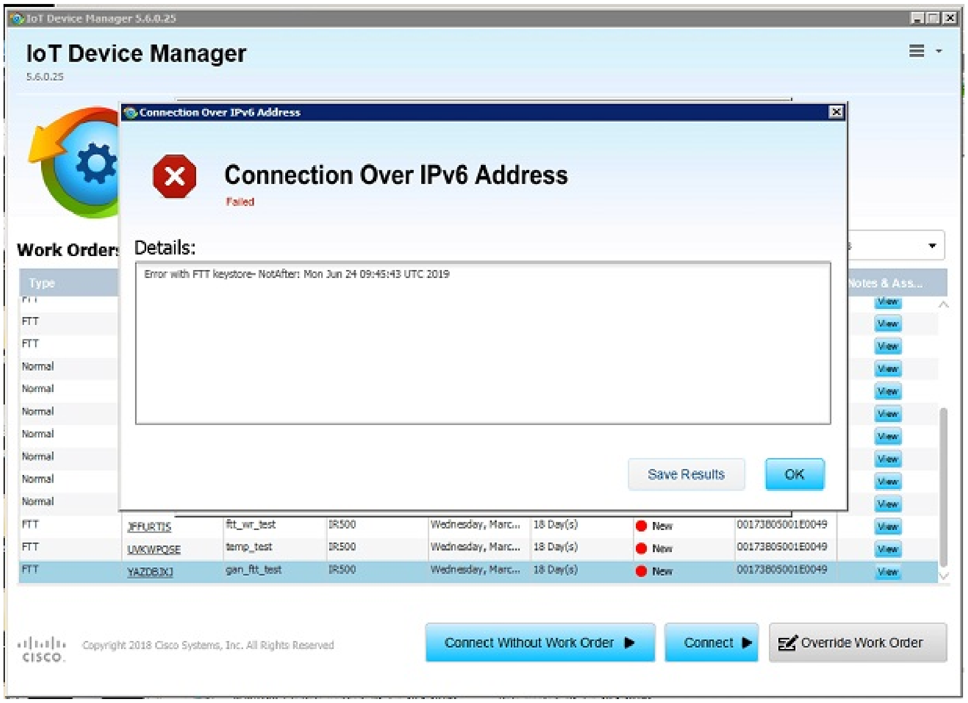
Connection Over IPv6 Address
Failed

Details:

Error with FTT keystore- FTT Keystore doesn't exit.Please import a valid keystore and try again.

```
FTT
FTT
Normal
Normal
Normal
Normal
Normal
Normal
Normal
FTT  JFFURTIS  ftt_wr_test  IR500  Wednesday, Marc...  18 Day(s)  ● New  00173B05001E0049  View
FTT  UVKWPQSE  temp_test    IR500  Wednesday, Marc...  18 Day(s)  ● New  00173B05001E0049  View
FTT  YAZDBJXJ  gan_ftt_test IR500  Wednesday, Marc...  18 Day(s)  ● New  00173B05001E0049  View
```

- If the certificate is expired while connecting to FTT, you will get an error as shown below.



IoT Device Manager 5.6.0.25
IoT Device Manager
5.6.0.25
Work Orders
Type
Notes & Ass...
View
Save Results
OK
Connect Without Work Order ▶
Connect ▶
Override Work Order
Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Connection Over IPv6 Address

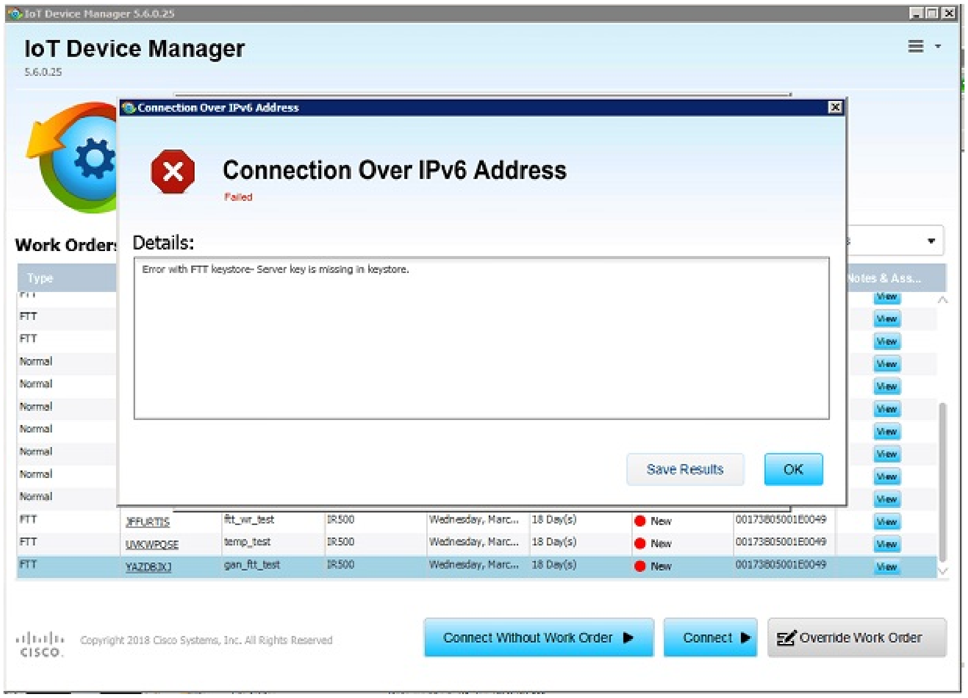
Connection Over IPv6 Address
Failed

Details:

Error with FTT keystore- NotAfter: Mon Jun 24 09:45:43 UTC 2019

```
FTT
FTT
Normal
Normal
Normal
Normal
Normal
Normal
Normal
FTT  JFFURTIS  ftt_wr_test  IR500  Wednesday, Marc...  18 Day(s)  ● New  00173B05001E0049  View
FTT  UVKWPQSE  temp_test    IR500  Wednesday, Marc...  18 Day(s)  ● New  00173B05001E0049  View
FTT  YAZDBJXJ  gan_ftt_test IR500  Wednesday, Marc...  18 Day(s)  ● New  00173B05001E0049  View
```

- If the server key alias is missing while connecting to FTT, you will get an error as shown below.



IoT Device Manager 5.6.0.25

IoT Device Manager

5.6.0.25

Connection Over IPv6 Address

Connection Over IPv6 Address

Failed

Details:

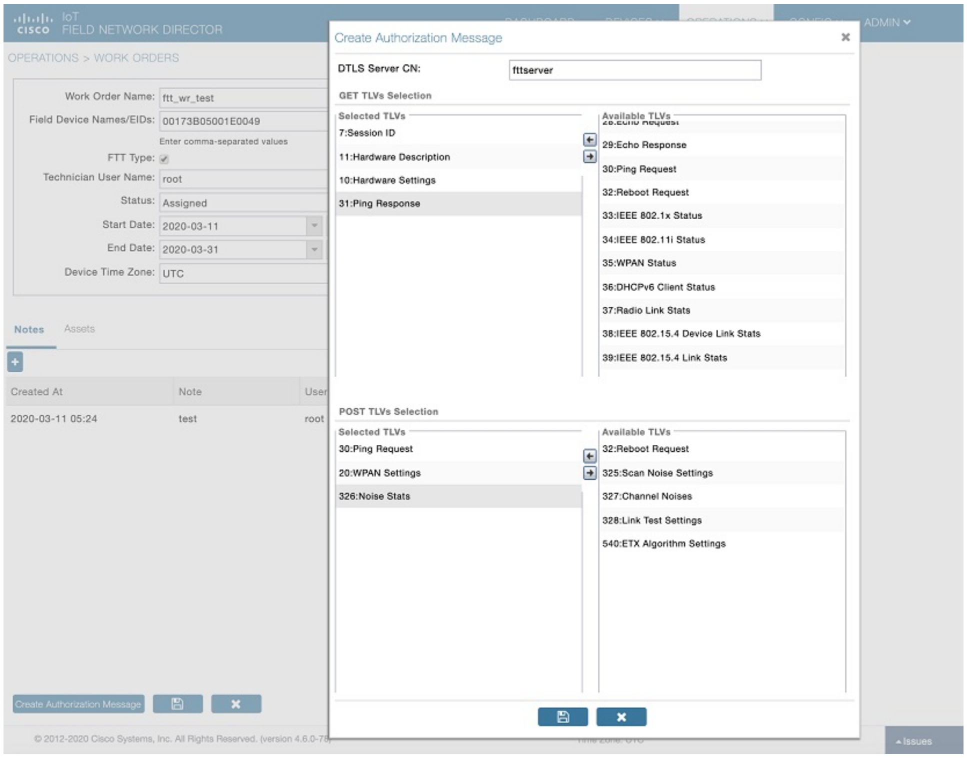
Error with FTT keystore- Server key is missing in keystore.

Work Orders

Type								Notes & Ass...
FTT								View
FTT								View
FTT								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
Normal								View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173805001E0049	View
FTT	UWKWPQSE	temp_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173805001E0049	View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	18 Day(s)	● New	00173805001E0049	View

Copyright 2018 Cisco Systems, Inc. All Rights Reserved

Create a work order from FND. Enter DTLS server Common Name, give permissions to GET and POST TLVs.



Work Order Name: ftt_wr_test

Field Device Names/EIDs: 00173B05001E0049

Enter comma-separated values

FTT Type: ☑

Technician User Name: root

Status: Assigned

Start Date: 2020-03-11

End Date: 2020-03-31

Device Time Zone: UTC

Created At	Note	User
2020-03-11 05:24	test	root

Create Authorization Message

DTLS Server CN: fttserver

GET TLVs Selection

Selected TLVs:
- 7:Session ID
- 11:Hardware Description
- 10:Hardware Settings
- 31:Ping Response

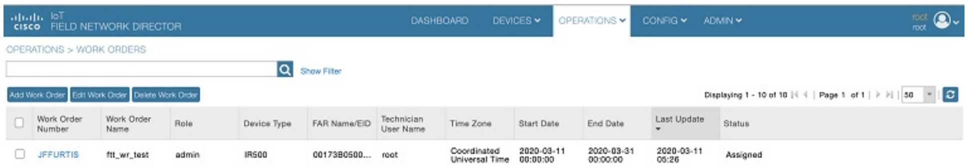
Available TLVs:
- 28:Echo Request
- 29:Echo Response
- 30:Ping Request
- 32:Reboot Request
- 33:IEEE 802.1x Status
- 34:IEEE 802.11i Status
- 35:WPAN Status
- 36:DHCPv6 Client Status
- 37:Radio Link Stats
- 38:IEEE 802.15.4 Device Link Stats
- 39:IEEE 802.15.4 Link Stats

POST TLVs Selection

Selected TLVs:
- 30:Ping Request
- 20:WPAN Settings
- 326:Noise Stats

Available TLVs:
- 32:Reboot Request
- 325:Scan Noise Settings
- 327:Channel Noises
- 328:Link Test Settings
- 540:ETX Algorithm Settings

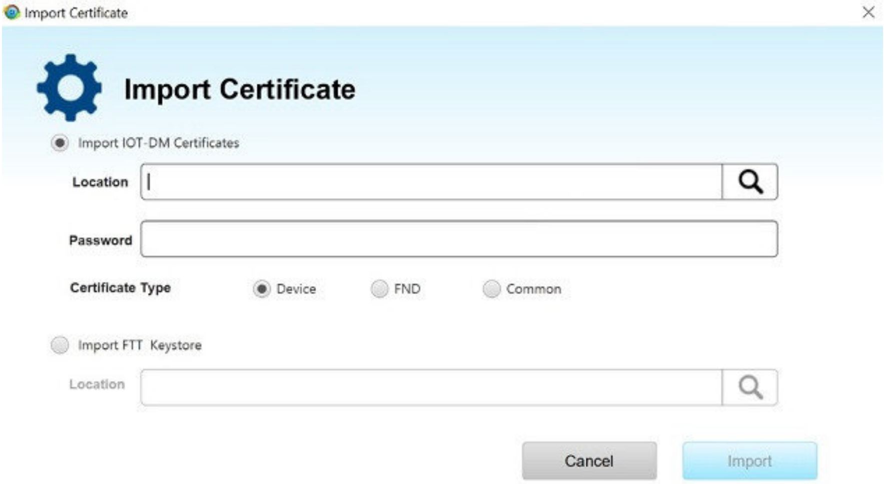
© 2012-2020 Cisco Systems, Inc. All Rights Reserved. (version 4.6.0-78)



	Work Order Number	Work Order Name	Role	Device Type	FAR Name/EID	Technician User Name	Time Zone	Start Date	End Date	Last Update	Status
□	JFFURTIS	ftt_wr_test	admin	IR500	00173B0500...	root	Coordinated Universal Time	2020-03-11 00:00:00	2020-03-31 00:00:00	2020-03-11 05:26	Assigned

Use one of the following ways to sync the created WR from FND to IOT-DM:

1. Import the FND custom web certificate in to IOT-DM: IOT-DM Application → Settings → Import Certificate → Select Import IOT-DM certificates → Select FND radio button → choose the *.pfx file → enter password and click on Import.



● Import IOT-DM Certificates

Location: |

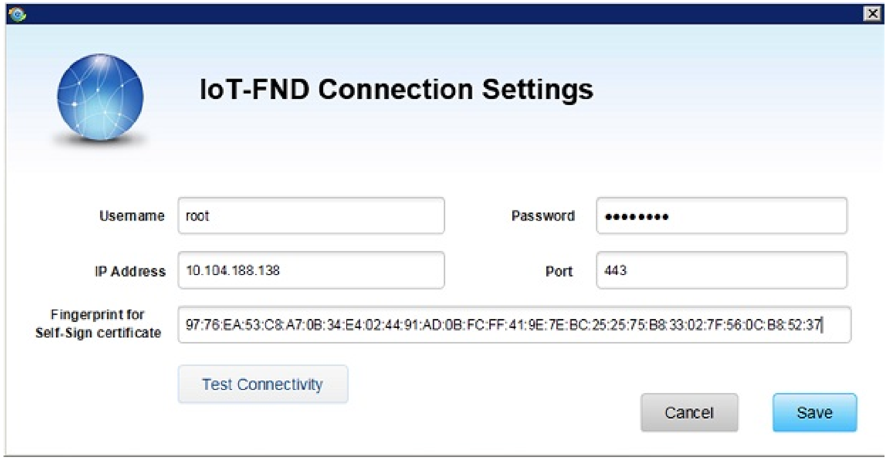
Password:

Certificate Type: ● Device ○ FND ○ Common

○ Import FTT Keystore

Location:

2. Enter the fingerprint of web certificate in IOT-FND Connection Settings.



Username: root

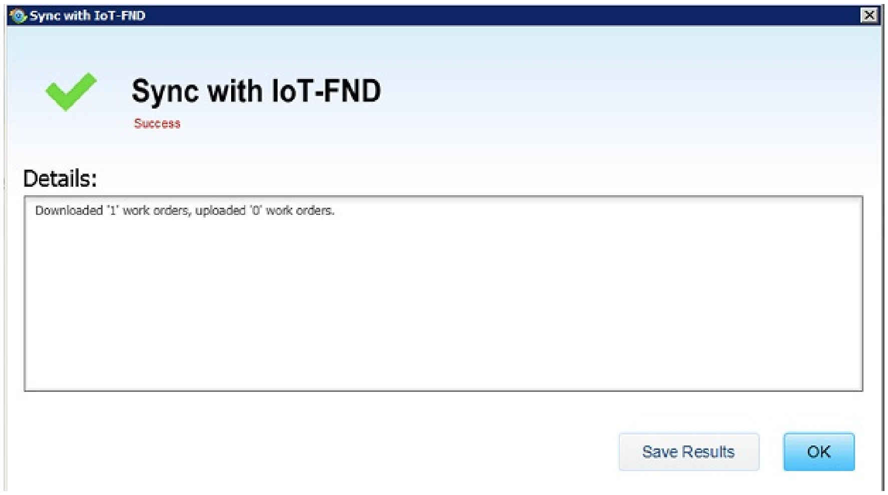
Password: ••••••••

IP Address: 10.104.188.138

Port: 443

Fingerprint for Self-Sign certificate: 97:76:EA:53:C8:A7:0B:34:E4:02:44:91:AD:0B:FC:FF:41:9E:7E:BC:25:25:75:B8:33:02:7F:56:0C:B8:52:37

Click on Sync with IOT-FND.



Sync with IoT-FND

Sync with IoT-FND

Success

Details:

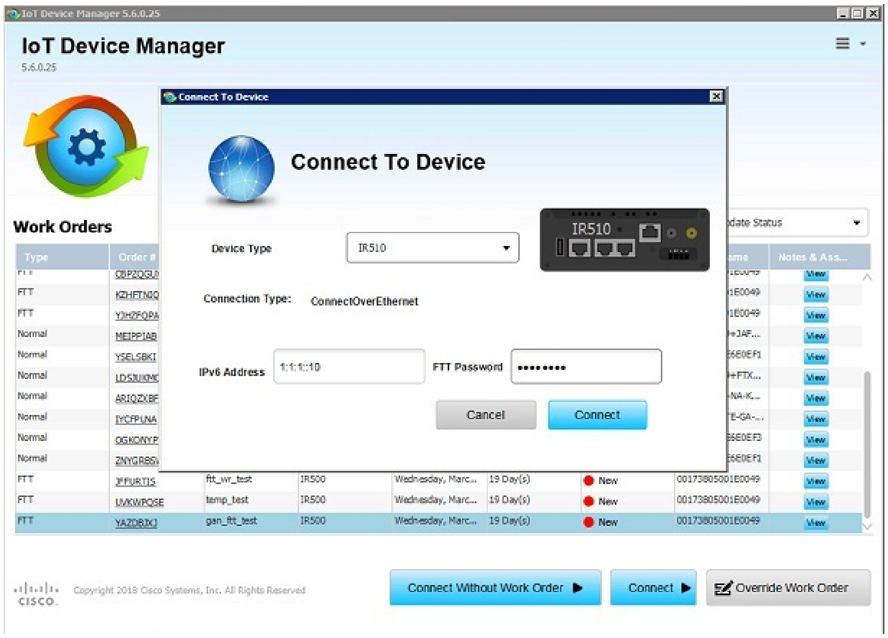
Downloaded '1' work orders, uploaded '0' work orders.

Viewing the Imported FTT keystore in IOT-DM

Select the downloaded FTT type work order and click the Connect button. Select IR510 as device type, enter Relay node IPv6 address, and provide FTT password, then click on connect. Once the dashboard page is launched, disconnect from device.

Note The feature will only be enabled when you connect to the device with work order which has TLV 342 message. If the work order is non FTT type, the IR510 device connected com port. If the work order type is FTT, the Connect button redirects to another screen and you need to provide IPV6 address of the relay node and FTT password. Connect to IR510 via IPV6. Once the connection to IR510 is established through IPV6 Address, the DTLS server 1.2 will be started. IoT-DM uses port number 5556 for DTLS server.

- Connectivity to Relay Node With Work Order



IoT Device Manager 5.6.0.25

IoT Device Manager

5.6.0.25

Connect To Device

Connect To Device

Device Type: IR510

Connection Type: ConnectOverEthernet

IPv6 Address: 1:1:1::10

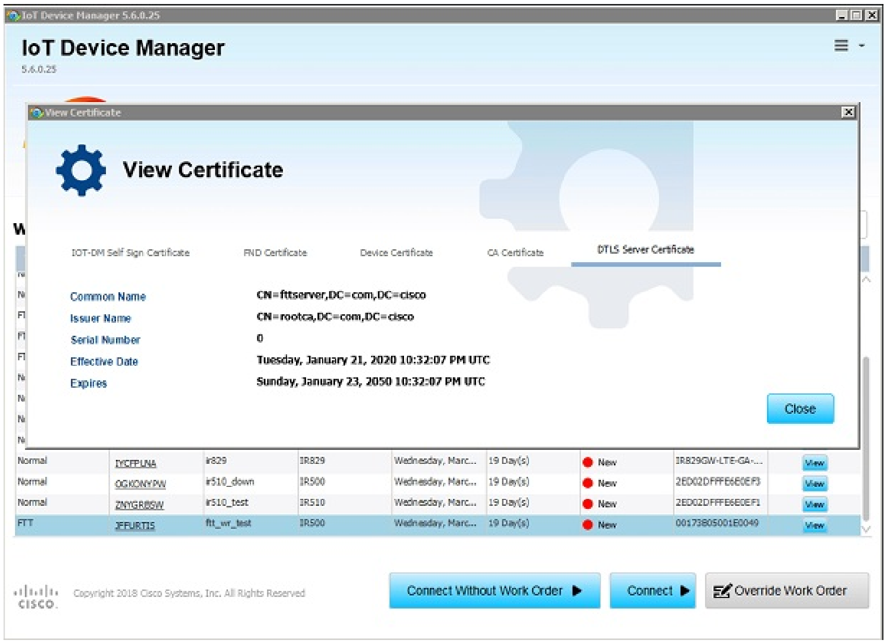
FTT Password: ••••••••

Work Orders

Type	Order #						...ame	Notes & Ass...
FTT	CBPZQGU						1E0049	View
FTT	KZHFTNIQ						1E0049	View
FTT	YJHZFQPA						1E0049	View
Normal	MEIPPIAB						+JAF...	View
Normal	YSELSBKI						E6E0EF1	View
Normal	LDSJUKMC						+FTX...	View
Normal	ARIQZXBF						-NA-K...	View
Normal	IYCFPLNA						E-GA-...	View
Normal	OGKONYP						E6E0EF3	View
Normal	ZNYGRBSV						E6E0EF1	View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173805001E0049	View
FTT	UVKWPQSE	temp_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173805001E0049	View
FTT	YAZDBJXJ	gan_ftt_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173805001E0049	View

Copyright 2018 Cisco Systems, Inc. All Rights Reserved

- Once the ftt.keystore is imported, they can be viewed in the View Certificate tab as shown below,



IoT Device Manager 5.6.0.25

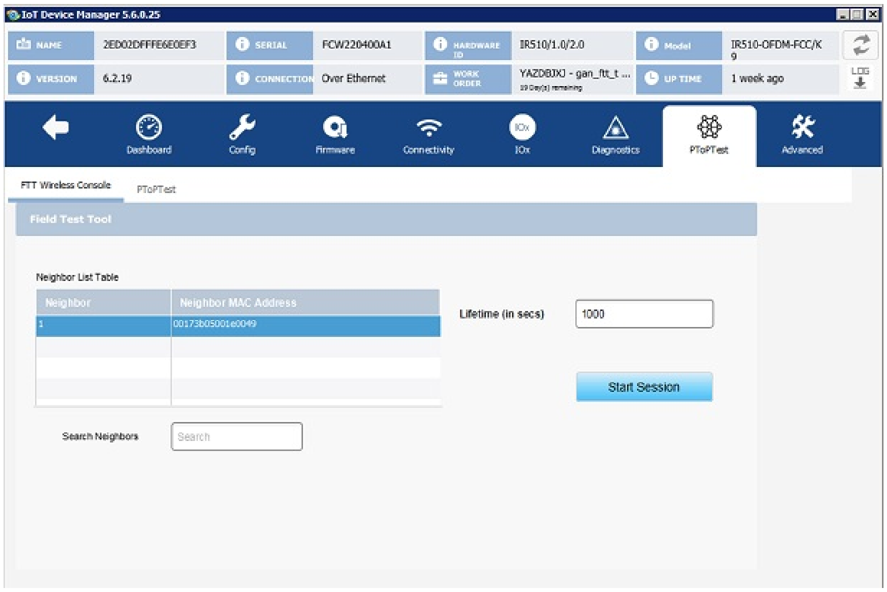
View Certificate

Common Name	CN=fttserver,DC=com,DC=cisco
Issuer Name	CN=rootca,DC=com,DC=cisco
Serial Number	0
Effective Date	Tuesday, January 21, 2020 10:32:07 PM UTC
Expires	Sunday, January 23, 2050 10:32:07 PM UTC

Normal	IYCFPUNA	ir829	IR829	Wednesday, Marc...	19 Day(s)	● New	IR829GW-LTE-GA-...	View
Normal	OGKONYPW	ir510_down	IR500	Wednesday, Marc...	19 Day(s)	● New	2ED02DFFFE6E0EF3	View
Normal	ZNYGR8SW	ir510_test	IR510	Wednesday, Marc...	19 Day(s)	● New	2ED02DFFFE6E0EF1	View
FTT	JFFURTIS	ftt_wr_test	IR500	Wednesday, Marc...	19 Day(s)	● New	00173B05001E0049	View

Copyright 2018 Cisco Systems, Inc. All Rights Reserved

- Login again with the same work order and navigate to PToPTest tab. You need to choose neighbour target node from "Neighbour List table" (populated based on TLV 52), enter the lifetime (in seconds) and click on Start Session. It will post TLV 341 and connect to the respective target node and establish DTLS channel. IoT-DM will send authorization message to the connected target node. If the target node address is not matching with the target node EUI ID mentioned in the authorization message, target node will reject the request. Otherwise, it will establish the connection.



IoT Device Manager 5.6.0.25

NAME	2ED02DFFFE6E0EF3	SERIAL	FCW220400A1	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.2.19	CONNECTION	Over Ethernet	WORK ORDER	YAZDBJXJ - gan_ftt_t ... 19 Day(s) remaining	UP TIME	1 week ago

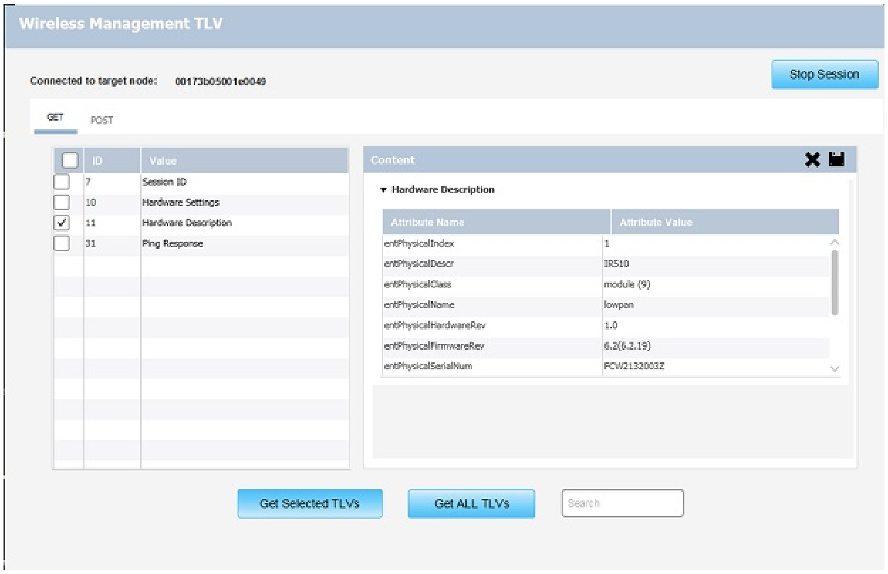
Neighbor List Table

Neighbor	Neighbor MAC Address
1	00173b05001e0049

Lifetime (in secs): 1000

Wireless Console Screen

- GET Authorized TLV Tab



Wireless Management TLV

Connected to target node: 00173b05001e0049

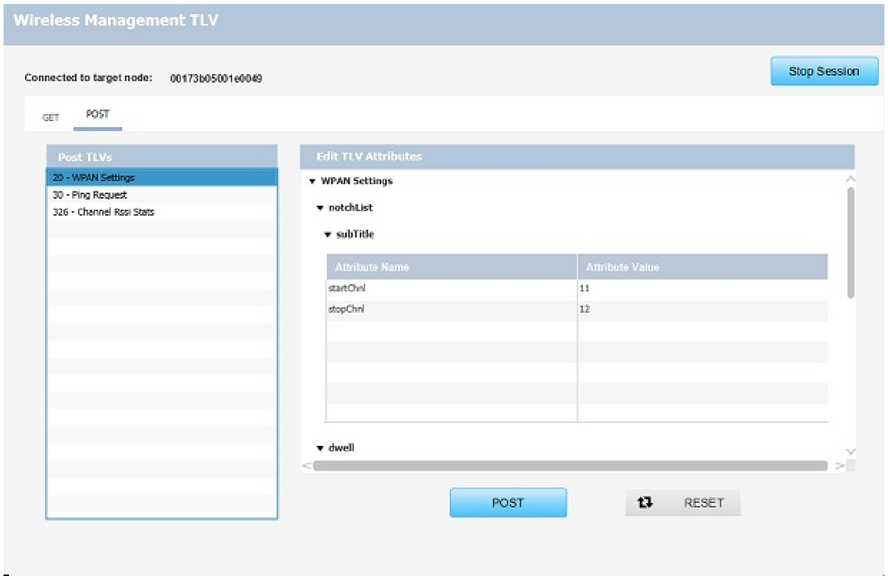
□	ID	Value
□	7	Session ID
□	10	Hardware Settings
☑	11	Hardware Description
□	31	Ping Response

Content

▾ Hardware Description

Attribute Name	Attribute Value
entPhysicalIndex	1
entPhysicalDescr	IR510
entPhysicalClass	module (9)
entPhysicalName	lowpan
entPhysicalHardwareRev	1.0
entPhysicalFirmwareRev	6.2(6.2.19)
entPhysicalSerialNum	FCW2132003Z

- POST Authorized TLV Tab



Wireless Management TLV

Connected to target node: 00173b05001e0049

Post TLVs

20 - WPAN Settings
30 - Ping Request
326 - Channel Rssi Stats

Edit TLV Attributes

▾ WPAN Settings

▾ notchList

▾ subTitle

Attribute Name	Attribute Value
startChnl	11
stopChnl	12

▾ dwell

- To terminate the session, click the Stop Session button.

Note As part of this feature, management command support via FTT wireless console is removed, hence the "wireless management console screen" supported by starting the wireless console session will be removed from IOT-DM Release 5.6 and later.

Running Point to Point Test Between Two IR510s

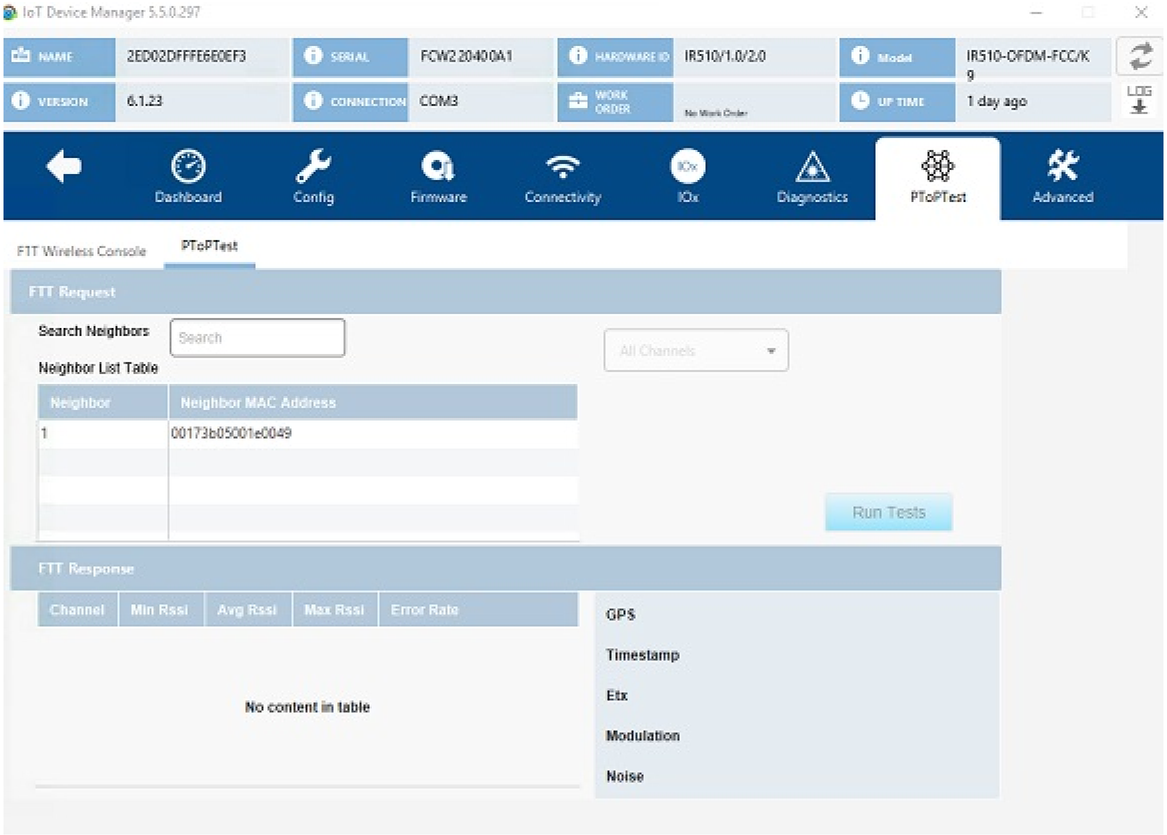
Use the **PToPTest** page to run point to point test between two IR510s.

Step 1 Connect to IR 510 via IOT-DM.

Step 2 Click the **PToPTest** tab, select a neighbour, choose a channel option, and click the **Run Tests** button. If you do not choose a channel option, the test will be running with the default of "All Channels."

Use the Select channel drop-down menu to select one of the following channel options.

- All Channels: the default selection
- Single Channel: choose from 0 to 32
- Channel Range: choose the start channel and the end channel
- Multi Channels: enter channel numbers seperated by commas (for example, "1,5,23,") in the text box



IoT Device Manager 5.5.0.297

NAME	2ED02DFFFE6E0EF3	SERIAL	FCW2 20400A1	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.1.23	CONNECTION	COM3	WORK ORDER	No Work Order	UP TIME	1 day ago

FTT Request

Search Neighbors: Search

All Channels

Neighbor List Table

Neighbor	Neighbor MAC Address
1	00173b05001e0049

FTT Response

Channel	Min Rssi	Avg Rssi	Max Rssi	Error Rate

No content in table

GPS

Timestamp

Etx

Modulation

Noise

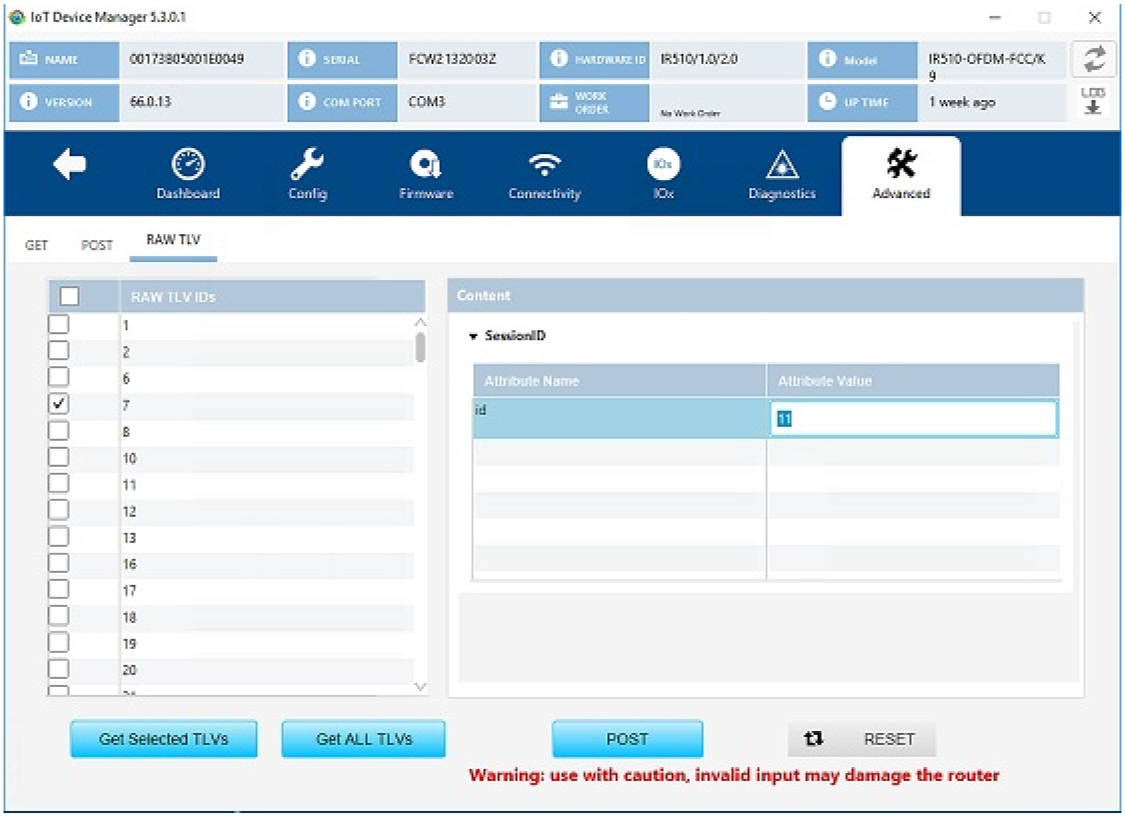
Step 3 (Optional) If you want to search a specific neighbor, enter the physical address in the **Search Neighbours** text box.

The function of searching a specific neighbor is only supported on firmware version CG-Mesh 6.0 and later.

Step 4 After the test is completed, the results are dispalyed for RSSI, Error Rate, ETX, Noise, Modulation, GPS, and Timestamp.

Raw TLV Support on IR510

The RAW TLV tab was introduced for IR510 on the Advanced tab. When you click the **RAW TLV** tab, all TLVs (including newly added TLVs) will be displayed as a list. Select TLVs from the list and click the **Get Selected TLVs** button will display the information about the selected TLVs. Click the **Get ALL TLVs** button will display information of all TLVs in the list. To change the TLV attribute values, click the **POST** button.



NAME	00173805001E0049	SERIAL	FCW2132003Z	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.6.0.13	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	1 week ago

☐	RAW TLV IDs
☐	1
☐	2
☐	6
☑	7
☐	8
☐	10
☐	11
☐	12
☐	13
☐	16
☐	17
☐	18
☐	19
☐	20

Content

▾ SessionID

Attribute Name	Attribute Value
id	11

Warning: use with caution, invalid input may damage the router

Note If you change the field value and click the POST button, the data will be posted to the IR510 device WITHOUT ANY VALIDATION.

Note On the **RAW TLV** tab, every fields of a TLV will be displayed. If some fields are not postable, the post operation will fail.

Disconnecting from the IR500

After finishing your work on the IR500, click the left arrow on the left side of the menu tabs area on the main page to disconnect Device Manager from the IR500. Click **Yes** to confirm that you want to disconnect from the device. Device Manager disconnects and displays the Device Manager opening page.

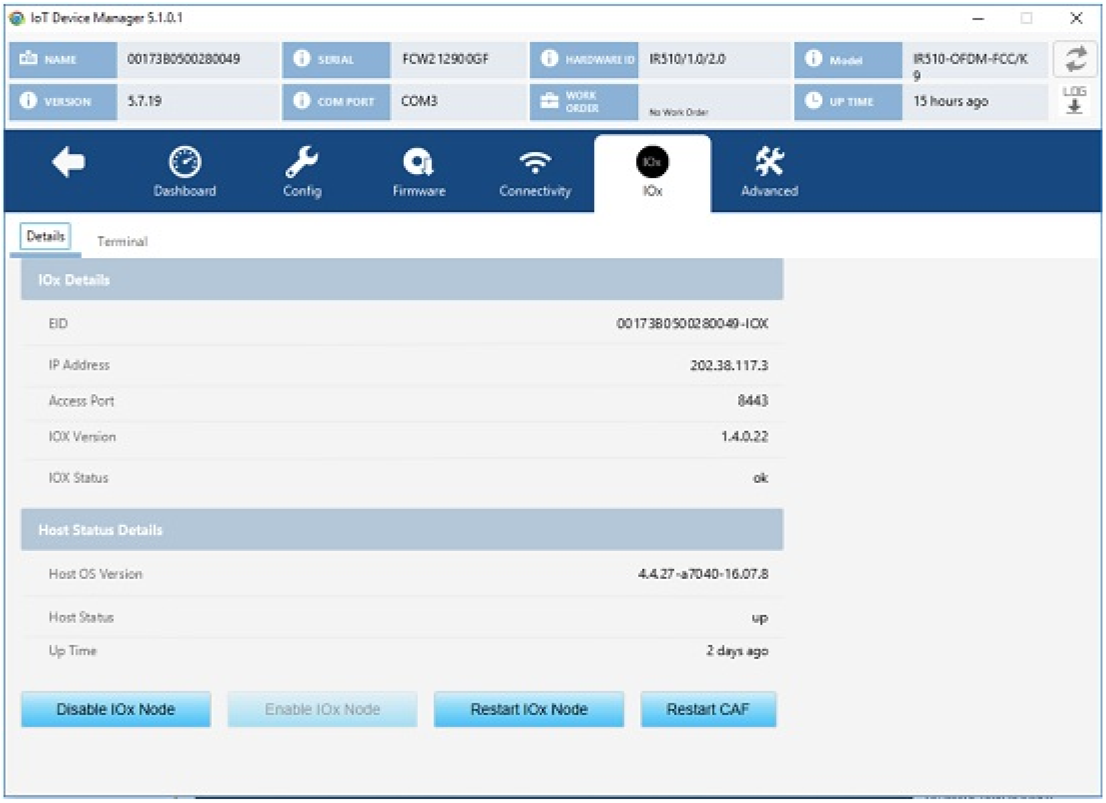
Managing IOx Nodes on IR510

From IoT Device Manager Release 5.2, you can perform management operations on the Linux/IOx nodes on the IR510 device. You can also view the current information of the IOx nodes.

Note The IOx node on IR510 should already have been setup via FND or manually, so that you can perform the management operations on it from IOT-DM.

The following image shows the IOx tab which contains 4 management operation buttons and and a text area showing the details of IOx node in the device.

Figure 5: IOx Tab



IoT Device Manager 5.1.0.1

NAME	00173B0500280049	SERIAL	FCW212900GF	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	5.7.19	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	15 hours ago

IOx Details

EID	00173B0500280049-IOX
IP Address	202.38.117.3
Access Port	8443
IOX Version	1.4.0.22
IOX Status	ok

Host Status Details

Host OS Version	4.4.27-a7040-16.07.8
Host Status	up
Up Time	2 days ago

You can perform the following actions

- Enable IOx Node - This operation only takes effect if the IOx Node was in disabled state.

- Disable IOx Node - This operation only takes effect if the IOx Node was in enabled state.
- Restart IOx - This operation only takes effect if the IOx Node was in enabled state.
- Restart CAF - This operation only takes effect if the IOx Node was in enabled state.

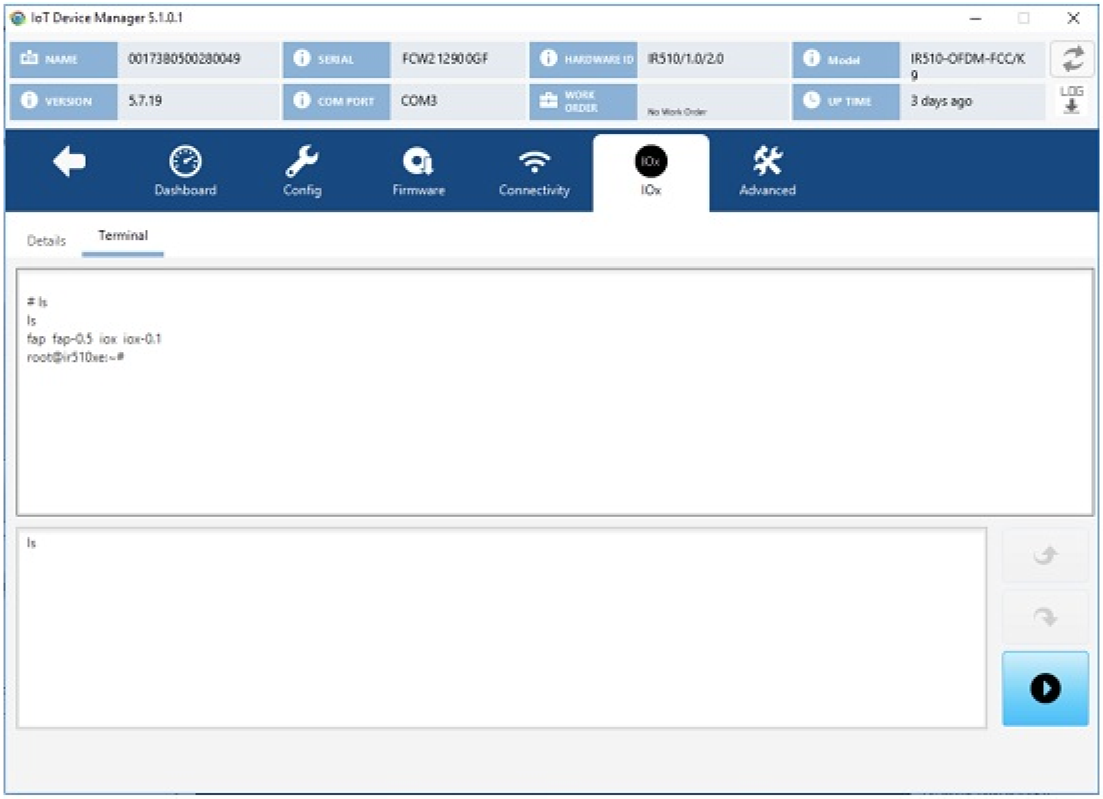
Using the IOx Terminal

You can connect to the Linux/IOx nodes on the IR510 device and execute commands or troubleshoot issues locally by using the IOx terminal on the IOx tab.

Note Linux node on the IR500 device should have UDP server running on 8335 port which will be used to connect via IOT-DM Client over PPP.

To access the IOx Terminal, click the IOx tab and choose Terminal as the following figure shows. An interactive command prompt will display where you can execute the commands on Linux/IOx terminal.

Figure 6: IOx Terminal



IoT Device Manager 5.1.0.1

NAME	00173805002800049	SERIAL	FCW2 1290 0GF	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K 9
VERSION	5.7.19	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	3 days ago

```
# ls
ls
fap  fap-0.5  iox  iox-0.1
root@ir510xe:~#
```

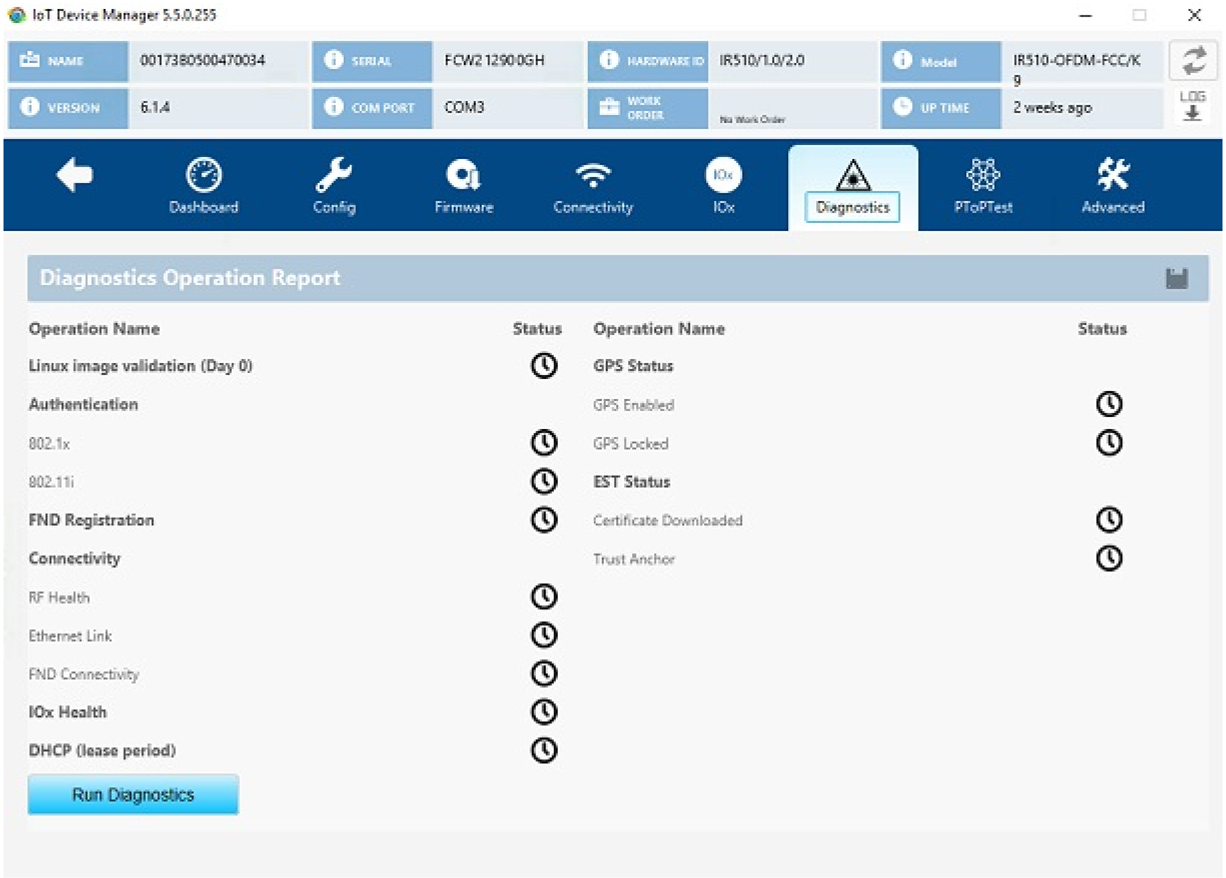
```
ls
```

Diagnostic Operations on IR510

From IoT Device Manager Release 5.3, you can run diagnostic operations on IR510. Once completed, a simple report will be disaplayed to indicate overall health status of the device which includes any issues with the device, suggestions to correct those issues, and possible troubleshooting steps.

The following figure shows the Diagnostics tab.

Figure 7: Diagnostics Tab



IoT Device Manager 5.5.0.255

NAME	0017380500470034	SERIAL	FCW2 12900GH	HARDWARE ID	IR510/1.0/2.0	Model	IR510-OFDM-FCC/K9
VERSION	6.1.4	COM PORT	COM3	WORK ORDER	No Work Order	UP TIME	2 weeks ago

Diagnostics Operation Report

Operation Name	Status	Operation Name	Status
Linux image validation (Day 0)	🕓	GPS Status	
Authentication		GPS Enabled	🕓
802.1x	🕓	GPS Locked	🕓
802.11i	🕓	EST Status	
FND Registration	🕓	Certificate Downloaded	🕓
Connectivity		Trust Anchor	🕓
RF Health	🕓		
Ethernet Link	🕓		
FND Connectivity	🕓		
IOx Health	🕓		
DHCP (lease period)	🕓		

To run diagnostics, click the **Diagnostics** tab. Then click the **Run Diagnostics** button, a message dialog box showing "*Diagnostic operation is under progress, please wait.*" will be displayed. Other operations will not be allowed until the diagnostic operation is completed.

After all diagnostics are completed, successful operations will be shown as green and failed ones will be shown as red. Failed operation will have the suggestions shown when a mouse is hovered on it.

The following diagnostic operations are supported:

- Image Validation - Identifies whether the image (ROMMON or LINUX) installed on the device is in a good state.

  Error messages:

  - LINUX image is either not installed or it is corrupt. Please re-install LINUX image and try again.

    - ROMMON is up and running. Please load LINUX and try again.

- Authentication Check - Checks if the device has completed 802.1x and 802.11i authentications in the network.
    - 802.1x

      Error message: Seems like 802.1x is disabled. Please follow the instructions to configure 802.1x authentication correctly.
    - 802.11i

      Error messages:
        - 802.11i is disabled. Please follow the instructions to configure 802.11i authentication correctly.
        - Seems like pmkId is not set. Please carryout 802.1x authentication.
        - Device should have at least one gtkId to participate in 802.11i authentication process.
        - gtkid is expired. Please renew it.

- DHCP Check - Verifies whether the device has the DHCP lease period and got IPV6 address assigned.

  Error message: DHCP lease is expired. Please renew it.
- FND Registration Check - Identifies whether the device is successfully registered with FND server. The following checks will be performed:
    - Time synchronization issue - IoT-DM compares the time of IR510 with the time of FND to check if the time is synchronized. If their is a time sync issue then below error message is shown:

      Error message: Device time is not synched properly. Please correct the device time and try again.
    - Registration process issue - Displays the registration failure cause.

      Error message: There seems to be issue with registration process. Error Code: xxx.
    - Certificate validity

      Error message: NMS Certificate is invalid. Please load the valid NMS certificate and try again.

  Default message: Check if the device is added in FND DB.

  Note As part of the FND registration diagnostic operation , there will be an FND API call to get the Current Time. Credentials will be taken from the CGMS Settings page if field technician had entered it before. If not, a seperate screen would be shown to you to enter the details of FND Server with which the time sync operation will be performed. You may choose to skip it if you do not want to enter the details of the FND server. In that case, the Time synchronization check will be ignored while performing diagnostic operations.

- Connectivity Diagnostic operations - Identifies whether the device connectivity is up to the mark with other interfaces on the field.
    - RF Health Check - Status of WPAN LED will be displayed.

    - Ethernet Link Check - Status of Ethernet will be displayed.
    - FND connectivity Check
- IOx Health Check - Performs the diagnostic operations on the IOx module installed in the device.
    - IOx Host Status - The status of the host on which IOx runs will be displayed.
    - IOx Status - The status of IOx process will be displayed.
- GPS Status Check
    - GPS enabled or not
    - GPS locked or not
- EST Status Check
    - Certificate downloaded or not
    - Trust anchor present or not