Industrial Network Director リリース 1.10.x リリースノート

初版:2021 年 5 月 14 日

このリリースノートでは、産業用イーサネットスイッチの設定と管理をサポートする Cisco Industrial Network Director（IND）アプリケーションのリリース 1.10.0 に関する最新情報について説明します。

IND アプリケーションには 3 つのタイプのオンラインヘルプ（OLH）があります。状況依存ヘルプ、ガイド付きツアーのような組み込み型ヘルプ、およびツールヒントです。

注:IND リリース 1.10.0 は、英語、フランス語、ドイツ語、日本語、およびスペイン語のオンラインヘルプをサポートしています。

マニュアル

注: この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

Organization

このリリースノートの内容は、次のとおりです。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザーが値を指定する関数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

(注) *読者に留意していただきたいことを示します。*役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

「注意:」は、***注意が必要なことを示しています。機器の損傷またはデータ損失を予防するための注意事項が記述されています。***

Cisco IND について

Cisco Industrial Network Director は簡単に統合できる管理システムで、産業用ネットワークの運用チームはネットワーク監視とトラブルシューティングを合理化できるため、オペレータと技術者の生産性が向上します。IND はシスコの包括的な IoT ソリューションの一部です。

- シスコの産業用イーサネット製品ファミリの全機能を活用し、IT 部門外の運用担当者がネットワークを利用することを可能にする、使いやすい産業用ネットワーク管理システムです。
- 産業用プロトコル(BACnet/IP、CIP、Modbus、PROFINET、OPC UA)の検出機能を使用して自動化およびネットワーキング資産の動的な統合トポロジを作成し、運用担当者と IT 担当者に共通のフレームワークを提供します。これにより、ネットワークの監視とトラブルシューティングが可能になり、計画外のダウンタイムから速やかに回復できるようになります。
- リッチ API により、既存の産業用アセット管理システムにネットワーク情報を簡単に統合できます。また、顧客やシステムインテグレータは、モニタリングとアカウンティングに関する特定のニーズに合わせてカスタマイズされたダッシュボードを作成できます。
- 既存システムへの統合、およびシステムインテグレータによるカスタマイズ。

- カスタマイズ可能な権限マッピングを備えたユーザ管理により、システムアクセスが機能ごとに承認されたユーザに制限されます。
- ネットワークの変更、追加、改良に関して運用上の可視性を維持するために詳細な監査証跡を取得することで、変更の管理用にネットワークデバイスに対するユーザアクションが記録されます。
- 主な機能に検索機能が統合されているため、機能および情報を簡単に検索できます。
- Cisco Active Advisor は無償のクラウドベースサービスで、セキュリティと製品の更新プログラムを最新状態に維持するのに必要なネットワークライフサイクル情報を提供します。
- ガイド付きツアーは段階的なガイダンスで、生産性を最大化し、導入を容易にします。

IND 1.8 から IND 10.0 へのアップグレード

注:IND 1.8.x から IND 1.10.x にアップグレードすると、ネットワーク管理者ロールにディスカバリ権限が自動的に割り当てられ、新しいロール名「Network Discovery Administrator」が付与されます。さらに、次のパターンもあります。

- アップグレード時に、すべてのユーザがデフォルトルートグループに割り当てられます。
- 選択したグループ(グループコンテキストビュー)とそのサブグループにリストされているデバイスのみがインベントリに表示されます。
- ロールにネットワーク設定権限が含まれるユーザのみが、承認グループ内のグループサブツリー内のグループを表示、更新、または削除できます。
- 選択したグループ(グループコンテキストビュー)およびそのサブグループ内のデバイスに関連するアラームのみが [Alarms] ページに表示されます。

サポートされる新しいプラットフォームと機能

次の新しい機能が IND リリース 1.10.0 でサポートされています。

- Media Redundancy Protocol のネットワークモニタリング(4 ページ)
- Parallel Redundancy Protocol(PRP)のネットワークモニタリング(4 ページ)
- デバイスを手動で追加(5 ページ)
- 検出デバイスのフィールドの手動更新(6 ページ)

このリリースノートでは、IND とそのユーザインターフェイスでサポートされる 4 つの主要機能に含まれる新機能について説明します。

- 設計
- 操作(オペレーション)
- 保守(メンテナンス)
- 設定

IND オンラインヘルプには、次の新機能の関連情報が含まれています。

Media Redundancy Protocol のネットワークモニタリング

Media Redundancy Protocol（MRP）のネットワークモニタリングを実行できます。MRP は、国際電気標準会議（IEC）によって IEC 62439-2 として標準化されたデータ ネットワーク プロトコルです。MRP は、イーサネットスイッチのリングが、スパニングツリープロトコルよりもはるかに短い回復時間で単一の障害を克服することを可能にします。ほとんどの産業用イーサネット アプリケーションに適しています。

MRP は MAC レイヤで動作し、製造業における産業ネットワークの PROFINET 規格と合わせて一般的に使用されます。

MRP は、産業オートメーション ネットワークのリングネットワークトポロジで高速コンバージェンスを実現します。MRP Media Redundancy Manager（MRM）は、リングの最大リカバリ時間を 10 ミリ秒、30 ミリ秒、200 ミリ秒、500 ミリ秒の範囲で定義します。

IND は、MRP をサポートする Cisco スイッチおよび Siemens Profinet PLC/IO デバイスに対してのみ MRP モニタリングをサポートします。

注：MRP をサポートする Profinet PLC および I/O デバイスは、IND でライセンスおよび監視できます。

次の MRP 関連情報が IND によって収集されます。

- MRP リング情報
- MRP ポート情報

次の MRP アラームがサポートされています。

- MRP リングのオープン：デバイスが開始した SNMP トラップに基づいて処理されました。マネージャの役割を果たしている Cisco スイッチにのみ適用されます。
- MRP マネージャの変更：検出された MRP リングのマネージャロールの変更を示すアラームがシステムによって生成されました。このアラームは、マネージャロールが変更されたデバイスの定期的またはオンデマンドのデータ収集中に発生します。

注：MRP マネージャの変更アラームは、インベントリ内の次のロールが変更されたデバイスに対して発生します。

- **現在のロール**：マネージャ ----> **新しいロール**：クライアント
- **現在のロール**：クライアント ----> **新しいロール**：マネージャ

サポートされるデバイス：

- MRP をサポートする IE2000、IE4000、IE4010、IE5000、および IE3x00 製品ファミリ PID
- MRP をサポートする Siemens Profinet PLC/IO デバイス

Parallel Redundancy Protocol（PRP）のネットワークモニタリング

Parallel Redundancy Protocol（PRP）のネットワークモニタリングを実行できます。PRP は、国際規格 IEC 62439-3 で定義されているように、イーサネットネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。

PRP は、他の冗長プロトコルとは異なる方式を使用します。この方式では、2 つのネットワーク インターフェイスを 2 つの独立した分離されたパラレルネットワークに接続することで、（ネットワーク要素ではなく）エンドノードが冗長性を実装します。

IND は、Cisco IOS 15.2(6) 以降のリリースを実行しているデバイスで PRP をサポートし、PRP の CIP/SNMP サポートを組み込みます。

次の PRP 関連情報が IND によって収集されます。

- 次のものを含む、PRP ノード（RedBox および DAN）の詳細。
  - チャネル設定とインターフェイスの詳細
  - LAN-A および LAN-B ポートのエラーカウント（インターフェイスカウンタから取得）を含むチャネル統計情報。
  - ノードテーブルと VDAN テーブル（DAN のみ）
- 障害が発生した場合のアラーム。デバイスからのトラップがない場合には、定期的およびオンデマンド更新中にアラームが発生します。

サポートされるデバイス：

- ENT2P ControlLogix Ethernet/IP モジュールなどの CIP オブジェクト 56 および 57 をサポートする IACS デバイス
- 産業用イーサネットスイッチ：IE 4000、IE 4010、IE 5000、IE2000U、いくつかの PID、s5400、s5410、IE3400 および IE3400H スイッチ

各デバイスには、PRP チャネルに参加する定義済みのポートがあります。小さい番号のギガビット イーサネット メンバーポートがプライマリポートで、LAN-A に接続します。大きい番号のポートがセカンダリポートで、LAN-B に接続します。

次のアラームは、PRP 障害が発生した場合の定期的およびオンデマンド更新中に生成されます。

- PRP Channel Interface Down：PRP チャネルのいずれかのポートがダウンするとトリガーされます。
- LAN-A で表示される PRP 警告/LAN-B で表示される PRP 警告：入力警告統計値に基づいて発生します。これは、LAN-A/LAN-B ポートに潜在的な問題があることを示しています。
- LAN-A で表示される PRP 警告数/LAN-B で表示される PRP 警告数：LAN-A/LAN-B で入力警告数の増加が確認されるとトリガーされます。

注：CIP/SNMP をサポートする PRP は、Cisco IOS 15.2(6) で初めてサポートされました。

デバイスを手動で追加

デバイスを検出できない場合、**または**デバイスが MAC アドレスや IP アドレスなどの必要な情報を返さない場合、またはデバイスが IND でサポートされている検出プロトコル通信に応答できない場合、IND インベントリにエンドポイントデバイスを手動で追加できます。

これらのデバイスを手動で追加することにより、IND は、デバイスに対してタギング、グループへの割り当て、pxGrid サービスを介した ISE へのアセット情報の送信をサポートできます。

単一のデバイスを追加することも、CSV ファイルを使用してデバイスの一括追加を実行することも可能です。

検出権限を持つユーザは、[Discovery] ページの左側にある [Manually Add Device] メニュータイルをクリックしてデバイスを追加できます。

[Operate] > [Discovery]

検出デバイスのフィールドの手動更新

デバイスが検出中にすべての関連情報を返さない場合、またはフィールドにカスタム値を追加する場合は、任意のデバイスのデバイス情報を手動で更新できます。

更新は、プロトコルが MULTIPROTOCOL の場合、検出されたデバイスの [Name] および [Description] フィールドでのみサポートされます。

更新は、共通フィールドでのみサポートされ、プロトコル固有のフィールドではサポートされません。

デバイス管理権限を持つユーザは、デバイスを更新できます。

手動で更新したフィールド値は、自動更新より優先されます。具体的には、手動で更新された値は、定期的なインベントリデータ更新または手動でのデータ更新時にデバイスから取得されたデータで上書きされません。ユーザがデバイスの属性を更新すると、その属性は、デバイスが削除され再検出されるまで、自動検出により更新されることはありません。

[Operate] > [Discovery]

システム要件

表 1　システム要件

デスクトップ要件	最小要件
Windows オペレーティング システム（OS）	Windows 7 Enterprise または Professional、サービスパック 2 Windows 10 Windows 2012 R2 Server
ブラウザ	Chrome：バージョン 50.0.2661.75、53.0.2785.116 以降 Firefox：55.0.3、57.04、63.0.3 以降
CPU	クワッドコア 1.8 GHz
RAM	8 GB
ストレージ	50 GB

IE スイッチの事前設定要件

ここでは、IND がサポート対象のデバイスを検出するために必要な CLI での設定を示します。

- Cisco IOS が動作する IE スイッチについては、「Cisco IOS を実行するすべての IE スイッチに必要な前提条件の設定」を参照してください。
- IE1000 スイッチについては、「Cisco IOS の検出と管理に必要な設定」を参照してください。

Cisco IOS を実行するすべての IE スイッチに必要な前提条件の設定

ここでは、システムがライセンスデバイスを検出し、デバイスの状態を [Unlicensed] から [Licensed] に移行するために必要な CLI の設定について説明します。

また、IE 1000 スイッチで必要なデバイスマネージャの設定についても説明します。

注：TACACS が利用可能な場合、デバイスのローカルアカウントは必要ありません。

Cisco IOS の検出と管理に必要な設定

この機能の設定情報は、IND 1.10 OLH の *[Device Prerequisite Configuration]* という見出しの下にあります。

次の手順に従って、IND がデバイスを検出し、UNLICENSED 状態から LICENSED 状態に移行できるようにスイッチを設定します。

1. グローバル コンフィギュレーション モードを開始します。

   configure terminal

2. システムが正確にデバイスを検出できるように SNMP を設定します。

   snmp-server community *read-community* **ro**

read-community は、システムのアクセスプロファイルで定義されている SNMP V2 読み取り文字列と一致している必要があります。アクセスプロファイルは、ディスカバリプロファイルに関連付けられています。デフォルトの read-community 文字列は「public」です。

3. 次のコマンドを入力して、システムがライセンス付与されたデバイスを検出し、SNMPv3 を使用して UNLICENSED 状態から LICENSED 状態にデバイスを移行できるようにします。作成したグループとモードは、次のステップで設定する SNMPv3 ユーザに関連付けるために使用します。グループに対して選択したモードに基づいて、ユーザの認証、プライバシープロトコル、およびパスワードを設定できます。

   snmp-server group *group_name* **v3** *mode*

   mode は次のいずれかです。

   priv：Data Encryption Standard（DES; データ暗号規格）パケットの暗号化を有効にします

   auth：Message Digest（MD5）および Secure Hash Algorithm（SHA）によるパケット認証が可能です

   noauth：noAuthNoPriv というセキュリティレベルをイネーブルにします。no-keyword が指定されている場合、これがデフォルトです。

4. SNMP グループに対して新規ユーザを追加します。

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

   注：**auth** または **priv** のパスワードは 64 文字を超えないようにします。

   — **auth**：認証レベル設定セッションです。HMAC-MD5-96（**md5**）または HMAC-SHA-96（**sha**）認証レベルのどちらかを指定でき、パスワードストリング *auth-password* が必要です。サポートされている privacy_type の値は **{aes | 128 | des}** です

   — **priv**：プライベート（**priv**）暗号化アルゴリズムおよびパスワードストリング *priv-password* を設定します

5. システムがデバイスを UNLICENSED 状態から LICENSED 状態に正常に移行するように、次を設定します。これは、システムのアクセスプロファイルで指定されたデバイスアクセス用のユーザ名とパスワードと一致する必要があります。

   username *username* **privilege 15 password 0** *password*

6. 認証、認可、およびアカウンティング（AAA）を設定するには、次のコマンドを入力します。

   aaa new-model

   aaa authentication login default local

   aaa authorization exec default local

7. セキュアシェル(SSH)サーバを設定します。

   ip ssh version 2

8. HTTP/HTTPS サーバを設定します。

   ip http server

   ip http secure-server

   ip http authentication aaa login-authentication default

9. 回線の Telnet セッションの数(回数)と Telnet パスワードを設定します。

   line vty 0 15

   login authentication default

   transport input all

   transport output all

10. 特権 EXEC モードに戻ります。

    end

IE 1000 スイッチの検出と管理に必要なデバイスマネージャの設定

1. IE 1000 デバイスマネージャにログインします。
2. ユーザ名フィールドは空白にして、パスワードとして **cisco** と入力します。
3. [Admin] > [Users] を選択します。
4. デバイスアクセスユーザを作成し、IND のアクセスプロファイルでも同じユーザを使用します。
5. SNMP コミュニティストリングを読み取り専用(ro)に設定します。

   a. [Configure] > [SNMP] を選択します。ポップアップウィンドウで [OK] をクリックして SNMP を確定します。

   b. チェックボックスをオンにすると、SNMP モードがグローバルに有効になります。[Submit] をクリックします。

6. [Community Strings] タブを選択します。コミュニティストリング *public* の読み取り専用アクセスを追加します。(デフォルトでは、これは読み取り専用(ro)ストリングです)

   SNMPv3 の場合:

   a. [Users] タブを選択し、名前、セキュリティレベル、認証プロトコル、認証パスワード、プライバシープロトコル、およびプライバシーパスワードを使用して snmpv3 ユーザを追加します。**OK** をクリックします。

   b. [Group] タブを選択し、作成したユーザを選択し、グループ名を指定します。**OK** をクリックします。

7. [Admin] > [Access Management] を選択します。

   a. SSH または Telnet を有効にするには、このチェックボックスをオンにします。(このオプションは IE1000 と IND の通信方法を決定します)

   b. [Submit] をクリックします。

IE スイッチのブートストラップ設定

関連していますか？更新がありますか？

システム内でデバイスをライセンス状態に移行すると、次の設定がプッシュされます。

注: 次の設定スクリプトでは、**{certificate key length}** はデバイスのアクセスプロファイルから取得されます。

```
# Secure-mode only
# If the device has a self-signed certificate with RSA key pair length <{certificate-key-length}.The
certificate key length is obtained from the device access profile.\ (or) if the device does not have a
self-signed certificate in nvram
crypto key generate rsa label IND_HTTPS_CERT_KEYPAIR
modulus <{certificate-key-length}>
crypto pki trustpoint IND_HTTP_CERT_KEYPAIR
enrollment selfsigned
subject-name OU=”IOT”
rsakeypair IND_HTTPS_CERT_KEYPAIR
hash sha256
crypto pki enroll IND_HTTPS_CERT_KEYPAIR
# Enable SCP server
# Used for transferring ODM file from the system to device
# For insecure mode the system uses FTP to transfer ODM file
ip scp server enable

# If AAA is not enabled on the device
ip http authentication local
#Secure mode only
ip http secure-server
ip http secure-port {secure-mode-access-port}
#Insecure mode only
ip http server
ip http port {regular-mode-access-port}

# Configure WSMA
# The system uses WSMA for management
wsma agent exec
profile exec
# Secure-mode only
wsma profile listener exec
transport https path /wsma/exec
# Insecure mode only
wsma profile listener exec
transport http path /wsma/exec

# SNMP configuration
# Trap destination. The system supports both v2c and v3
snmp-server host <ind-ip-address> version 2c {snmpv2-read-community} udp-port 30162
# Trap destination for v3 security
snmp-server host {ind-ip-address} version 3 {snmpv3_mode} {snmpv3_username} udp-port 30162

# Bootstrap configuration for SNMPv3
# The system needs the following configuration to be able to query bridge-mib with SNMPv3
security in IOS devices.
# This bridge-mib is required by inventory service to get MAC-Table from SNMP when the
system moves device from new to managed state.
snmp-server group {group_name} v3 {snmpv3_mode} context vlan- match prefix
# Enable RFC2233 compliant for linkDown and linkUp trap
snmp-server trap link ietf
```

```
# Enable traps supported by the system
snmp-server enable traps snmp linkdown linkup coldstart
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps rep
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps flash insertion removal
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps alarms informational
snmp-server enable traps errdisable
snmp-server enable traps mac-notification change move threshold
# Configure SNMP to retain ifindex across reboots
snmp ifmib ifindex persist

# Enable dual-power supply
# Not applicable for S5410, IE5K, CGS2K, IE3010
power-supply dual

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

IE 1000S スイッチのブートストラップ設定

関連していますか？

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

設置上の注意事項

IND アプリケーションのインストール

IND のインストール手順については、『Installation Guide for Industrial Network Director for Release 1.10.0』を参照してください。

デバイスパックのインストール

インストール要件

IND デバイスパックは、*バージョン番号*が一致する IND アプリケーションでのみインストールできます。*リリース番号*は、IND リリース番号以降である**必要があります**。

たとえば、リリース 1.10.x の場合、1.10 がバージョン番号、x がリリース番号です。

新しいデバイスパックはバージョン 1.10.0 である必要があります。

インストールの手順

デバイスパックのインストール手順については、『Installation Guide for Cisco Industrial Network Director, Release 1.10.0』を参照してください。

特記事項

Windows OS、Cisco IOS ソフトウェアと IND の PID サポートに関する次の情報をご確認ください。

- 1.8 から 1.10 にアップグレードする場合は、IND pxGrid 証明書を ISE に再アップロードする必要があります。

  自己署名証明書は、自己署名証明書の有効期間を 398 日に制限することで、MacOS で発行されます。

  すべてのシステム自己署名証明書は、iOS 13 および macOS 10.15 の TLS サーバ証明書の新しいセキュリティ要件を満たすためにアップグレード時に再生成されます。

サポートされる IND リリースアップグレード

次の IND アップグレードを実行できます。

- 1.9.0 から 1.10.0 へのアップグレード。
- 1.8.0 から 1.9.0 へのアップグレード
- 1.7.1 から 1.8.0 へのアップグレード
- 1.7.0 から 1.8.0 へのアップグレード
- 1.6.1 から 1.8.0 へのアップグレード
- 1.6.1 から 1.8.0 へのアップグレード
- 1.6.0 から 1.8.0 へのアップグレード
- 1.6.x から 1.7.x へのアップグレード

制限事項と制約事項

IoT IND の使用を開始する前に、このセクションを確認することをお勧めします。対処できない問題が存在することも判明しており、問題の回避策がない場合もあります。一部の機能は設計通りに動作しなかったり、ソフトウェアに加えた最新の変更の影響を受けたりすることも考えられます。

- IND は、6 つのグループで管理対象デバイスをアップグレードします。このアプローチは、サーバリソースが過負荷にならないように設計されています。
- IND を実行している Windows サーバが突然シャットダウンしないようにしてください。シャットダウンすると、IND が機能するために必要なファイルが失われる可能性があります。
- 15.2(7)E1a より前の Cisco IOS リリースを実行している新たに検出されたデバイスの状態遷移は、セキュアモードで Unlicensed 状態から Licensed 状態に移行できません。15.2(7)E1a より前の Cisco IOS リリースを実行している IND によってすでに管理されているデバイスのメトリック収集は、セキュアモードでの自己署名証明書の期限切れにより失敗します。Telnet は、15.2(7)E1a より前のソフトウェアバージョンを実行しているスイッチで問題なく動作します。
- スイッチが Cisco IOS リリース 15.2(4) ソフトウェアを実行している場合は、デバイスとのセキュアな通信に弱い暗号を使用する**必要があります**。弱い暗号は、IND でデフォルトで無効になっています。有効にするには、[Settings] > [System Settings] > [Security Settings] に移動します。
- IND でのデバイスイメージのアップグレード：デバイスがセキュアモードで IND で管理されている場合、イメージのアップグレードは、メモリが少なく SD フラッシュをサポートしていないデバイスではサポート**されません**。イメージをアップグレードするにはデバイスマネージャを使用してください。
- SNMPv3 プロトコルは、16.10.1 で動作するデバイス IE3x00 では機能しません
- PnP プロセスは、Cisco IOS リリース 15.2(6)E1 のシングルホーム（シングル IP）IND サーバでのみサポートされます。

  注：AAA コマンドが機能しないため、Cisco IOS リリース 15.2(6)E0a で PnP サービスエラー 1410 が発生します。（CSCvg64039）。CDET で現在「再現不能」とマークされている警告です。**注**：この問題は、Cisco IOS 15.2(6)E0a 以降のソフトウェアリリースで解決されています。
- IE 5000：水平スタッキングはサポートされていません。スタックされたデバイスは IND で検出できますが、ライセンスを取得することはできません。
- IOS デバイスには、ソフトウェアイメージのアップグレードを使用して IND からデバイスをアップグレードするための十分なスペースがフラッシュディレクトリに必要です。メモリが少ないデバイスの場合は、リムーバブル SD フラッシュメモリカードを使用します。
- IND の以前のバージョンで検出された PRP または MRP 対応デバイスは、IND 1.10 へのアップグレード後に PRP または MRP をサポートしません。PRP または MRP サポートを有効にするには、IND 1.10 でデバイスを再検出する必要があります。

警告

このセクションでは、このリリースの未解決および解決済みの警告と、この警告の詳細を確認するための Bug Search Tool の使用方法について説明します。セクションのトピックは次のとおりです。

未解決の警告

表 2　未解決の不具合

警告番号	説明
CSCvq23714	IE1k PnP が CA 署名付き証明書で失敗します。
CSCvy03179	自己署名証明書が IE1K 1.8.1 で失敗します。

解決済みの警告

表 3　解決済みのプラットフォーム関連の警告

警告番号	説明
CSCvv10572	2.4 P13 で ISE に IND を登録できない

Bug Search Tool へのアクセス

問題と利用可能な回避策の説明など、このリリースの警告に関する情報を探すには、Bug Search Tool を使用することができます。Bug Search Tool には、未解決の不具合と解決済みの不具合の両方が表示されます。

Bug Search Tool にアクセスするには、次のアイテムが必要です。

- インターネット接続
- ウェブ ブラウザ
- Cisco .com のユーザ ID とパスワード

Bug Search Tool にアクセスするには、この URL（https://tools.cisco.com/bugsearch/search）を使用してください

特定のバグ ID を使用して検索するには、この URL（https://tools.cisco.com/bugsearch/bug/*<BUGID>*）を使用してください。

関連資料

Installation Guide for Industrial Network Director Application for Release 1.10.0

Cisco Industrial Ethernet スイッチのドキュメントを参照してください（関連するスイッチのリンクを選択してページ下部のユーザガイドにアクセスします）

- Cisco Industrial Ethernet 1000 シリーズ スイッチ
- Cisco Industrial Ethernet 4000 シリーズ スイッチ
- Cisco Industrial Ethernet 4010 シリーズ スイッチ
- Cisco Industrial Ethernet 5000 シリーズスイッチ

本ドキュメントでは、併用は承認されておらず、意図されてもいません。

関連資料