



収集ジョブの管理

ここでは、次の内容について説明します。

- [収集ジョブについて](#) (1 ページ)
- [収集ジョブの作成](#) (33 ページ)
- [収集ジョブの削除](#) (39 ページ)
- [収集ジョブのモニタリング](#) (39 ページ)
- [SNMP での収集用に事前にロードしたトラップと MIB のリスト](#) (43 ページ)
- [MDT での収集用に事前にロードした YANG モジュールのリスト](#) (49 ページ)

収集ジョブについて

収集ジョブは、Cisco Crosswork Data Gateway が実行することが期待されるタスクを記述します。アプリケーションは、収集ジョブを介してデータ収集を要求します。次に、Cisco Crosswork はこれらの収集ジョブを Cisco Crosswork Data Gateway に割り当てて、要求に対応できるようにします。

個別の収集ジョブを使用して、一度に複数のタイプのデータを収集できます。

作成した収集ジョブごとに、Cisco Crosswork Data Gateway は収集要求を実行し、収集したデータを優先データ先に保管します。

Cisco Crosswork Data Gateway では、次のタイプの収集ジョブを作成できます。

- [CLI 収集ジョブ](#) (2 ページ)
- [SNMP 収集ジョブ](#) (4 ページ)
- [MDT 収集ジョブ](#) (12 ページ)
- [gNMI 収集ジョブ](#) (14 ページ)
- [Syslog 収集ジョブ](#) (23 ページ)



- (注)
1. Cisco Crosswork Data Gateway は、対応する（リスニング）収集ジョブの要求がない場合は着信トラフィックをドロップします。また、未承認デバイス（つまり、Cisco Crosswork Data Gateway に接続されていないデバイス）から受信したデータ、syslog イベント、および SNMP トラップもドロップします。
 2. ポーリングされたデータは、Cisco Crosswork Data Gateway がデータを処理して送信する準備ができるまでデバイスから要求できません。

アクティブ収集ジョブのスマートライセンス

データをサードパーティの宛先に転送できる収集ジョブを作成できるようにするには、次のスマートライセンス要件が満たされていることを確認してください。

1. メインメニューから、**[管理 (Administration)] > [アプリケーション管理 (Application Management)] > [スマートライセンス (Smart License)]** に移動し、Cisco Crosswork アプリケーションを選択します。
2. ステータスが次のようになっていることを確認します。
 - **[登録ステータス (Registration Status)]** : **[登録済み (Registered)]**
Cisco Smart Software Manager (CSSM) に登録済みであり、予約済みライセンス機能の使用が許可されていることを示します。
 - **[ライセンス認証ステータス (License Authorization Status)]** : **[認証済み (Authorized)]** (**[準拠 (In Compliance)]**)
外部収集ジョブのデバイス数を超えていないことを示します。

評価期間 (**[登録ステータス (Registration Status)]** が未登録、**[ライセンス承認ステータス (License Authorization Status)]** が評価モード) では、評価期間が終了するまで収集ジョブを作成することができます。この後、ライセンス機能を使用するには、Cisco Smart Software Manager (CSSM) に登録する必要があります。詳細については、「[ライセンスの管理](#)」セクションを参照してください。

評価期間の終了後に Cisco Smart Software Manager (CSSM) に登録しないと、収集ジョブを作成できません。ただし、この場合も収集ジョブは表示および削除できます。

CLI 収集ジョブ

Cisco Crosswork Data Gateway は、ネットワークデバイスからの CLI ベースのデータ収集をサポートしています。このタイプの収集ジョブでは、show コマンドのみがサポートされています。



- (注)
- UI のすべての収集ジョブの初期ステータスは不明です。CLI 収集ジョブを受信すると、Cisco Crosswork Data Gateway は基本的な検証を実行します。収集ジョブが有効な場合、そのステータスは[成功 (Successful)] に変わります。それ以外の場合は[失敗 (Failed)] に変わります。
 - CLI 収集を適切に動作させるためには、デバイスにバナー設定を含めないでください。これをオフにする方法については、デバイスのマニュアルを参照してください。
 - **Cadence** の値は秒単位です。センサーが 1 回だけ収集されるように構成されていることを示すには、0 に設定する必要があります。
または
60 (つまり、少なくとも 1 分) から最大 2764800 秒 (つまり最大 32 日) である必要があります。これは、設定されたセンサーデータを収集する頻度を示します。
 - 前の実行がまだ進行中であるためにデバイスからの収集がスキップされると、Cisco Crosswork Data Gateway は警告ログを生成します。このシナリオではアラートは生成されません。

以下は、CLI 収集ジョブのサンプルです。詳細については、[Cisco DevNet](#) の API ドキュメントを参照してください。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "658adb03-cc61-448d-972f-4fcec32cbfe8"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "cadence_in_millisec": "tel:60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
```

```

        "cli_sensor": {
            "command": "show platform"
        }
    },
    "destination": {
        "destination_id": "1e71f2fb-ea65-4242-8efa-e33cec71b369",
        "context_id": "topic1"
    }
}
]
}
}

```

SNMP 収集ジョブ

Cisco Crosswork Data Gateway では、デバイスでサポートされている OID に基づく SNMP ベースのデータ収集をサポートしています。

SNMP コレクタは、設定プロファイル（収集する MIB オブジェクトのリストと取得先のデバイスのリスト）を取得するためのポーリング要求を Cisco Crosswork に行います。事前にパッケージ化された MIB モジュールのリストまたは MIB モジュールのカスタムリストを検索して、対応する OID を決定します。



- (注) Cisco Crosswork Data Gateway は、システムにすでに含まれている標準的な MIB のサードパーティ製デバイスで SNMP ポーリングを有効にします。独自の MIB は、収集要求が独自の MIB から MIB テーブル名またはスカラー名を参照する場合にのみ必要です。ただし、要求が OID ベースの場合、MIB は必要ありません。

OID が解決されると、SNMP コレクタへの入力として提供されます。

[カスタム ソフトウェア パッケージの追加](#)の説明に従って、Crosswork Data Gateway VM にデバイスパッケージをインポートできます。

次の SNMP バージョンがサポートされています。

- SNMPv1
- SNMPv2c
- SNMPv3

次の表に、サポートされているプライバシープロトコルと、SNMP および SNMP トラップ収集ジョブの収集ペイロードで指定する必要のある値を示します。

プロトコル	SNMP 収集ペイロード	SNMP トラップ収集ペイロード
aes	AES	該当なし
des56	DES	該当なし
3des	3DES	該当なし

プロトコル	SNMP 収集ペイロード	SNMP トラップ収集ペイロード
aes 128	AES128	該当なし
aes 192	AES192 または CiscoAES192 (シスコ固有)	該当なし
aes 256	AES256 または CiscoAES256 (シスコ固有)	該当なし



- (注)
- UIのすべての収集ジョブの初期ステータスは不明です。SNMP収集ジョブを受信すると、Cisco Crosswork Data Gatewayは基本的な検証を実行します。収集ジョブが有効な場合、そのステータスは[成功 (Successful)]に変わります。それ以外の場合は[失敗 (Failed)]に変わります。
 - **Cadence**の値は秒単位です。センサーが1回だけ収集されるように設定されていることを示すには、0に設定する必要があります。
または
60 (つまり、少なくとも1分) から最大 2764800 秒 (つまり最大 32 日) である必要があります。これは、設定されたセンサーデータを収集する頻度を示します。
 - 前の実行がまだ進行中であるためにデバイスからの収集がスキップされると、Cisco Crosswork Data Gatewayは警告ログを生成します。このシナリオではアラートは生成されません。
 - SNMPv1/v2cの場合、ペイロード内のデバイスの詳細 (ホストやコミュニティストリングなど) が正しくない場合、Cisco Crosswork Data Gatewayはデバイスから受信したトラップを無視し、WARNメッセージをログに記録します。
 - SNMPトラップでは、SNMPv1およびSNMPv2cバージョンのみがサポートされています。
 - SNMPv3の場合、ペイロード内のデバイスの詳細 (auth、priv、セキュリティ名の詳細など) が正しくない場合、Cisco Crosswork Data Gatewayはそれを除外するため、トラップを受信しません。したがって、WARNメッセージはログに記録されません。

デバイスでの設定例：

表 1:

バージョン	コマンド	目的
V1	<pre>snmp-server group <group_name> v1 snmp-server user <user_name> <group_name> v1</pre>	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	<pre>snmp-server host <host_ip> traps <community_string> udp-port 1062</pre> <p>次の例を参考にしてください。</p> <pre>snmp-server host a.b.c.d traps test udp-port 1062</pre>	トラップデータの転送先を定義します。
	<pre>snmp-server traps snmp linkup snmp-server traps snmp linkdown</pre>	リンクステータスを通知するトラップを有効にします。
V2c	<pre>snmp-server group <group_name> v2c snmp-server user <user_name> <group_name> v2c</pre>	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	<pre>snmp-server host <host_ip> traps SNMP version <community_string> udp-port 1062</pre> <pre>snmp-server host a.b.c.d traps version 2c v2test udp-port 1062</pre>	トラップデータの転送先を定義します。
	<pre>snmp-server traps snmp linkup snmp-server traps snmp linkdown</pre>	リンクステータスを通知するトラップを有効にします。

バージョン	コマンド	目的
V3	<pre>snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name> snmp-server view <user_name> 1.3 included</pre>	SNMP バージョン、ユーザー/ユーザーグループの詳細を定義します。
	<pre>snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password> snmp-server host <host_IP> traps version 3 priv <user_name> udp-port 1062</pre>	トラップデータの転送先を定義します。
	<pre>snmp-server traps snmp linkup snmp-server traps snmp linkdown</pre>	リンクステータスを通知するトラップを有効にします。

SNMP コレクタは、次の操作をサポートしています。

- スカラー
- TABLE
- MIB_WALK
- TRAP
- DEVICE_PACKAGE

これらの操作は、センサー設定で定義されます（以下のペイロード例を参照）。



(注) デバイスの応答時間が非常に長い場合に使用する必要があるオプションの **deviceParams** 属性 **snmpRequestTimeoutMillis**（サンプルペイロードには表示されていません）があります。デバイスの応答時間が非常に長いことが確実にない限り、**snmpRequestTimeoutMillis** を使用することは推奨されません。

snmpRequestTimeoutMillis の値はミリ秒単位で指定する必要があります。

デフォルト値は 1500 ミリ秒です。

最小値は 1500 ミリ秒です。

ただし、この属性の最大値に制限はありません。

次に、SNMP 収集ジョブの例を示します。

```

{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SNMP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c70fc034-0cbd-443f-ad3d-a30d4319f937",
            "8627c130-9127-4ed7-ace5-93d3b4321d5e",
            "c0067069-c8f6-4183-9e67-1f2e9bf56f58"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        },
        "cadence_in_millisec": "60000"
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_461cb8aa-a16a-44b8-b79f-c3daf3ea925f"
        }
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {

```



```

        "oid": "1.3.6.1.2.1.31.1.1",
        "snmp_operation": "TABLE"
    }
}
},
"destination": {
    "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
    "context_id": "topic2_e7ed6300-fc8c-47ee-8445-70e543057f8a"
}
}
]
}
}
}

```

SNMP トラップ収集ジョブ

SNMP トラップも同様の方法で処理されます。トラップリスナーはポートでリッスンし、（関心のあるトピックに基づいて）受信者にデータをディスパッチします。

Cisco Crosswork Data Gateway は、次の3つのタイプの非 YANG/OID ベースのトラップをサポートします。

センサーパス	目的
*	フィルタなしでデバイスからプッシュされたすべてのトラップを取得します。
MIB レベルトラップ	1 つの MIB 通知の OID (例: すべての isis-mib レベルトラップを取得する場合は 1.3.6.1.2.1.138.0)
特定のトラップ	特定のトラップの OID (例: linkUp トラップを取得する場合は 1.3.6.1.6.3.1.1.5.4)



- (注)
- デバイスは、トラップによって事前に設定されている必要があります。
 - Cisco Crosswork Data Gateway は UDP ポート 1062 でトラップをリッスンします。
 - 収集ジョブが無効か、デバイスに設定がないか、またはトラップが受信されない場合、ジョブのステータスは [不明 (Unknown)] のままです。
 - サポートされているトラップと MIB のリストについては、「[SNMP での収集用に事前にロードしたトラップと MIB のリスト \(43 ページ\)](#)」を参照してください。

トラップを受信すると、Cisco Crosswork Data Gateway は次の検証を行います。

1. デバイスに対して収集ジョブが作成されているかどうかを確認します。
2. トラップバージョンとコミュニティ文字列を確認します。
3. SNMP v3 の場合は、ユーザー認証と priv プロトコルとログイン情報を検証します。

Cisco Crosswork Data Gateway は、センサーパスに示されたトラップ OID に基づいてトラップをフィルタ処理し、要求されたトラップのみを送信します。

Cisco Crosswork Data Gateway は、次の YANG パスをサポートしています。

センサーパス	目的
snmp-trap-raw-oper:traps/data	フィルタなしでデバイスからプッシュされたすべてのトラップを取得します。
IF-MIB:notifications	すべての IF-MIB 通知（例：linkUp、linkDown など）を取得します。
ISIS-MIB:notifications	すべての ISIS-MIB 通知を取得します。
SNMPv2-MIB:notifications	すべての SNMPv2 MIB 通知を取得します。

次に、SNMP トラップ収集ジョブの例を示します。

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "TRAP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "a9b8f43d-130b-4866-a26a-4d0f9e07562a",
            "8c4431a0-f21d-452d-95a8-84323a19e0d6",
            "eaab2647-2351-40ae-bf94-6e4a3d79af3a"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_696600ae-80ee-4a02-96cb-3a01a2415324"
        }
      }
    ]
  }
}
```

```

    ]
  }
}

```

外部アプリケーションへのトラップ転送の有効化

現在の実装では、SNMPトラップ収集ジョブの場合、SNMPトラップOIDがセンサーパスに指定されていなくても、すべてのトラップが指定されたデータ宛先に送信されます。



(注) Crosswork で必要なトラップのみをデバイスで選択的に有効にすることもお勧めします。

接続先で受信したデータのトラップタイプを識別するには、*oid* (OBJECT_IDENTIFIER。1.3.6.1.6.3.1.1.4.1.0 など) と *OidRecords* の *oid* に関連付けられている *strValue* を検索します (アプリケーションは対象の OID を照合してトラップの種類を特定できます)。

以下は、いくつかのサンプル値とサンプルペイロードです。

- リンク アップ

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4
```

- Link Down

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3
```

- Syslog

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1
```

- Cold Start

```
1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1
```

```

{
  "nodeIdStr": "BF5-XRV9K1.tr3.es",
  "nodeIdUuid": "C9tZ51JoSJKf5OZ67+U5JQ==",
  "collectionId": "133",
  "collectionStartTime": "1580931985267",
  "msgTimestamp": "1580931985267",
  "dataGpbkv": [
    {
      "timestamp": "1580931985267",
      "name": "trapsensor.path",
      "snmpTrap": {
        "version": "V2c",
        "pduType": "TRAP",
        "v2v3Data": {
          "agentAddress": "172.70.39.227",
          "oidRecords": [
            {
              "oid": "1.3.6.1.2.1.1.3.0",
              "strValue": "7 days, 2:15:17.02"
            },
            {
              "oid": "1.3.6.1.6.3.1.1.4.1.0", // This oid is the Object Identifier.
              "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
            kind of trap.
          }
        }
      }
    }
  ]
}

```

```

    {
      "oid": "1.3.6.1.2.1.2.2.1.1.8",
      "strValue": "8"
    },
    {
      "oid": "1.3.6.1.2.1.2.2.1.2.8",
      "strValue": "GigabitEthernet0/0/0/2"
    },
    {
      "oid": "1.3.6.1.2.1.2.2.1.3.8",
      "strValue": "6"
    },
    {
      "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
      "strValue": "down"
    }
  ]
}
}
],
"collectionEndTime": "1580931985267",
"collectorUuid": "YmNjZjEzMTktZjFlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVE9S",

"status": {
  "status": "SUCCESS"
},
"modelData": {},
"sensorData": {
  "trapSensor": {
    "path": "1.3.6.1.6.3.1.1.5.4"
  }
},
"applicationContexts": [
  {
    "applicationId": "APP1",
    "contextId": "collection-job-snmp-traps"
  }
]
}

```

MDT 収集ジョブ

Crosswork Data Gateway は、モデル駆動型テレメトリ（MDT）を使用してネットワークデバイスからのデータ収集をサポートし、デバイスからのテレメトリストリームを直接消費します（IOS-XR ベースのプラットフォームのみ）。



- (注)
- MDT コレクタは、デバイスのテレメトリプロトコルの一部として提供されるコレクション ID を保持します。この動作は、コレクションのシーケンス番号に基づいてコレクション ID を計算する CLI および SNMP コレクタとは異なります。
 - MDT 収集ジョブでは、デバイス上でいくつかの設定を行う必要があります。この設定は、NSO によって自動的に処理されます。NSO が統合され、適切に機能していることを確認する
 - バックアップ操作と復元操作の間に既存の MDT ジョブに変更（削除/更新）がある場合、Cisco Crosswork ではプロバイダー（NSO）が関与するため、デバイスで設定更新のジョブは再生されません。プロバイダー/デバイスの設定を復元する必要があります。Cisco Crosswork はデータベース内のジョブを復元するだけです。
 - YANG モジュールを使用する前に、サポートされているかどうかを確認します。「[MDT での収集用に事前にロードした YANG モジュールのリスト（49 ページ）](#)」の項を参照してください。

次のトランスポートモードのデータ収集をサポートします。

- MDT TCP ダイアルアウトモード

次に、MDT 収集のペイロードの例を示します。

```
{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "device_group": "mdt"
      }
    },
    "sensor_output_configs": [{
      "sensor_data": {
        "mdt_sensor": {
          "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"

        }
      },
      "destination": {
        "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
        "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
      }
    },
    {
      "sensor_data": {
        "mdt_sensor": {
          "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"

        }
      },
      "destination": {
        "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
        "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
      }
    }
  ]
}
```

```

    ],
    "sensor_input_configs": [{
      "sensor_data": {
        "mdt_sensor": {
          "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"
        }
      },
      "cadence_in_millisec": "70000"
    }, {
      "sensor_data": {
        "mdt_sensor": {
          "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
        }
      },
      "cadence_in_millisec": "70000"
    }
  ],
  "application_context": {
    "context_id": "c4",
    "application_id": "a4-mdt"
  },
  "collection_mode": {
    "lifetime_type": "APPLICATION_MANAGED",
    "collector_type": "MDT_COLLECTOR"
  }
}

```

gNMI 収集ジョブ

Cisco Crosswork は、Cisco Crosswork Data Gateway を介した gRPC ネットワーク管理インターフェイス (gNMI) ベースのテレメトリデータの収集をサポートしています。サブスクリプションに基づく gNMI ダイアライン (gRPC ダイアライン) ストリーミングのテレメトリデータと、要求した宛先への後続のサブスクリプション応答 (通知) のリレーのみをサポートします。



- (注) モデルがターゲットのデバイスプラットフォームでサポートされている限り、gNMI 収集はサポートされます。gNMI 収集ジョブを送信するには、デバイスで gNMI を設定しておく必要があります。プラットフォーム固有のマニュアルを確認します。

デバイスの設定例については、「[デバイスの設定例 : gNMI \(16 ページ\)](#)」を参照してください。

gNMI では、セキュアモードと非セキュアモードの両方をデバイスで共存させることができます。Cisco Crosswork は、インベントリで渡された情報に基づいて、非セキュアモードよりもセキュアモードを優先します。

デバイスがリロードされると、gNMI コレクタは既存のサブスクリプションがデバイスに再サブスクライブされるようにします。

gNMI 仕様には、メッセージの終わりをマークする方法がありません。したがって、宛先またはディスパッチのパターンは gNMI コレクタではサポートされません。

Cisco Crosswork Data Gateway は、すべてのタイプのストリームベースのサブスクリプションをサポートしています。

- サンプル：パターンベースの収集。
- ON_CHANGE：最初の応答には、サブスクライブしているパスのすべての要素の状態が含まれ、その後に、変更リーフ値に対する後続の更新が含まれています。
- TARGET_DEFINED：ルータ/デバイスは、サブスクライブしているパス（つまり、SAMPLE または ON_CHANGE のいずれか）に基づいてリーフ単位でサブスクリプションのモードを選択します。



- (注)
- Cisco Crosswork Data Gateway は、1 つ以上のモードのサポートの宣言をデバイスに依存します。
 - デフォルト値の gNMI センサーパスはペイロードを表示しません。これは既知の protobuf の動作です。
- ブール値の場合、デフォルト値は false になります。enum の場合は、gnmi.proto が指定されます。

例 1：

```
message GNMIDeviceSetting {
  bool suppress_redundant = 1;
  bool allow_aggregation = 4;
  bool updates_only = 6;
}
```

例 2：

```
enum SubscriptionMode {
  TARGET_DEFINED = 0; //default value will not be printed
  ON_CHANGE = 1;
  SAMPLE = 2;
}
```

次に、gNMI 収集ペイロードのサンプルを示します。

```
{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "device_group": "gnmi"
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "gnmi_sensor": {
            "path": {
              "origin": "",
              "elem": [
                {
                  "name": "interfaces"
                }
              ]
            }
          }
        }
      }
    ]
  }
}
```

```

        {
            "name": "interface",
            "key": {
                "name": "GigabitEthernet0/0/0/4"
            }
        }
    ]
},
"mode": "SAMPLE"
}
},
"cadence_in_millisecc": "30000"
}
],
"sensor_output_configs": [
    {
        "sensor_data": {
            "gnmi_sensor": {
                "path": {
                    "origin": "",
                    "elem": [
                        {
                            "name": "interfaces"
                        },
                        {
                            "name": "interface",
                            "key": {
                                "name": "GigabitEthernet0/0/0/4"
                            }
                        }
                    ]
                },
                "mode": "SAMPLE"
            }
        },
        "destination": {
            "context_id": "topic_gnmi",
            "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
    }
],
"application_context": {
    "context_id": "gnmi_test_context",
    "application_id": "gnmi"
},
"collection_mode": {
    "lifetime_type": "APPLICATION_MANAGED",
    "collector_type": "GNMI_COLLECTOR"
}
}
}

```

デバイスの設定例 : gNMI

Cisco IOS XR デバイス

1. HTTP/2 接続で gRPC を有効にします。

```

Router#configure
Router(config)#grpc
Router(config-grpc)#port <port-number>

```


ポート番号の範囲は 57344 ~ 57999 です。ポート番号が使用できない場合は、エラーが表示されます。

2. セッションパラメータを設定します。

```
Router(config)#grpc{ address-family | dscp | max-request-per-user | max-request-total
| max-streams |
max-streams-per-user | no-tls | service-layer | tls-cipher | tls-mutual |
tls-trustpoint | vrf }
```

値は次のとおりです。

- `address-family`: アドレスファミリ識別子タイプを設定します
- `dscp`: 送信された gRPC で QoS マーキング DSCP を設定します
- `max-request-per-user`: ユーザーあたりの同時要求の最大数を設定します
- `max-request-total`: 合計同時要求の最大数を設定します
- `max-streams`: 同時 gRPC 要求の最大数を設定します。サブスクリプションの上限は 128 要求です。デフォルトは 32 要求です
- `max-streams-per-user`: ユーザーあたりの同時 gRPC 要求の最大数を設定します。サブスクリプションの上限は 128 要求です。デフォルトは 32 要求です
- `no-tls`: トランスポートレイヤセキュリティ (TLS) を無効化します。TLS はデフォルトで有効になっています。
- `service-layer`: gRPC サービスレイヤの設定を有効にします
- `tls-cipher`: gRPC TLS 暗号スイートを有効にします
- `tls-mutual`: 相互認証を設定します
- `tls-trustpoint`: トラストポイントを設定します
- `vrf`: サーバー VRF を有効にします

3. TPA (サードパーティ製アプリケーションのトラフィック保護) を有効にします。

```
tpa
vrf default
address-family ipv4
default-route mgmt
update-source dataports MgmtEth0/RP0/CPU0/0
```

Cisco IOS XE デバイス

次に、gNMI サーバを非セキュアモードで有効にする例を示します。

```
Device# configure terminal
Device(config)# gnmi-yang
Device(config)# gnmi-yang server
Device(config)# gnmi-yang port 50000 <The default port is 50052.>
Device(config)# end
Device
```

次に、gNMI サーバをセキュアモードで有効にする例を示します。

証明書とトラストポイントは、セキュア gNMI サーバにのみ必要です。

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port 50001 <The default port is 50051.>
Device(config)# end
Device
```

デバイスの証明書

証明書とトラストポイントは、セキュア gNMI サーバにのみ必要です。

Linux での OpenSSL を使用した証明書の作成

次に、Linux マシン上で OpenSSL を使用して証明書を作成する例を示します。

```
# Setting up a CA
openssl genrsa -out rootCA.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=rootCA -x509 -new -nodes -key rootCA.key -sha256 -out
  rootCA.pem

# Setting up device cert and key
openssl genrsa -out device.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=<hostnameFQDN> -new -key device.key -out device.csr
openssl x509 -req -in device.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
  device.crt -sha256
# Encrypt device key - needed for input to IOS
openssl rsa -des3 -in device.key -out device.des3.key -passout pass:<password - remember
  this for later>

# Setting up client cert and key
openssl genrsa -out client.key 2048
openssl req -subj /C=/ST=/L=/O=/CN=gnmi_client -new -key client.key -out client.csr
openssl x509 -req -in client.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
  client.crt -sha256
```

Cisco IOS XR デバイスへの証明書のインストール

Cisco IOS XR に証明書をインストールするには、次のパスのファイルを置き換えます。

1. XR マシンにログインします。
2. 端末プロンプトで `run` コマンドを入力します。


```
RP/0/RP0/CPU0:xrvr-7.2.1#run
```
3. 次のディレクトリに移動します。


```
cd /misc/config/grpc
```
4. 次のファイルの内容を置き換えます。
 - `ems.pem` の内容を `device.crt` に置き換えます。
 - `ems.key` の内容を `device.key` に置き換えます。
 - `ca.cert` の内容を `rootCA.pem` に置き換えます。

Cisco IOS XE デバイスへの証明書のインストール

次に、Cisco IOS XE デバイスに証明書をインストールする例を示します。

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#
```

デバイスと Crosswork Data Gateway 間でのセキュア gNMI 通信の有効化

セキュアな gNMI 設定ワークフロー：

1. トラストチェーンを Cisco Crosswork の Crosswork Crosswork 証明書管理 UI にアップロードします。「[gNMI 証明書の設定 \(20 ページ\)](#)」を参照してください。
2. Cisco Crosswork の UI からセキュア gNMI ポートの詳細を使用してデバイス設定を更新します。[Cisco Crosswork の UI からのデバイス設定 \(22 ページ\)](#) を参照してください

gNMI 証明書の設定

Crosswork Data Gateway は gNMI クライアントとして機能し、デバイスは gNMI サーバーとして機能します。Crosswork Data Gateway は、信頼チェーンを使用してデバイスを検証します。すべてのデバイスにグローバルな信頼チェーンがあることが期待されます。信頼チェーンが複数ある場合は、すべてのデバイス信頼チェーン（単一または複数のベンダー）を 1 つの .pem ファイルに追加し、この .pem ファイルを Crosswork 証明書管理の UI にアップロードします。デバイスにトラストポイントを設定するためのサンプルデバイス設定については、「[デバイスの設定例 : gNMI \(16 ページ\)](#)」を参照してください。



(注) Crosswork にアップロードできる gNMI 証明書は 1 つのみです。

gNMI 証明書を設定するには、次の手順を実行します。

ステップ 1 Cisco Crosswork の UI から、[管理 (Administration)] > [証明書管理 (Certificate Management)] に移動します。

ステップ 2 [+] アイコンをクリックして証明書を追加します。

ステップ 3 [証明書の追加 (Add Certificate)] ウィンドウで、次の詳細情報を入力します。

- [デバイス証明書名 (Device Certificate Name)] : 証明書の名前を入力します。
- [証明書のロール (Certificate Role)] : [デバイスgNMI通信 (Device gNMI Communication)] を選択します。
- [デバイス信頼チェーン (Device Trust Chain)] : ローカルファイルシステムを参照して .pem ファイルの場所を探し、ファイルを選択します。

🏠 / Administration / Certificate Management / Add Certificate

Add Certificate

Certificate Name *

Certificate Role *

Device Trust Chain *

Save

Cancel

- (注) gNMI 証明書がすでに設定されている場合で、別の信頼チェーンを使用してデバイスをオンボーディングするときは、既存の .pem ファイルを更新して新しい CA の詳細を含めます。リストから既存の gNMI 証明書を選択し、[編集 (Edit)] アイコンをクリックして、新しい .pem ファイルをアップロードします。

ステップ 4 [保存 (Save)] をクリックします。

gNMI 証明書が正常に追加されると、設定済みの証明書のリストに表示されます。

Crosswork Network Automation

Administration / Certificate Management

Certificates

+ ✎

	Name		Expiration Date
<input type="checkbox"/>	Device-gNMI-Certs		Fri, Jan 7, 2022, 3:31:...
<input type="checkbox"/>	Crosswork-Internal-Communic...		Sun, Jan 22, 2023, 7:..
<input type="checkbox"/>	Crosswork-ZTP-Device-SUDI		Mon, May 14, 2029, 1.
<input type="checkbox"/>	Crosswork-ZTP-Owner		Sun, Jan 22, 2023, 7:..

Cisco Crosswork の UI からのデバイス設定

Crosswork UI で gNMI 証明書を設定したら、安全なプロトコルの詳細でデバイスを更新します。

1. Cisco Crosswork UI から、[デバイス管理 (Device Management)] > [ネットワークデバイス (Network Devices)] に移動します。
2. デバイスを選択し、[編集 (Edit)] をクリックして、[プロトコル (Protocol)] フィールドの詳細を次のように更新します。

安全な通信のための [プロトコル (Protocol)] : **GNMI_SECURE** ポート。

Edit Device Details
×

▼ General

Configured State* <input type="text" value="DOWN"/>	UUID <input type="text" value="3166bf90-bbbd-4d19-933e-817caacfa"/>
Reachability Check* <input type="text" value="ENABLE"/>	Serial Number <input type="text"/>
Credential Profile* <input type="text" value="xrvr"/>	Mac Address <input type="text"/>
Host Name <input type="text" value="xrvr2"/>	Capability* <input type="text" value="SNMP, YANG_CLI"/>
Inventory ID <input type="text"/>	Tags <input type="text"/>
Data Gateway <input type="text" value="None"/>	Product Type <input type="text" value="CISCO-XRv9000"/>
Software Type <input type="text" value="IOS XR"/>	Syslog Format <input type="text" value="UNKNOWN"/>
Software Version <input type="text" value="6.6.2"/>	

▼ Connectivity Details

Protocol *	IP Address / Subnet Mask *	Port *	Timeout	Encoding Type *	
<input type="text" value="SSH"/>	<input type="text" value="10.11.0.11"/> / <input type="text" value="16"/>	<input type="text" value="22"/>	<input type="text" value="30"/>	<input type="text"/>	<input type="text" value="🗑"/>
<input type="text" value="SNMP"/>	<input type="text" value="10.11.0.11"/> / <input type="text" value="16"/>	<input type="text" value="161"/>	<input type="text" value="30"/>	<input type="text"/>	<input type="text" value="🗑"/>
<input type="text" value="GNMI_SECURE"/>	<input type="text" value="10.11.0.11"/> / <input type="text" value="16"/>	<input type="text" value="57400"/>	<input type="text" value="1500"/>	<input type="text" value="PROTO"/>	<input type="text" value="🗑"/>

[+ Add Another](#)

> Routing Info

Syslog 収集ジョブ

Cisco Crosswork Data Gateway は、デバイスからの Syslog ベースのイベント収集をサポートしています。サポートされている Syslog 形式は次のとおりです。

- RFC5424 syslog 形式
- RFC3164 syslog 形式



(注) Syslog 収集ジョブを送信する前に、デバイスで Syslog を設定する必要があります。プラットフォーム固有のドキュメントを参照してください。

デバイスの設定例については、「[RFC3164/RFC5424 形式の Syslog の設定 \(24 ページ\)](#)」を参照してください。

以下は、Syslog 収集ペイロードの例です。

```

{
  "collection_job": {
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c6f25a33-92e6-468a-ba0d-15490f1ce787"
          ]
        }
      }
    }
  }
}

```

```

    }
  },
  "sensor_output_configs": [
    {
      "sensor_data": {
        "syslog_sensor": {
          "pris": {
            "facilities": [0, 1, 3, 23,4],
            "severities": [0, 4, 5, 6, 7]
          }
        }
      },
      "destination": {
        "context_id": "syslogtopic",
        "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
      }
    }
  ],
  "sensor_input_configs": [
    {
      "sensor_data": {
        "syslog_sensor": {
          "pris": {
            "facilities": [0,1, 3, 23,4],
            "severities": [0,4, 5, 6, 7]
          }
        }
      },
      "cadence_in_millisecc": "60000"
    }
  ],
  "application_context": {
    "context_id": "demomillesstone2syslog",
    "application_id": "SyslogDemo2"
  },
  "collection_mode": {
    "lifetime_type": "APPLICATION_MANAGED",
    "collector_type": "SYSLOG_COLLECTOR"
  }
}
}
}

```

ペイロードに記載されている機能と重大度に基づいて、一致する Syslog イベントが指定された宛先に送信されます。一致しない他のすべての syslog イベントはドロップされます。

RFC3164/RFC5424 形式の Syslog の設定

この項では、デバイスで RFC3164 形式または RFC5424 形式の syslog を設定するための設定例を示します。同じ設定を、デバイスの非セキュア Syslog 設定に使用することもできます。

RFC3164 Syslog 形式の設定



(注) 次のコードで強調表示されている設定は、解析された出力でのフォーマットの問題を回避するために必要です。

Cisco IOS XR デバイスの場合：


```
logging <server 1> port 9514 OR logging <server 1> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
```

```
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
```

Cisco IOS XE デバイスの場合：

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host 172.29.194.174 transport tcp port 9898 session-id string <sessionidstring>
--> To use TCP channel
OR
logging host 172.29.194.174 transport udp port 9514 session-id string <sessionidstring>
--> To use UDP channel
OR
logging host <cdg ip> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
```

RFC5424 Syslog 形式の設定

Cisco IOS XR デバイスの場合：

```
logging <server 1> port 9514 OR logging <server 1> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
logging format rfc5424
```

Cisco IOS XE デバイスの場合：

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host 172.29.194.174 transport tcp port 9898 session-id string <sessionidstring>
--> To use TCP channel
OR
logging host 172.29.194.174 transport udp port 9514 session-id string <sessionidstring>
--> To use UDP channel
OR
logging host <cdg ip> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```

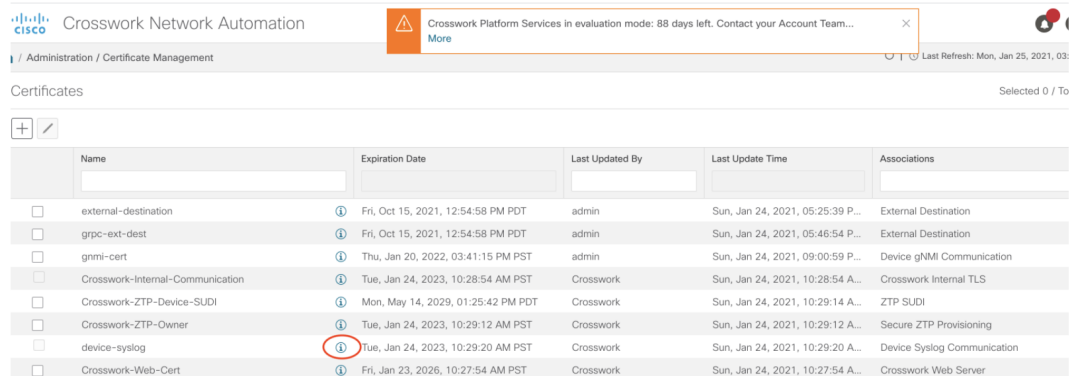
デバイスでのセキュア Syslog の設定

デバイスへのセキュアな syslog 通信を確立するには、次の手順を実行します。

1. Crosswork の [証明書管理UI (Certificate Management UI)] ページから Cisco Crosswork 信頼チェーンをダウンロードします。
2. syslog 設定用の Crosswork トラストチェーンを使用してデバイスを設定します。

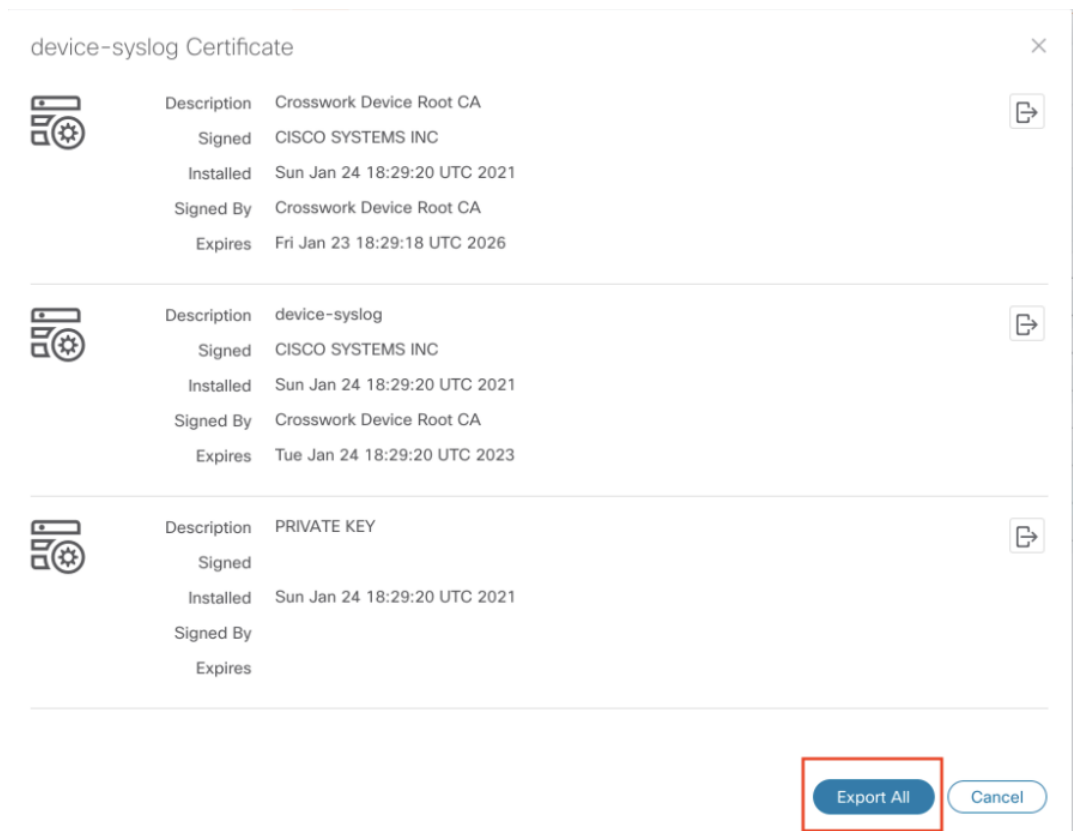
Syslog 証明書のダウンロード

1. Cisco Crosswork の UI で、[管理 (Administration)] > [証明書管理 (Certificate Management)] に移動します。
2. 下の画像に示すように、「device-syslog」行で i をクリックします。





	Name	Expiration Date	Last Updated By	Last Update Time	Associations
<input type="checkbox"/>	external-destination	i Fri, Oct 15, 2021, 12:54:58 PM PDT	admin	Sun, Jan 24, 2021, 05:25:39 P...	External Destination
<input type="checkbox"/>	grpc-ext-dest	i Fri, Oct 15, 2021, 12:54:58 PM PDT	admin	Sun, Jan 24, 2021, 05:46:54 P...	External Destination
<input type="checkbox"/>	gnmi-cert	i Thu, Jan 20, 2022, 03:41:15 PM PST	admin	Sun, Jan 24, 2021, 09:00:59 P...	Device gNMI Communication
<input type="checkbox"/>	Crosswork-Internal-Communication	i Tue, Jan 24, 2023, 10:28:54 AM PST	Crosswork	Sun, Jan 24, 2021, 10:28:54 A...	Crosswork Internal TLS
<input type="checkbox"/>	Crosswork-ZTP-Device-SUDI	i Mon, May 14, 2029, 01:25:42 PM PDT	Crosswork	Sun, Jan 24, 2021, 10:29:14 A...	ZTP SUDI
<input type="checkbox"/>	Crosswork-ZTP-Owner	i Tue, Jan 24, 2023, 10:29:12 AM PST	Crosswork	Sun, Jan 24, 2021, 10:29:12 A...	Secure ZTP Provisioning
<input type="checkbox"/>	device-syslog	i Tue, Jan 24, 2023, 10:29:20 AM PST	Crosswork	Sun, Jan 24, 2021, 10:29:20 A...	Device Syslog Communication
<input type="checkbox"/>	Crosswork-Web-Cert	i Fri, Jan 23, 2026, 10:27:54 AM PST	Crosswork	Sun, Jan 24, 2021, 10:27:54 A...	Crosswork Web Server


3. [すべてエクスポート (Export All)] をクリックして、証明書をダウンロードします。



device-syslog Certificate




 Description Crosswork Device Root CA
Signed CISCO SYSTEMS INC
Installed Sun Jan 24 18:29:20 UTC 2021
Signed By Crosswork Device Root CA
Expires Fri Jan 23 18:29:18 UTC 2026

 Description device-syslog
Signed CISCO SYSTEMS INC
Installed Sun Jan 24 18:29:20 UTC 2021
Signed By Crosswork Device Root CA
Expires Tue Jan 24 18:29:20 UTC 2023

 Description PRIVATE KEY
Signed
Installed Sun Jan 24 18:29:20 UTC 2021
Signed By
Expires

Export All Cancel

次のファイルがシステムにダウンロードされます。

Name
 intermediate.key
 intermediate.crt
 ca.crt

デバイスの Syslog 設定

TLS を有効にする XR デバイスの設定例

```
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-root
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k(config-trustp)#end
RP/0/RSP0/CPU0:ASR9k#
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-root
Fri Jan 22 11:07:41.880 GMT
```

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIGKzCCBBOgAwIBAgIRAKfyU89yjmrXVDRKBWuSGPgWdQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.....
jPQ/UrO8N3sC1gGJX7CIh5cE+KIJ51ep8ileKSJ5whWRTmv342MnG2StgOTtaFF
vrkWHd02o6jRuYXDWEUptDOg8oEritZb+SNPXWUC/2mbYog6ks6EeMC69VjkZPo=
-----END CERTIFICATE-----
```

```
Read 1583 bytes as CA certificate
Serial Number : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
Subject:
          CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By :
          CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:09 UTC Sat Jan 16 2021
Validity End : 02:37:09 UTC Thu Jan 15 2026
SHA1 Fingerprint:
          209B3815271C22ADF78CB906F6A32DD9D97BBDBA
```

Fingerprint: 2FF85849EBAAB9B059ACB9F5363D5C9CDo you accept this certificate? [yes/no]:
yes

```
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-inter
Fri Jan 22 11:10:30.090 GMT
```

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIRAKhqHQXcJzQzeQK6U2wn8PIwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAGTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.....
```

```

.....
5lBk617z6cxFER5c+/PmJFhcreisTxXglaJbFdnB5C8f+0uUIdLghykQ/zaZGuBn
AAB70c9r9OeKJWzvvle2U8HH1pdQ/nd
-----END CERTIFICATE-----

Read 1560 bytes as CA certificate
Serial Number : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
Subject:
CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By :
CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:11 UTC Sat Jan 16 2021
Validity End : 02:37:11 UTC Mon Jan 16 2023
SHA1 Fingerprint:
B06F2BFDE95413A8D08A01EE3511BC3D42F01E59

CA Certificate validated using issuer certificate.
RP/0/RSP0/CPU0:ASR9k#show crypto ca certificates
Fri Jan 22 15:45:17.196 GMT

Trustpoint : syslog-root
=====
CA certificate
Serial Number : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
Subject:
CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By :
CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:09 UTC Sat Jan 16 2021
Validity End : 02:37:09 UTC Thu Jan 15 2026
SHA1 Fingerprint:
209B3815271C22ADF78CB906F6A32DD9D97BBDBA

Trustpoint : syslog-inter
=====
CA certificate
Serial Number : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
Subject:
CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Issued By :
CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
Validity Start : 02:37:11 UTC Sat Jan 16 2021
Validity End : 02:37:11 UTC Mon Jan 16 2023
SHA1 Fingerprint:
B06F2BFDE95413A8D08A01EE3511BC3D42F01E59
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname 10.13.0.159
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#severity debugging
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#vrf default
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#commit
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#exit
RP/0/RSP0/CPU0:ASR9k(config)#exit
RP/0/RSP0/CPU0:ASR9k#exit
RP/0/RSP0/CPU0:ASR9k#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG Southbound IP>
!
```

```
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates
```

RP/0/RSP0/CPU0:ASR9k#

TLS を有効にする XE デバイスの設定例

```
csr8kv(config)#crypto pki trustpoint syslog-root
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation stop
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-root
```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIFPjCCAYYCCQCO6pK5AOGYdjANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBACMCElpbHBpdGFzMQ4wDAYDVQQKDAVdXNj
.....
JbimOpXAncoBLo14DXOJLVMVRjn1EULE9AXXCnfnrnBx7jL4CV+qHgEtF6oqclFW
JEA=
-----END CERTIFICATE-----
```

```
Certificate has the following attributes:
  Fingerprint MD5: D88D6D8F E53750D4 B36EB498 0A435DA1
  Fingerprint SHA1: 649DE822 1C222C1F 5101BEB8 B29CDF12 5CEE463B
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

```
csr8kv(config)#crypto pki trustpoint syslog-intermediate
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation continue syslog-root
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-intermediate
```

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIFfTCCA2WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMakGA1UEBhMCMVVMx
EzARBgNVBAGMCKNhG1mb3JuaWEwDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQKDAVd
.....
Nmz6NQynd7bxdQa9Xq9kyPuY3ZVKXkf312IRH0MEy2yFX/tAen9JqOeZ1g8canmw
TxswA5TLzylRmxqQh88f0CM=
-----END CERTIFICATE-----
```

```
Trustpoint 'syslog-intermediate' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
  Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
  Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19
```

```
csr8kv(config)#logging host <CDG Southbound IP> transport tls port 6514
csr8kv(config)#logging trap informational syslog-format rfc5424
```

```
csr8kv(config)#logging facility user
csr8kv(config)#service timestamps log datetime msec year show-timezone

csr8kv(config)#logging tls-profile tlsv12
```

Syslog 収集ジョブの出力

Cisco Crosswork の UI からデバイスを追加する場合 ([デバイス管理 (Device Management)] > [ネットワークデバイス (Network Devices)] > [デバイスの詳細 (Device Details)])、[Syslog 形式 (Syslog Format)] フィールドで選択した値によって、デバイスから受信した syslog イベントを Syslog コレクタで解析する形式が設定されます。[不明 (UNKNOWN)]、[RFC5424]、または [RFC3164] のいずれかを選択できます。

次に、各オプションの出力例を示します。

1. 不明 : Syslog 収集ジョブの出力に、デバイスから受信した syslog イベントが含まれていません。



(注) デバイスは RFC5424/RFC3164 形式で syslog イベントを生成するように設定されていても [Syslog 形式 (Syslog Format)] フィールドに形式が指定されていない場合、デフォルトでは [不明 (UNKNOWN)] と見なされます。

サンプル出力 :

```
node_id_str: "xrv9k-VM8"
node_id_uuid: ".i\300\216>\366BM\262\270@\337\225\2723&"
collection_id: 1056
collection_start_time: 1616711596200
msg_timestamp: 1616711596201
data_gpbkv {
  timestamp: 1616711596201
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<6>1 Mar 25 15:34:41.321 PDT - SSHD_69570 - - 98949:
RP/0/RP0/CPU0:SSHD_[69570]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated
user \'admin\' from \'40.40.40.116\' on \'vty0\'(cipher \'aes128-ctr\', mac
\'hmac-sha1\') \n"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "40.40.40.30"
  }
}
collection_end_time: 1616711596200
collector_uuid: "17328736-b726-4fe3-b922-231a4a30a54f:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
model_data {
}
sensor_data {
  syslog_sensor {
    pris {
      facilities: 0
      facilities: 3
      facilities: 4
    }
  }
}
```

```

        facilities: 23
        severities: 0
        severities: 5
        severities: 6
        severities: 7
    }
}
}
application_contexts {
    application_id: "SyslogApp-xr-8-job1"
    context_id: "xr-8-job1"
}
}
version: "1"

```

2. [RFC5424] : デバイスが syslog イベントを RFC5424 形式で生成するように設定され、[Syslog 形式 (Syslog Format)] フィールドで [RFC5424] 形式が選択されている場合、Syslog 収集ジョブの出力には、デバイスから受信した syslog イベント (未処理) とデバイスからの RFC5424 のベストエフォート解析済みの syslog イベントが含まれます。



(注) syslog コレクタは、次の Java RegEx パターンに従って syslog イベント (ベストエフォート) を解析します。

RFC5424

```

"^(?<pri>\d+)>(?!<version>\d{1,3})\s*(?!<date>([[0-9]{9}T:.Z-]+))\s*(?!<host>\S+)\s*(?!<processname>\S+)\s*<message>.+)$";

```

サンプル出力 :

```

....
....

collection_start_time: 1596307542398
msg_timestamp: 1596307542405
data_gpbkv {
  timestamp: 1596307542405
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<13>1 2020 Aug 1 12:03:32.461 UTC: iosxr254node config 65910 -
- 2782: RP/0/RSP0/CPU0:2020 Aug 1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \n"
  }
  fields {
    name: "RFC5424"
    string_value: "pri=13, severity=5, facility=1, version=1,
date=2020-08-01T12:03:32.461, remoteAddress=/172.28.122.254, host='iosxr254node'",

```

```

message=\'2782: RP/0/RSP0/CPU0:2020 Aug  1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \',
messageId=null, processName=config, structuredDataList=null"
}
fields {
  name: "DEVICE_IP"
  string_value: "172.28.122.254"
}
}
collection_end_time: 1596307542404
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
...
...

```

3. [RFC3164] : デバイスが syslog イベントを RFC3164 形式で生成するように設定され、[Syslog 形式 (Syslog Format)] フィールドで [RFC3164] 形式が選択されている場合、Syslog 収集の出力には、未処理 (デバイスから受信したもの) syslog イベントとデバイスからの RFC3164 のベストエフォート解析済みの syslog イベントの両方が含まれます。



(注) syslog コレクタは、次の Java RegEx パターンに従って syslog イベント (ベストエフォート解析) を解析します。

RFC3164

```

"^((<(?<pri>\d+)>[:]*\s*)?(?<date>(\*[a-zA-Z]{3}\s+\d+\s+
[a-zA-Z]{3}\s+\d+\s+\d+:\d+:\d+.[\*\d{3}\s+]+[[a-zA
<procid>\d+)\|])?)*\s*(?<message>.+)$";

```

サンプル出力 :

```

....
.....
collection_id: 20
collection_start_time: 1596306752737
msg_timestamp: 1596306752743
data_gpbkv {
  timestamp: 1596306752743
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<14>2020 Aug  1 11:50:22.799 UTC: iosxr254node 2756:
RP/0/RSP0/CPU0:2020 Aug  1 11:50:22.799 UTC: config[65910]: %MGBL-CONFIG-6-DB_COMMIT
: Configuration committed by user \'admin\'. Use \'show configuration commit changes
1000000580\' to view the changes. \n"
  }
  fields {
    name: "RFC3164"
  }
}

```



```
    string_value: "pri=14, severity=6, facility=1, version=null,
date=2020-08-01T11:50:22.799, remoteAddress=/172.28.122.254, host='iosxr254node',
message='RP/0/RSP0/CPU0:2020 Aug 1 11:50:22.799 UTC: config[65910]:
%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user \'admin\'. Use \'show
configuration commit changes 1000000580\' to view the changes. \', tag=2756"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "172.28.122.254"
  }
}
collection_end_time: 1596306752742
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
....
....
```

Syslog コレクタが [Syslog形式 (Syslog Format)] フィールドで指定された形式に従って syslog イベントを解析できない場合、Syslog 収集ジョブの出力には、デバイスから受信した syslog イベントが含まれます。

収集ジョブの作成

収集ジョブを作成するには、次の手順を実行します。



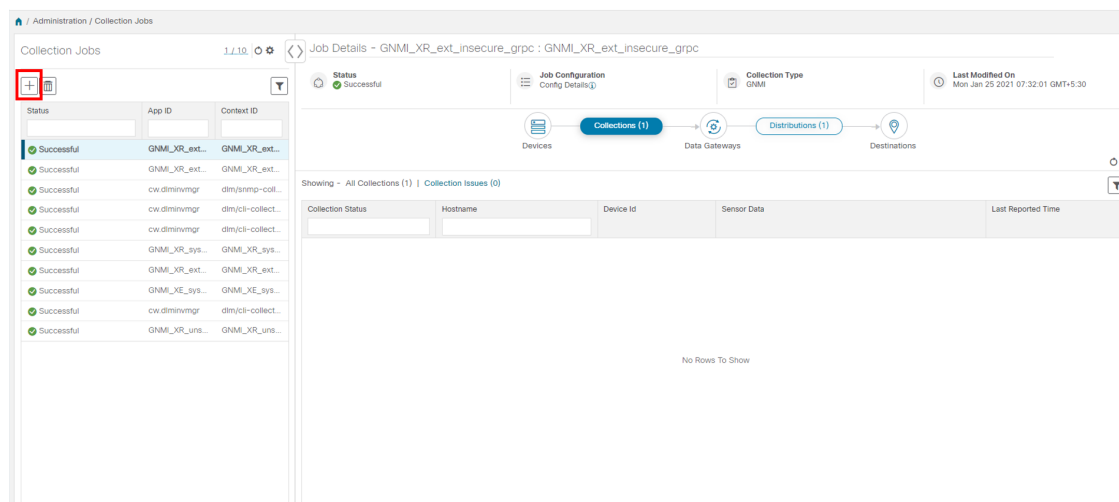
(注) Cisco Crosswork の UI ページを使用して作成した収集ジョブは、1 回のみパブリッシュできません。

始める前に

収集したデータを保存するためのデータ送信先が作成されている (アクティブになっている) ことを確認します。また、データを収集する予定のセンサーパスと MIB の詳細を確認します。

ステップ 1 メインメニューから、[管理 (Administration)] > [収集ジョブ (Collection Jobs)] に移動します。

ステップ 2 左側の [収集ジョブ (Collection Jobs)] ペインで、 ボタンをクリックします。

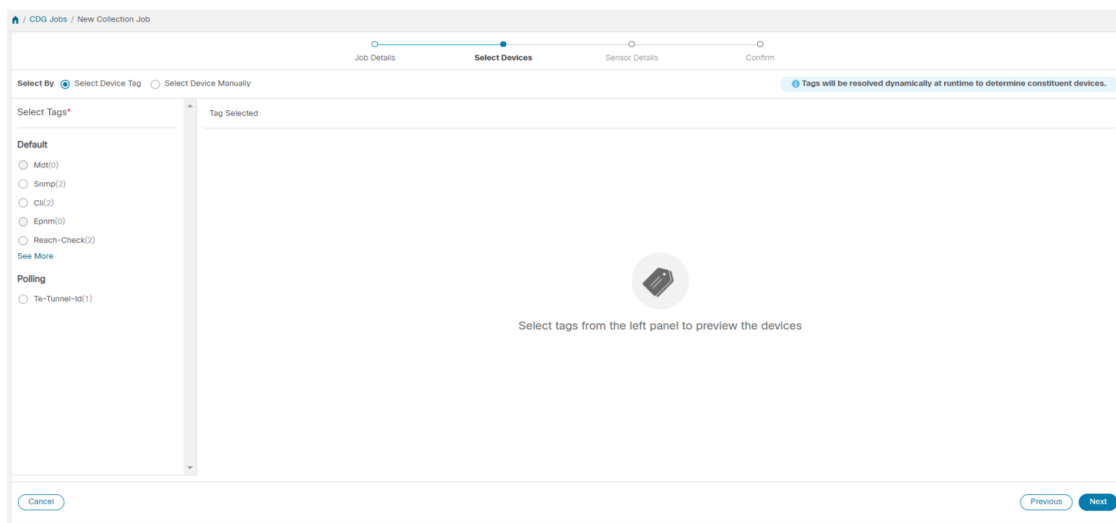


ステップ3 [ジョブの詳細 (Job details)] ページで、次のフィールドに値を入力します。

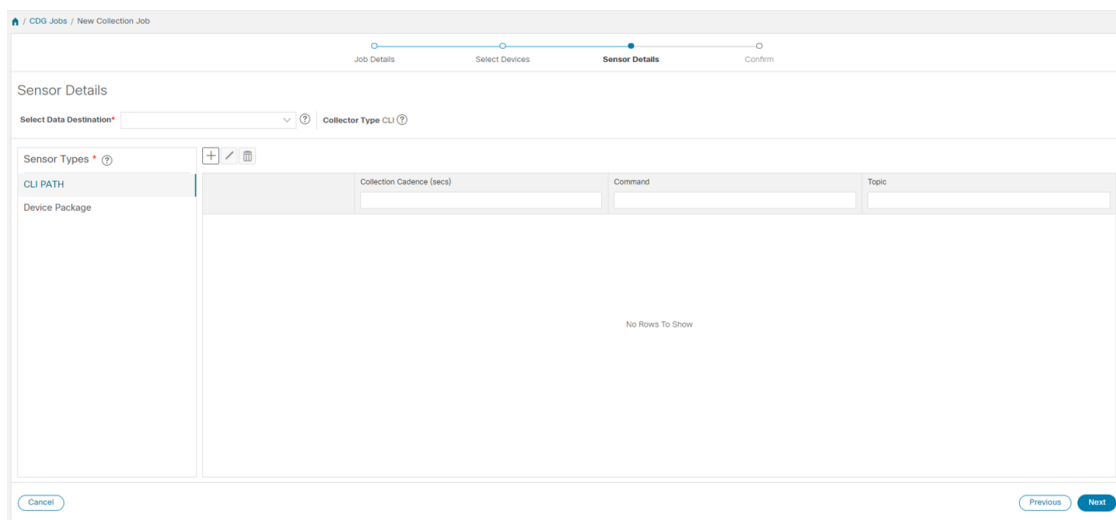
- [アプリケーション ID (Application ID)] : アプリケーションの一意的識別子。
- [コンテキスト (Context)] : すべての収集ジョブでアプリケーションのサブスクリプションを識別するための一意的識別子。
- [コレクタタイプ (Collector Type)] : 収集のタイプ (CLI または SNMP) を選択します。

[次へ (Next)] をクリックします。

ステップ4 データを収集するデバイスを選択します。デバイスタグに基づいて選択することも、手動で選択することもできます。[次へ (Next)] をクリックします。

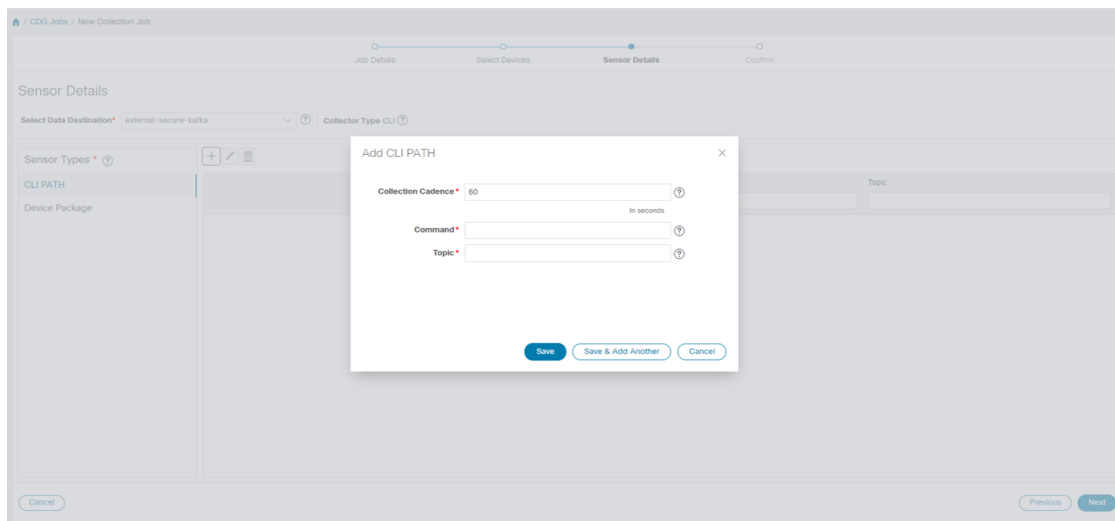


ステップ 5 (CLI での収集の場合にのみ適用) 次のセンサーの詳細を入力します。



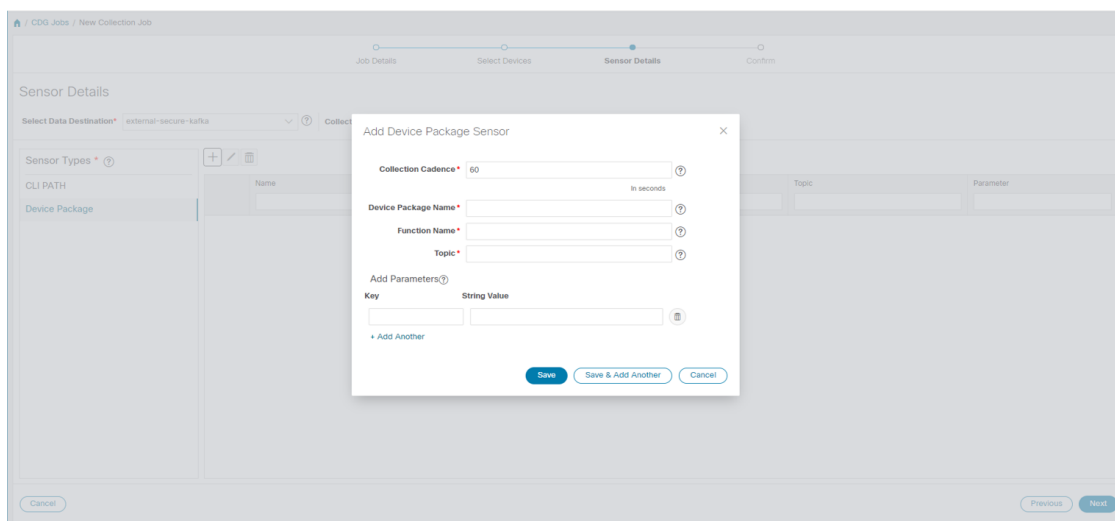
- [データ送信先を選択 (Select Data Destination)] ドロップダウンからデータ送信先を選択します。
- 左側の [センサータイプ (Sensor Types)] ペインからセンサータイプを選択します。

[CLI パス (CLI PATH)] を選択した場合は、**+** ボタンをクリックして、[CLI パスの追加 (Add CLI Path)] ダイアログボックスに次のパラメータを入力します。



- [収集パターン (Collection Cadence)] : プッシュまたはポーリングパターンを秒単位で指定します。
- [コマンド (Command)] : CLI コマンド
- [トピック (Topic)] : 出力先に関連付けられているトピック。

[デバイスパッケージ (Device Package)] を選択した場合は、**+** ボタンをクリックし、[デバイスパッケージセンサーの追加 (Add Device Package Sensor)] ダイアログボックスに次のパラメータの値を入力します。



- [収集パターン (Collection Cadence)] : プッシュまたはポーリングパターンを秒単位で指定します。
- [デバイスパッケージ名 (Device Package Name)] : デバイスパッケージの作成時に使用するカスタム XDE デバイスパッケージの ID。
- [関数名 (Function Name)] : カスタム XDE デバイスパッケージ内の関数名。
- [トピック (Topic)] : 出力先に関連付けられているトピック。

パラメータのキーと文字列の値を入力します。

[保存 (Save)] をクリックします。

ステップ 6 (SNMP での収集の場合にのみ適用) 次のセンサーの詳細を入力します。

- [データ送信先の選択 (Select Data Destination)] ドロップダウンからデータ送信先を選択します。
- 左側の [センサータイプ (Sensor Types)] ペインからセンサータイプを選択します。

[SNMP MIB] を選択した場合は、**+** ボタンをクリックして、[SNMP MIB の追加 (Add SNMP MIB)] ダイアログボックスに次のパラメータを入力します。

- [収集パターン (Collection Cadence)] : プッシュまたはポーリングパターンを秒単位で指定します。
- OID
- [操作 (Operation)] : リストから操作を選択します。

- [トピック (Topic)] : 出力先に関連付けられているトピック。

[デバイスパッケージ (Device Package)] を選択した場合は、**+** ボタンをクリックし、[デバイスパッケージセンサーの追加 (Add Device Package Sensor)] ダイアログボックスに次のパラメータの値を入力します。

- [収集パターン (Collection Cadence)] : プッシュまたはポーリングパターンを秒単位で指定します。
- [デバイスパッケージ名 (Device Package Name)] : デバイスパッケージの作成時に使用するカスタムデバイスパッケージの ID。
- [関数名 (Function Name)] : カスタムデバイスパッケージ内の関数名。
- [トピック (Topic)] : 出力先に関連付けられているトピック。

パラメータのキーと文字列の値を入力します。

[保存 (Save)] をクリックします。

ステップ 7 [収集ジョブの作成 (Create Collection Job)] をクリックします。

(注) 外部の Kafka 接続先 (つまり安全でない Kafka) に対して収集ジョブが送信されると、Kafka へのディスパッチジョブは接続に失敗します。コレクタのログに

```
「org.apache.kafka.common.errors.TimeoutException: Topic cli-job-kafka-unsecure not present in metadata after 60000 ms」というエラーが表示されます。Kafka のログには「SSL authentication error "[2021-01-08 22:17:03,049] INFO [SocketServer brokerId=0] Failed authentication with /80.80.80.108 (SSL handshake failed) (org.apache.kafka.common.network.Selector)」というエラーが表示されます。
```

これは、外部の Kafka VM でポートがブロックされているために発生します。次のコマンドを使用して、ポートが Kafka Docker/サーバーポートでリッスンしているかどうかを確認できます。

```
netstat -tulpn
```

この問題を修正するには、Kafka VM を再起動します。

収集ジョブの削除

問題が発生するため、システムと Cisco Crosswork Change Automation and Health Insights 収集ジョブは削除しないでください。[収集ジョブ (Collection Jobs)] ページからは、外部収集ジョブのみを削除できます。

収集ジョブを削除するには、次の手順を実行します。

-
- ステップ 1 [管理 (Administration)] > [収集ジョブ (Collection Jobs)] に移動します。
 - ステップ 2 左側の [収集ジョブ (Collection Jobs)] ペインで、削除する収集ジョブを選択します。
 - ステップ 3 [削除 (Delete)] ボタンをクリックします。
 - ステップ 4 プロンプトが表示されたら、[削除 (Delete)] をクリックします。
-

収集ジョブのモニタリング

[収集ジョブ (Collection Jobs)] ページから、Cisco Crosswork に登録されているすべての Cisco Crosswork Data Gateway インスタンスで現在アクティブな収集ジョブのステータスをモニターできます。

Cisco Crosswork メインメニューから、[管理 (Administration)] > [収集ジョブ (Collection Jobs)] に移動します。

[収集ジョブ (Collection Jobs)] ペインには、すべてのアクティブな収集ジョブのリストが、ステータス、アプリケーション ID、およびコンテキスト ID とともに表示されます。

[ジョブの詳細 (Job Details)] ペインには、[収集ジョブ (Collection Jobs)] ペインで選択された特定のジョブの詳細が表示されます。

ジョブを選択すると、[ジョブの詳細 (Job Details)] ペインに詳細が表示されます。

- 収集ジョブに関連付けられたアプリケーション名とコンテキスト。
- 収集ジョブのステータス。



- (注)
- デバイスが Cisco Crosswork Data Gateway にマッピングされると、関連するすべての収集ジョブのステータスが「不明」に設定されます。次のいずれかの理由により、ジョブのステータスが「不明」になる可能性があります。
 - Cisco Crosswork Data Gateway はまだそのステータスを報告していません。
 - Cisco Crosswork Data Gateway と Crosswork 間の接続が失われた。
 - Cisco Crosswork Data Gateway は収集ジョブを受信したが、実際の収集はまだ保留中になっている。

- 収集ジョブが処理された後、処理が成功した場合はステータスが [成功 (Successful)] に変わり、それ以外の場合は [失敗 (Failed)] に変わります。
- 収集ジョブが低下状態の場合、その原因の 1 つとして、デバイスへの静的ルートが Crosswork Data Gateway から消去されていることが考えられます。
- Health Insights : KPI ジョブは、拡張 Crosswork Data Gateway VM にマッピングされたデバイスでのみ有効にする必要があります。Health Insights : 標準の Crosswork Data Gateway VM にマップされたデバイスで有効になっている KPI ジョブのジョブステータスは低下、収集ステータスは失敗になります。


- REST API 要求で渡す収集ジョブのジョブ設定。ジョブの設定を表示するには、[設定の詳細 (Config Details)] の横にある ⓘ アイコンをクリックします。この場合、Cisco Crosswork では、次の 2 つのモードで設定を表示できます。

- ビュー モード
- テキストモード

- 収集タイプ
- 収集ジョブの最終変更日時。
- [収集 (x) (Collections (x))] : x は、センサーパスによってデバイスにまたがる要求された収集の入力を指します。対応する [(y) 問題 ((y) Issues)] は [不明 (UNKNOWN)] 状態または [失敗 (FAILED)] 状態の入力収集の数です。

- [配布 (x) (Distributions (x))] : x は、センサーパスによってデバイスにまたがる要求された出力収集を指します。対応する [(y) 問題 (y Issues)] は [不明 (UNKNOWN)] 状態または [失敗 (FAILED)] 状態の出力収集の数です。

Cisco Crosswork は、収集と配布に関する次の詳細も表示します。

フィールド	説明
収集/配布ステータス (Collection/Distribution Status)	収集/配布のステータス。変更ベースで Crosswork Data Gateway 報告されます。詳細については、[収集/配信ステータス (Collection/Distribution Status)] の横にある ⓘ をクリックします。
ホスト名 (Hostname)	収集ジョブが関連付けられているデバイスのホスト名。
デバイス ID (Device Id)	データの収集元のデバイスの一意的識別子。
センサーデータ (Sensor Data)	<p>センサーパス</p> <p>収集/配布の概要を表示するには、 ⓘ をクリックします。センサーデータの概要ポップアップから [クリップボードにコピー (Copy to Clipboard)] をクリックしてセンサーデータをコピーできます。</p> <p>収集/配布メトリックの概要を表示するには、  をクリックします。メトリックはパターンベース、つまりデフォルトでは10分ごとに1回報告されます。収集に関する次のメトリックが表示されます。</p> <ul style="list-style-type: none"> • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec <p>収集に関する次のメトリックが表示されます。</p> <ul style="list-style-type: none"> • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count

フィールド	説明
接続先 (Destination)	ジョブのデータ接続先。
最後のステータス変更の報告時刻 (Last Status Change Reported Time)	デバイスセンサーペアの最後のステータス変更が Crosswork Data Gateway から報告された日時。



- (注)
- Create Failed エラーは、N 台のデバイスのうちの一部のデバイスの設定に失敗したことを示します。ただし、収集は正常に設定されたデバイスで行われます。Control Status API を使用して、このエラーの原因となっているデバイスを特定できます。
 - NSO エラーが原因で特定のデバイスでジョブの作成が失敗した場合は、NSO エラーを修正した後、デバイスの管理状態を手動で最初に [ダウン (Down)] にしてから [アップ (Up)] に変更する必要があります。ただし、これを行うと、デバイス上の収集がリセットされます。



- (注)
- [作成/削除失敗 (Create/Delete failed)] エラーが別の画面ポップアップに表示されます。エラーの詳細を表示するには、ジョブステータスの横にある ⓘ をクリックします。
- 同じペイロードで PUT 収集ジョブ API を使用してジョブを再作成することもできます。

SNMP での収集用に事前にロードしたトラップと MIB のリスト

この項では、Cisco Crosswork Data Gateway が SNMP 収集でサポートしているトラップと MIB を示します。



- (注)
- このリストは、Crosswork がターゲットアプリケーションの場合にのみ適用され、ターゲットが外部アプリケーションの場合は制限されません。

次の制約事項に注意してください。

- システムは、概念テーブルの OID からインデックス値を抽出できません。概念テーブルのインデックスを定義する列のいずれかが入力されていない場合、インデックス値はデータプレーンで行のインスタンス識別子 (oid サフィックス) に置き換えられます。

- システムは、**AUGMENT** キーワードを含む概念テーブルからインデックス値を抽出したり、他のテーブルのインデックスを参照したりすることはできません。
- (整数構文を使用した) 名前付き数の列挙は、数値を使用して回線上で送信されます。

表 2: サポートされているトラップ

トラップ	OID
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
coldStart	1.3.6.1.6.3.1.1.5.1
isisAdjacencyChange	1.3.6.1.2.1.138.0.17

ADSL-LINE-MIB.mib	CISCO-LWAPP- INTERFACE-MIB.mib	IANA-ITU-ALARM- TC-MIB.mib
ADSL-TC-MIB.mib	CISCO-LWAPP- IPS-MIB.mib	IANA-LANGUAGE- MIB.mib
AGENTX-MIB.mib	CISCO-LWAPP- LINKTEST-MIB.mib	IANA-RTPROTO- MIB.mib
ALARM-MIB.mib	CISCO-LWAPP- LOCAL-AUTH-MIB.mib	IANAifType-MIB.mib
APS-MIB.mib	CISCO-LWAPP- MDNS-MIB.mib	IEEE8021-CFM-MIB.mib
ATM-FORUM-MIB.mib	CISCO-LWAPP- MESH-BATTERY-MIB.mib	IEEE8021-PAE-MIB.mib
ATM-FORUM- TC-MIB.mib	CISCO-LWAPP- MESH-LINKTEST-MIB.mib	IEEE8021-TC-MIB.mib
ATM-MIB.mib	CISCO-LWAPP- MOBILITY-EXT-MIB.mib	IEEE802171-CFM- MIB.mib
ATM-TC-MIB.mib	CISCO-LWAPP- MOBILITY-MIB.mib	IEEE8023-LAG-MIB.mib
ATM2-MIB.mib	CISCO-LWAPP- NETFLOW-MIB.mib	IEEE802dot11-MIB.mib
BGP4-MIB.mib	CISCO-LWAPP- REAP-MIB.mib	IF-INVERTED- STACK-MIB.mib
BRIDGE-MIB.mib	CISCO-LWAPP- RF-MIB.mib	IF-MIB.mib
CISCO-AAA- SERVER-MIB.mib	CISCO-LWAPP- SI-MIB.mib	IGMP-STD-MIB.mib
CISCO-AAA- SESSION-MIB.mib	CISCO-LWAPP- TC-MIB.mib	INET-ADDRESS-MIB.mib
CISCO-AAL5-MIB.mib	CISCO-LWAPP- TRUSTSEC-MIB.mib	INT-SERV-MIB.mib

CISCO-ACCESS-ENVMON-MIB.mib	CISCO-LWAPP- TSM-MIB.mib	INTEGRATED-SERVICES-MIB.mib
CISCO-ATM-EXT -MIB.mib	CISCO-LWAPP- WLAN-MIB.mib	IP-FORWARD-MIB.mib
CISCO-ATM-PVCTRAP-EXTN-MIB.mib	CISCO-LWAPP-WLAN-SECURITY-MIB.mib	IP-MIB.mib
CISCO-ATM- QOS-MIB.mib	CISCO-MEDIA-GATEWAY-MIB.mib	IPMCAST-MIB.mib
CISCO-AUTH-FRAMEWORK-MIB.mib	CISCO-MOTION-MIB.mib	IPMROUTE-MIB.mib
CISCO-BGP-POLICY-ACCOUNTING-MIB.mib	CISCO-MPLS-LSR-EXT-STD-MIB.mib	IPMROUTE-STD -MIB.mib
CISCO-BGP4-MIB.mib	CISCO-MPLS-TC-EXT-STD-MIB.mib	IPV6-FLOW-LABEL-MIB.mib
CISCO-BULK-FILE -MIB.mib	CISCO-MPLS-TE-STD-EXT-MIB.mib	IPV6-ICMP-MIB.mib
CISCO-CBP-TARGET -MIB.mib	CISCO-NAC-TC -MIB.mib	IPV6-MIB.mib
CISCO-CBP-TARGET-TC-MIB.mib	CISCO-NBAR-PROTOCOL-DISCOVERY-MIB.mib	IPV6-MLD-MIB.mib
CISCO-CBP-TC-MIB.mib	CISCO-NETSYNC -MIB.mib	IPV6-TC.mib
CISCO-CCME-MIB.mib	CISCO-NTP-MIB.mib	IPV6-TCP-MIB.mib
CISCO-CDP-MIB.mib	CISCO-OSPF- MIB.mib	IPV6-UDP-MIB.mib
CISCO-CEF-MIB.mib	CISCO-OSPF- TRAP-MIB.mib	ISDN-MIB.mib
CISCO-CEF-TC.mib	CISCO-OTN-IF-MIB.mib	ISIS-MIB.mib
CISCO-CLASS-BASED-QOS-MIB.mib	CISCO-PAE-MIB.mib	ITU-ALARM-MIB.mib
CISCO-CONFIG- COPY-MIB.mib	CISCO-PAGP-MIB.mib	ITU-ALARM-TC- MIB.mib
CISCO-CONFIG- MAN-MIB.mib	CISCO-PIM-MIB.mib	L2TP-MIB.mib
CISCO-CONTENT-ENGINE-MIB.mib	CISCO-PING-MIB.mib	LANGTAG-TC-MIB.mib
CISCO-CONTEXT-MAPPING-MIB.mib	CISCO-POLICY-GROUP-MIB.mib	LLDP-EXT-DOT1 -MIB.mib
CISCO-DATA-COLLECTION-MIB.mib	CISCO-POWER-ETHERNET-EXT-MIB.mib	LLDP-EXT-DOT3 -MIB.mib
CISCO-DEVICE-EXCEPTION-REPORTING-MIB.mib	CISCO-PRIVATE-VLAN-MIB.mib	LLDP-MIB.mib
CISCO-DIAL-CONTROL-MIB.mib	CISCO-PROCESS-MIB.mib	MAU-MIB.mib
CISCO-DOT11-ASSOCIATION-MIB.mib	CISCO-PRODUCTS- MIB.mib	MGMD-STD-MIB.mib

CISCO-DOT11-HT-PHY-MIB.mib	CISCO-PTP-MIB.mib	MPLS-FTN-STD-MIB.mib
CISCO-DOT11-IF-MIB.mib	CISCO-RADIUS-EXT-MIB.mib	MPLS-L3VPN-STD-MIB.mib
CISCO-DOT11-SSID-SECURITY-MIB.mib	CISCO-RF-MIB.mib	MPLS-LDP-ATM-STD-MIB.mib
CISCO-DOT3-OAM-MIB.mib	CISCO-RF-SUPPLEMENTAL-MIB.mib	MPLS-LDP-FRAME-RELAY-STD-MIB.mib
CISCO-DS3-MIB.mib	CISCO-RTTMON-TC-MIB.mib	MPLS-LDP-GENERIC-STD-MIB.mib
CISCO-DYNAMIC-TEMPLATE-MIB.mib	CISCO-SELECTIVE-VRF-DOWNLOAD-MIB.mib	MPLS-LDP-MIB.mib
CISCO-DYNAMIC-TEMPLATE-TC-MIB.mib	CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB.mib	MPLS-LDP-STD-MIB.mib
CISCO-EIGRP-MIB.mib	CISCO-SESS-BORDER-CTRLR-EVENT-MIB.mib	MPLS-LSR-MIB.mib
CISCO-EMBEDDED-EVENT-MGR-MIB.mib	CISCO-SESS-BORDER-CTRLR-STATS-MIB.mib	MPLS-LSR-STD-MIB.mib
CISCO-ENHANCED-IMAGE-MIB.mib	CISCO-SMI.mib	MPLS-TC-MIB.mib
CISCO-ENHANCED-MEMPOOL-MIB.mib	CISCO-SONET-MIB.mib	MPLS-TC-STD-MIB.mib
CISCO-ENTITY-ASSET-MIB.mib	CISCO-ST-TC.mib	MPLS-TE-MIB.mib
CISCO-ENTITY-EXT-MIB.mib	CISCO-STACKWISE-MIB.mib	MPLS-TE-STD-MIB.mib
CISCO-ENTITY-FRU-CONTROL-MIB.mib	CISCO-STP-EXTENSIONS-MIB.mib	MPLS-VPN-MIB.mib
CISCO-ENTITY-QFP-MIB.mib	CISCO-SUBSCRIBER-IDENTITY-TC-MIB.mib	MSDP-MIB.mib
CISCO-ENTITY-REDUNDANCY-MIB.mib	CISCO-SUBSCRIBER-SESSION-MIB.mib	NET-SNMP-AGENT-MIB.mib
CISCO-ENTITY-REDUNDANCY-TC-MIB.mib	CISCO-SUBSCRIBER-SESSION-TC-MIB.mib	NET-SNMP-EXAMPLES-MIB.mib
CISCO-ENTITY-SENSOR-MIB.mib	CISCO-SYSLOG-MIB.mib	NET-SNMP-MIB.mib
CISCO-ENTITY-VENDORTYPE-OID-MIB.mib	CISCO-SYSTEM-EXT-MIB.mib	NET-SNMP-TC.mib
CISCO-ENVMON-MIB.mib	CISCO-SYSTEM-MIB.mib	NHRP-MIB.mib
CISCO-EPM-NOTIFICATION-MIB.mib	CISCO-TAP2-MIB.mib	NOTIFICATION-LOG-MIB.mib
CISCO-ETHER-CFM-MIB.mib	CISCO-TC.mib	OLD-CISCO-CHASSIS-MIB.mib

CISCO-ETHERLIKE- EXT- MIB.mib	CISCO-TCP-MIB.mib	OLD-CISCO-INTERFACES -MIB.mib
CISCO-FABRIC- C12K-MIB.mib	CISCO-TEMP-LWAPP -DHCP-MIB.mib	OLD-CISCO-SYS- MIB.mib
CISCO-FIREWALL -TC.mib	CISCO-TRUSTSEC -SXP-MIB.mib	OLD-CISCO-SYSTEM -MIB.mib
CISCO-FLASH-MIB.mib	CISCO-TRUSTSEC -TC-MIB.mib	OPT-IF-MIB.mib
CISCO-FRAME- RELAY-MIB.mib	CISCO-UBE-MIB.mib	OSPF-MIB.mib
CISCO-FTP-CLIENT -MIB.mib	CISCO-UNIFIED- COMPUTING-ADAPTOR -MIB.mib	OSPF-TRAP-MIB.mib
CISCO-HSRP-EXT -MIB.mib	CISCO-UNIFIED- COMPUTING-COMPUTE -MIB.mib	OSPFV3-MIB.mib
CISCO-HSRP-MIB.mib	CISCO-UNIFIED- COMPUTING-ETHER -MIB.mib	P-BRIDGE-MIB.mib
CISCO-IETF-ATM2 -PVCTRAP- MIB.mib	CISCO-UNIFIED- COMPUTING-FC- MIB.mib	PIM-MIB.mib
CISCO-IETF-BFD -MIB.mib	CISCO-UNIFIED- COMPUTING-MEMORY -MIB.mib	PIM-STD-MIB.mib
CISCO-IETF-FRR -MIB.mib	CISCO-UNIFIED- COMPUTING -MIB.mib	POWER-ETHERNET -MIB.mib
CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED- COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED- COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED- COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS- TE-EXT-STD-03- MIB.mib	CISCO-VLAN- IFTABLE-RELATIONSHIP -MIB.mib	PTOPO-MIB.mib
CISCO-IETF-MPLS- TE-P2MP-STD-MIB.mib	CISCO-VLAN- MEMBERSHIP-MIB.mib	PerfHist-TC-MIB.mib
CISCO-IETF-MSDP -MIB.mib	CISCO-VOICE-COMMON -DIAL-CONTROL-MIB.mib	Q-BRIDGE-MIB.mib
CISCO-IETF-PIM-EXT -MIB.mib	CISCO-VOICE-DIAL -CONTROL-MIB.mib	RADIUS-ACC-CLIENT -MIB.mib

CISCO-IETF-PIM -MIB.mib	CISCO-VOICE-DNIS -MIB.mib	RADIUS-AUTH-CLIENT -MIB.mib
CISCO-IETF-PW- ATM-MIB.mib	CISCO-VPDN-MGMT -MIB.mib	RFC-1212.mib
CISCO-IETF-PW- ENET-MIB.mib	CISCO-VTP-MIB.mib	RFC-1215.mib
CISCO-IETF-PW-MIB.mib	CISCO-WIRELESS- NOTIFICATION-MIB.mib	RFC1155-SMI.mib
CISCO-IETF-PW- MPLS-MIB.mib	CISCOSB-DEVICEPARAMS -MIB.mib	RFC1213-MIB.mib
CISCO-IETF-PW -TC-MIB.mib	CISCOSB- HWENVIRONMENT.mib	RFC1315-MIB.mib
CISCO-IETF-PW -TDM-MIB.mib	CISCOSB-MIB.mib	RFC1398-MIB.mib
CISCO-IETF-VPLS -BGP-EXT-MIB.mib	CISCOSB-Physicaldescription -MIB.mib	RIPv2-MIB.mib
CISCO-IETF-VPLS -GENERIC-MIB.mib	DIAL-CONTROL-MIB.mib	RMON-MIB.mib
CISCO-IETF-VPLS- LDP-MIB.mib	DIFFSERV-DSCP-TC.mib	RMON2-MIB.mib
CISCO-IF-EXTENSION -MIB.mib	DIFFSERV-MIB.mib	RSTP-MIB.mib
CISCO-IGMP-FILTER -MIB.mib	DISMAN-NSLOOKUP -MIB.mib	RSVP-MIB.mib
CISCO-IMAGE-LICENSE -MGMT-MIB.mib	DISMAN-PING-MIB.mib	SMON-MIB.mib
CISCO-IMAGE-MIB.mib	DISMAN-SCHEDULE -MIB.mib	SNA-SDLC-MIB.mib
CISCO-IMAGE-TC.mib	DISMAN-SCRIPT-MIB.mib	SNMP-COMMUNITY -MIB.mib
CISCO-IP-LOCAL- POOL-MIB.mib	DISMAN-TRACEROUTE -MIB.mib	SNMP-FRAMEWORK -MIB.mib
CISCO-IP-TAP-MIB.mib	DOT3-OAM-MIB.mib	SNMP-MPD-MIB.mib
CISCO-IP-URPF-MIB.mib	DRAFT-MSDP-MIB.mib	SNMP-NOTIFICATION -MIB.mib
CISCO-IPMROUTE- MIB.mib	DS0-MIB.mib	SNMP-PROXY-MIB.mib
CISCO-IPSEC-FLOW -MONITOR-MIB.mib	DS1-MIB.mib	SNMP-REPEATER -MIB.mib
CISCO-IPSEC-MIB.mib	DS3-MIB.mib	SNMP-TARGET-MIB.mib
CISCO-IPSEC-POLICY -MAP-MIB.mib	ENTITY-MIB.mib	SNMP-USER-BASED -SM-MIB.mib
CISCO-IPSLA- AUTOMEASURE-MIB.mib	ENTITY-SENSOR-MIB.mib	SNMP-USM-AES -MIB.mib
CISCO-IPSLA- ECHO-MIB.mib	ENTITY-STATE-MIB.mib	SNMP-USM-DH- OBJECTS-MIB.mib

CISCO-IPSLA- JITTER-MIB.mib	ENTITY-STATE- TC-MIB.mib	SNMP-VIEW-BASED-ACM-MIB.mib
CISCO-IPSLA- TC-MIB.mib	ESO-CONSORTIUM -MIB.mib	SNMPv2-CONF.mib
CISCO-ISDN-MIB.mib	ETHER-WIS.mib	SNMPv2-MIB.mib
CISCO-LICENSE-MGMT-MIB.mib	EtherLike-MIB.mib	SNMPv2-SMI.mib
CISCO-LOCAL-AUTH-USER-MIB.mib	FDDI-SMT73-MIB.mib	SNMPv2-TC-v1.mib
CISCO-LWAPP- AAA-MIB.mib	FR-MFR-MIB.mib	SNMPv2-TC.mib
CISCO-LWAPP- AP-MIB.mib	FRAME-RELAY -DTE-MIB.mib	SNMPv2-TM.mib
CISCO-LWAPP-CCX-RM-MIB.mib	FRNETSERV- MIB.mib	SONET-MIB.mib
CISCO-LWAPP- CDP-MIB.mib	GMPLS-LSR- STD-MIB.mib	SYSAPPL-MIB.mib
CISCO-LWAPP-CLIENT-ROAMING-CAPABILITY.mib	GMPLS-TC-STD- MIB.mib	TCP-MIB.mib
CISCO-LWAPP-CLIENT-ROAMING-MIB.mib	GMPLS-TE-STD-MIB.mib	TOKEN-RING-RMON-MIB.mib
CISCO-LWAPP-DHCP -MIB.mib	HC-PerfHist-TC-MIB.mib	TOKENRING-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.mib	HC-RMON-MIB.mib	TRANSPORT-ADDRESS-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CCX-TC-MIB.mib	HCNUM-TC.mib	TUNNEL-MIB.mib
CISCO-LWAPP-DOT11-LDAP-MIB.mib	HOST-RESOURCES -MIB.mib	UDP-MIB.mib
CISCO-LWAPP- DOT11-MIB.mib	HOST-RESOURCES -TYPES.mib	VPN-TC-STD-MIB.mib
CISCO-LWAPP-DOWNLOAD-MIB.mib	IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib	VRRP-MIB.mib
CISCO-LWAPP- IDS-MIB.mib	IANA-GMPLS-TC-MIB.mib	

MDT での収集用に事前にロードした YANG モジュールのリスト

ここでは、Cisco Crosswork Data Gateway が Cisco IOS XR デバイスの MDT による収集をサポートする YANG モジュールのリストを示します。

cli_xr_bgp_oper.yang	Cisco-IOS-XR-ip-bfd-oper.yang
Cisco-IOS-XR-ipv4-bgp-oper.yang	Cisco-IOS-XR-asr9k-xbar-oper.yang

Cisco-IOS-XR-ipv4-acl-oper.yang	Cisco-IOS-XR-snmp-sensormib-oper.yang
Cisco-IOS-XR-shellutil-filesystem-oper.yang	Cisco-IOS-XR-config-cfgmgr-oper.yang
Cisco-IOS-XR-infra-alarm-logger-oper.yang	Cisco-IOS-XR-infra-fti-oper.yang
Cisco-IOS-XR-icpe-infra-oper.yang	Cisco-IOS-XR-dot1x-oper.yang
Cisco-IOS-XR-fretta-bcm-dpa-stats-oper.yang	Cisco-IOS-XR-sdr-invmgr-diag-oper.yang
Cisco-IOS-XR-cofo-infra-oper.yang	Cisco-IOS-XR-wanphy-ui-oper.yang
Cisco-IOS-XR-man-ems-oper.yang	Cisco-IOS-XR-bundlemgr-oper.yang
Cisco-IOS-XR-mpls-lsd-oper.yang	Cisco-IOS-XR-l2vpn-oper.yang
Cisco-IOS-XR-show-fpd-loc-ng-oper.yang	Cisco-IOS-XR-asr9k-qos-oper.yang
Cisco-IOS-XR-telemetry-model-driven-oper.yang	Cisco-IOS-XR-segment-routing-ms-oper.yang
Cisco-IOS-XR-shellutil-oper.yang	Cisco-IOS-XR-pfi-im-cmd-oper.yang
Cisco-IOS-XR-ip-iep-oper.yang	Cisco-IOS-XR-asic-errors-oper.yang
Cisco-IOS-XR-cdp-oper.yang	Cisco-IOS-XR-lib-keychain-oper.yang
Cisco-IOS-XR-ip-sbfd-oper.yang	Cisco-IOS-XR-sdr-invmgr-oper.yang
Cisco-IOS-XR-tty-management-cmd-oper.yang	Cisco-IOS-XR-ipv4-ospf-oper.yang
Cisco-IOS-XR-upgrade-fpd-oper.yang	Cisco-IOS-XR-pfm-oper.yang
Cisco-IOS-XR-crypto-macsec-secy-oper.yang	Cisco-IOS-XR-config-valid-ccv-oper.yang
Cisco-IOS-XR-ip-iarm-v6-oper.yang	Cisco-IOS-XR-ip-iarm-v4-oper.yang
Cisco-IOS-XR-ipv4-autorp-oper.yang	Cisco-IOS-XR-infra-statsd-oper.yang
Cisco-IOS-XR-pbr-vservice-ea-oper.yang	Cisco-IOS-XR-ipv4-vrrp-oper.yang
Cisco-IOS-XR-ip-domain-oper.yang	Cisco-IOS-XR-emproxy-oper.yang
Cisco-IOS-XR-ipv4-io-oper.yang	Cisco-IOS-XR-crypto-ssh-oper.yang
Cisco-IOS-XR-ipv4-hsrp-oper.yang	Cisco-IOS-XR-controller-optics-oper.yang
Cisco-IOS-XR-freqsync-oper.yang	Cisco-IOS-XR-atm-vcm-oper.yang
Cisco-IOS-XR-aaa-diameter-oper.yang	Cisco-IOS-XR-dnx-driver-fabric-plane-oper.yang
Cisco-IOS-XR-ip-tcp-oper.yang	Cisco-IOS-XR-asr9k-lc-fca-oper.yang
Cisco-IOS-XR-drivers-media-eth-oper.yang	Cisco-IOS-XR-mpls-vpn-oper.yang
Cisco-IOS-XR-infra-policymgr-oper.yang	Cisco-IOS-XR-asr9k-sc-envmon-oper.yang
Cisco-IOS-XR-fretta-bcm-dpa-hw-resources-oper.yang	Cisco-IOS-XR-es-acl-oper.yang
Cisco-IOS-XR-subscriber-ipsub-oper.yang	Cisco-IOS-XR-evpn-oper.yang
Cisco-IOS-XR-infra-rsi-oper.yang	Cisco-IOS-XR-rptiming-tmg-oper.yang
Cisco-IOS-XR-prm-server-oper.yang	Cisco-IOS-XR-ethernet-lldp-oper.yang
Cisco-IOS-XR-l2rib-oper.yang	Cisco-IOS-XR-ip-ntp-oper.yang

Cisco-IOS-XR-subscriber-pppoe-ma-oper.yang	Cisco-IOS-XR-mediasvr-linux-oper.yang
Cisco-IOS-XR-ocni-local-routing-oper.yang	Cisco-IOS-XR-ipv6-ma-oper.yang
Cisco-IOS-XR-reboot-history-oper.yang	Cisco-IOS-XR-infra-rmf-oper.yang
Cisco-IOS-XR-asr9k-lpts-oper.yang	Cisco-IOS-XR-infra-correlator-oper.yang
Cisco-IOS-XR-infra-serg-oper.yang	Cisco-IOS-XR-mpls-static-oper.yang
Cisco-IOS-XR-rgmgr-oper.yang	Cisco-IOS-XR-snmp-entitymib-oper.yang
Cisco-IOS-XR-ncs1k-mxp-headless-oper.yang	Cisco-IOS-XR-pbr-vservice-mgr-oper.yang
Cisco-IOS-XR-aaa-nacm-oper.yang	Cisco-IOS-XR-pfi-im-cmd-ctrlr-oper.yang
Cisco-IOS-XR-infra-rcmd-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-resources-oper.yang
Cisco-IOS-XR-crypto-macsec-mka-oper.yang	Cisco-IOS-XR-macsec-ctrlr-oper.yang
Cisco-IOS-XR-tunnel-vpdn-oper.yang	Cisco-IOS-XR-ipv6-nd-oper.yang
Cisco-IOS-XR-ipv4-dhcpd-oper.yang	Cisco-IOS-XR-tunnel-l2tun-oper.yang
Cisco-IOS-XR-ip-rip-oper.yang	Cisco-IOS-XR-infra-dumper-exception-oper.yang
Cisco-IOS-XR-ncs1001-otdr-oper.yang	Cisco-IOS-XR-syncc-oper.yang
Cisco-IOS-XR-asr9k-asic-errors-oper.yang	Cisco-IOS-XR-dnx-driver-oper.yang
Cisco-IOS-XR-pmengine-oper.yang	Cisco-IOS-XR-ncs1k-macsec-ea-oper.yang
Cisco-IOS-XR-linux-os-reboot-history-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-drop-stats-oper.yang
Cisco-IOS-XR-ppp-ea-oper.yang	Cisco-IOS-XR-infra-sla-oper.yang
Cisco-IOS-XR-asr9k-ptp-pd-oper.yang	Cisco-IOS-XR-ncs1001-ots-oper.yang
Cisco-IOS-XR-ipv4-igmp-oper.yang	Cisco-IOS-XR-nto-misc-shmem-oper.yang
Cisco-IOS-XR-ipv4-bgp-oc-oper.yang	Cisco-IOS-XR-ip-rib-ipv4-oper.yang
Cisco-IOS-XR-ip-pfilter-oper.yang	Cisco-IOS-XR-ipv4-pim-oper.yang
Cisco-IOS-XR-lpts-pre-ifib-oper.yang	Cisco-IOS-XR-pppoe-ea-oper.yang
Cisco-IOS-XR-ipv6-ospfv3-oper.yang	Cisco-IOS-XR-infra-syslog-oper.yang
Cisco-IOS-XR-asr9k-netflow-oper.yang	Cisco-IOS-XR-crypto-sam-oper.yang
Cisco-IOS-XR-infra-xtc-oper.yang	Cisco-IOS-XR-Ethernet-SPAN-oper.yang
Cisco-IOS-XR-sysdb-oper.yang	Cisco-IOS-XR-lpts-ifib-oper.yang
Cisco-IOS-XR-lib-mpp-oper.yang	Cisco-IOS-XR-ethernet-link-oam-oper.yang
Cisco-IOS-XR-infra-xtc-agent-oper.yang	Cisco-IOS-XR-mpls-ldp-oper.yang
Cisco-IOS-XR-ip-rib-ipv6-oper.yang	Cisco-IOS-XR-tty-management-oper.yang
Cisco-IOS-XR-rptiming-dti-oper.yang	Cisco-IOS-XR-lmp-oper.yang
Cisco-IOS-XR-wd-oper.yang	Cisco-IOS-XR-nto-misc-shprocmem-oper.yang
Cisco-IOS-XR-man-xml-ttyagent-oper.yang	Cisco-IOS-XR-procmem-oper.yang

Cisco-IOS-XR-ip-daps-oper.yang	Cisco-IOS-XR-Subscriber-infra-subdb-oper.yang
Cisco-IOS-XR-spirit-install-instmgr-oper.yang	Cisco-IOS-XR-asr9k-np-oper.yang
Cisco-IOS-XR-fretta-grid-svr-oper.yang	Cisco-IOS-XR-ptp-oper.yang
Cisco-IOS-XR-clns-isis-oper.yang	Cisco-IOS-XR-tunnel-nve-oper.yang
Cisco-IOS-XR-ipv4-bgp-oper.yang	Cisco-IOS-XR-ocni-oper.yang
Cisco-IOS-XR-ipv4-ma-oper.yang	Cisco-IOS-XR-ncs6k-acl-oper.yang
Cisco-IOS-XR-l2-eth-infra-oper.yang	Cisco-IOS-XR-manageability-object-tracking-oper.yang
Cisco-IOS-XR-plat-chas-invmgr-oper.yang	Cisco-IOS-XR-ocni-intfbase-oper.yang
Cisco-IOS-XR-dwdm-ui-oper.yang	Cisco-IOS-XR-infra-tc-oper.yang
Cisco-IOS-XR-policy-repository-oper.yang	Cisco-IOS-XR-subscriber-session-mon-oper.yang
Cisco-IOS-XR-ipv6-new-dhcpv6d-oper.yang	Cisco-IOS-XR-ip-udp-oper.yang
Cisco-IOS-XR-subscriber-srg-oper.yang	Cisco-IOS-XR-ipv6-acl-oper.yang
Cisco-IOS-XR-manageability-perfmgmt-oper.yang	Cisco-IOS-XR-crypto-macsec-pl-oper.yang
Cisco-IOS-XR-dnx-port-mapper-oper.yang	Cisco-IOS-XR-aaa-tacacs-oper.yang
Cisco-IOS-XR-mpls-te-oper.yang	Cisco-IOS-XR-man-ipsla-oper.yang
Cisco-IOS-XR-nto-misc-oper.yang	Cisco-IOS-XR-invmgr-oper.yang
Cisco-IOS-XR-ppp-ma-oper.yang	Cisco-IOS-XR-ipv4-arp-oper.yang
Cisco-IOS-XR-config-cfgmgr-exec-oper.yang	Cisco-IOS-XR-aaa-locald-oper.yang
Cisco-IOS-XR-perf-meas-oper.yang	Cisco-IOS-XR-ha-eem-policy-oper.yang
Cisco-IOS-XR-snmp-agent-oper.yang	Cisco-IOS-XR-ascii-ltrace-oper.yang
Cisco-IOS-XR-asr9k-lc-ethctrl-oper.yang	Cisco-IOS-XR-skp-qos-oper.yang
Cisco-IOS-XR-ifmgr-oper.yang	Cisco-IOS-XR-flowspec-oper.yang
Cisco-IOS-XR-iedge4710-oper.yang	Cisco-IOS-XR-icpe-sdacc-oper.yang
Cisco-IOS-XR-controller-otu-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-npu-stats-oper.yang
Cisco-IOS-XR-subscriber-accounting-oper.yang	Cisco-IOS-XR-alarmgr-server-oper.yang
Cisco-IOS-XR-ncs5500-qos-oper.yang	Cisco-IOS-XR-fia-internal-tcam-oper.yang
Cisco-IOS-XR-skywarp-netflow-oper.yang	Cisco-IOS-XR-tty-server-oper.yang
Cisco-IOS-XR-ncs1k-mxp-lldp-oper.yang	Cisco-IOS-XR-qos-ma-oper.yang
Cisco-IOS-XR-fib-common-oper.yang	Cisco-IOS-XR-aaa-protocol-radius-oper.yang
Cisco-IOS-XR-dnx-netflow-oper.yang	Cisco-IOS-XR-platform-pifib-oper.yang
Cisco-IOS-XR-lpts-pa-oper.yang	Cisco-IOS-XR-asr9k-fsi-oper.yang
Cisco-IOS-XR-ncs1k-mxp-oper.yang	Cisco-IOS-XR-ncs5500-coherent-node-oper.yang
Cisco-IOS-XR-asr9k-sc-invmgr-oper.yang	Cisco-IOS-XR-snmp-ifmib-oper.yang

Cisco-IOS-XR-ptp-pd-oper.yang	Cisco-IOS-XR-ip-mobileip-oper.yang
Cisco-IOS-XR-ethernet-cfm-oper.yang	Cisco-IOS-XR-wdsysmon-fd-oper.yang
Cisco-IOS-XR-pbr-oper.yang	Cisco-IOS-XR-infra-objmgr-oper.yang
Cisco-IOS-XR-ip-rsvp-oper.yang	Cisco-IOS-XR-ipv6-io-oper.yang
Cisco-IOS-XR-terminal-device-oper.yang	Cisco-IOS-XR-plat-chas-invmgr-ng-oper.yang
Cisco-IOS-XR-mpls-oam-oper.yang	Cisco-IOS-XR-ncs5500-coherent-portmode-oper.yang
Cisco-IOS-XR-sse-span-oper.yang	Cisco-IOS-XR-infra-dumper-oper.yang
Cisco-IOS-XR-asr9k-sc-diag-oper.yang	Cisco-IOS-XR-mpls-io-oper.yang

MDTでの収集用に事前にロードしたYANGモジュールのリスト