# デバイスの設定



# デバイスの追加

デバイスを追加するには、次の手順を実行します。

**ステップ 1** メインウィンドウで、[モニタ（Monitor）] > [デバイス（Devices）] または [設定（Configure）] > [デバイス（Devices）] をクリックします。もしくは、[設定（Configure）] > [データゲートウェイ（Data Gateways）] > [data_gateway_instance] の順に移動して、Crosswork Data Gateway にデバイスを追加、リンクすることもできます。

**ステップ 2** [Add Device] をクリックします。

**ステップ 3** CSV ファイルを使用してデバイスをインポートするには、[CSVのインポート（CSV Import）] をクリックします。

**ステップ 4** 単一のデバイスをインポートするには、次のフィールドに入力します。

**表 *1*：デバイスの追加のフィールドに関する説明**

| フィールド | 説明 |
|---|---|
| デバイス名（Device Name） | デバイスの表示名<br>（注） データプライバシー上の理由から、このフィールドはデバイスから自動的に入力されません。 |

| フィールド | 説明 |
|---|---|
| 説明（Description） | （任意）デバイスの説明を追加します。 |
| ホストネーム（Hostname） | Crosswork Data Gateway によって使用される DNS FQDN または IP アドレス。 |
| SSH ポート（SSH Port） | （任意）SSH アクセス用の TCP ポート。デフォルトは TCP/22 です。Crosswork Cloud Traffic Analysis に SSH アクセスは必要ありません。 |
| クレデンシャル：SSH（Credential: SSH） | 以前にクレデンシャルグループを作成した場合は、[クレデンシャル：SSH（Credential: SSH）] ドロップダウンリストから選択できます。新しいクレデンシャルグループを作成するには、[クレデンシャル：SSH（Credential: SSH）] ドロップダウンリストから [新しいクレデンシャルの追加（Add New Credential）] を選択します。クレデンシャルグループの詳細については、クレデンシャルの作成を参照してください。 |
| デバイスグループ（Device Group） | Crosswork Cloud Traffic Analysis 専用。以前にデバイスグループを作成した場合は、[デバイスグループ（Device Group）] ドロップダウンリストから選択できます。新しいデバイスグループを作成するには、[デバイスグループ（Device Group）] ドロップダウンリストから [新しいデバイスグループの追加（Add new device group）] を選択します。デバイスグループの詳細については、デバイスグループの設定を参照してください。 |
| 市区町村郡（City） | （任意）デバイスの位置情報の市区町村。 |
| 参照先（Location） | （任意）論理サイト識別子。 |
| 国（Country） | （任意）デバイスの位置情報の国。 |
| デバイスのタイムゾーン（Device Timezone） | （任意）デバイスに対してローカルなタイムゾーン。 |
| タグ（Tags） | （任意）デバイスのグループ化と識別に役立つタグを指定します。たとえば、システム内のルータタイプ（*edge* など）を識別するテキストを入力する場合があります。 |

残りのフィールドは、有効なライセンスがある Crosswork Cloud アプリケーションによって異なります。オプションとして、Crosswork Cloud Trust Insights の Crosswork Data Gateway インスタンスと Crosswork Cloud Traffic Analysis の Crosswork Data Gateway インスタンスの両方にデバイスをリンクすることもできます。

表 *2:* トラストインサイトのデバイスの追加のフィールドに関する説明

| フィールド | 説明 |
|---|---|
| [データゲートウェイ：トラストインサイト（Data Gateway: Trust Insights）] | スイッチを [オン（On）] に切り替え、デバイスの Crosswork Data Gateway インスタンスを選択します。Crosswork Data Gateway を追加するには、「Crosswork Data Gateway の情報の追加」を参照してください。 |

表 *3:* トラフィック分析のデバイスの追加のフィールドに関する説明

| フィールド | 説明 |
|---|---|
| データゲートウェイ：トラフィック分析（Data Gateway: Traffic Analysis） | スイッチを [オン（On）] に切り替え、デバイスの NetFlow Data Gateway インスタンスを選択します。 |
| NetFlow 送信元アドレス（NetFlow Source Address） | NetFlow 送信元アドレスを入力します。 |
| ASN | ASN を入力します。値はプライベート ASN の範囲（64512 ～ 65535）である必要があります。 |
| SNMPアドレス（SNMP Address） | SNMP アドレスを入力しない場合は、NetFlow アドレスが使用されます。 |
| クレデンシャル：SNMP（Credential: SNMP） | 以前にクレデンシャルグループを作成した場合は、[クレデンシャル：SNMP（Credential: SNMP）] ドロップダウンリストから選択できます。追加するデバイスの新しいクレデンシャルグループを作成するには、[クレデンシャル：SNMP（Credential: SNMP）] ドロップダウンリストから [新しいクレデンシャルの追加（Add New Credential）] を選択します。クレデンシャルグループの詳細については、クレデンシャルの作成を参照してください。 |
| BGPルータIDのIPアドレス（BGP Router ID IP Address） | — |
| クレデンシャル：BGP（Credential: BGP） | 以前にクレデンシャルグループを作成した場合は、[クレデンシャル：BGP（Credential: BGP）] ドロップダウンリストから選択できます。追加するデバイスの新しいクレデンシャルグループを作成するには、[クレデンシャル：BGP（Credential: BGP）] ドロップダウンリストから [新しいクレデンシャルの追加（Add New Credential）] を選択します。クレデンシャルグループの詳細については、クレデンシャルの作成を参照してください。 |

（注）　すべての BGP プレフィックスを Cisco Crosswork Data Gateway と共有する必要があります。

**ステップ 5** [保存（**Save**）] をクリックします。

保存操作が完了した後、メインウィンドウで [モニタ（Monitor）] > [デバイス（Devices）] または [設定（Configure）] > [デバイス（Devices）] をクリックすると、デバイスが表示されます。

# トラフィック分析用のデバイスを追加するための前提条件

トラフィック分析にデバイスを追加する前に、デバイスに SSH と次のプロトコルが設定されていることを確認します。

**表 *4:* プロトコル設定**

| プロトコル | 例 |
|---|---|
| SNMP | SNMP の構成例 （4 ページ） |
| BGP | Cisco IOS デバイス用 BGP の構成例 （5 ページ） |
| ネットワーク フロー モニタリング | • Cisco IOS XR デバイス用 Netflow の構成例 （7 ページ）<br>• Cisco IOS XR デバイス用 IPFIX の構成例 （8 ページ） |

デバイスが特定のコマンドを制限するように設定されている場合は、次の CLI コマンドが許可されていることを確認します。

- `show platform security integrity dossier`
- `show version`

以下のセクションには、構成例が含まれています。

## SNMP の構成例

次のコードは、SNMP の構成例を示しています。

- SNMPv2 の構成例：

  ```
  snmp-server community flow123 RO
  ```

  前の例では、**flow123** が SNMP コミュニティの構成と一致する必要があります。

- SNMPv3 の構成例
  - 認証なし、プライバシーなしの SNMPv3 の場合：

```
snmp-server group [groupname] v3 noauth
snmp-server user [username] [groupname] v3
```

- 認証あり、プライバシーなしの SNMPv3 の場合：

```
snmp-server group [groupname] v3 auth
snmp-server user [username] [groupname] auth [md5|sha] <auth-password>
```

- 認証あり、プライバシーありの SNMPv3 の場合：

```
snmp-server group [groupname] v3 priv
snmp-server user [username] [groupname] auth [md5|sha] <auth-password> priv [aes
 128] <priv-password>
```

Crosswork Cloud Traffic Analysis は、プライバシープロトコルに対してのみ SNMPv3 128 ビットをサポートします。

- （任意）**snmp-server view** コマンドを使用して、SNMPv3 アクセスを制限できます。次のコマンド例は、Crosswork Cloud Traffic Analysis によって読み取られる SNMP のオブジェクト識別子（OID）を示しています。

```
snmp-server view [view_name] 1.3.6.1.2.1.1 included
snmp-server view [view_name] 1.3.6.1.2.1.2 included
snmp-server view [view_name] 1.3.6.1.2.1.31 included

snmp-server group [groupname] v3 [noauth|auth|priv] read [view_name]
```

# Cisco IOS デバイス用 BGP の構成例

次のコードは、Cisco IOS デバイスの BGP 構成の例です。

（注） すべての BGP プレフィックスを Cisco Crosswork Data Gateway と共有する必要があります。

**Cisco IOS XE**

```
router bgp <asn> << This must match the ASN in the CDG DEVICE configuration page in the
 Crosswork Cloud UI
>>
bgp router-id <router-id>
bgp log-neighbor-changes
no bgp default ipv4-unicast
neighbor <CDG-ipv4-address> remote-as <CDG-asn>  << This must match the ASN of the CDG
in the Crosswork Cloud UI. It should be a Private ASN number. >>
neighbor <CDG-ipv4-address> description Cisco CrossWork Cloud CDG IPv4
neighbor <CDG-ipv4-address> ebgp-multihop 255
neighbor <CDG-ipv4-address> update-source <src-interface>
!
neighbor <CDG-ipv6-address> remote-as <CDG-asn>   << This must match the ASN of the CDG
 in the Crosswork Cloud UI. It should be a Private ASN number. >>
neighbor <CDG-ipv6-address> description Cisco CrossWork Cloud CDG IPv6
neighbor <CDG-ipv6-address> ebgp-multihop 255
neighbor <CDG-ipv6-address> update-source <src-interface>
!
address-family ipv4
  neighbor <CDG-ipv4-address> activate
  neighbor <CDG-ipv4-address> send-community both
  neighbor <CDG-ipv4-address> filter-list 2 in
```

```
  neighbor <CDG-ipv4-address> filter-list 1 out
exit-address-family
!
address-family ipv6
  neighbor <CDG-ipv6-address> activate
  neighbor <CDG-ipv6-address> send-community both
  neighbor <CDG-ipv6-address> filter-list 2 in
  neighbor <CDG-ipv6-address> filter-list 1 out
exit-address-family
!
ip as-path access-list 1 permit .*   <<All BGP prefixes from the device must be shared
with Cisco CrossWork Cloud CDG>>
ip as-path access-list 2 deny .*
!
```

### Cisco IOS XR

```
router bgp <asn> << This must match the ASN in the CDG DEVICE configuration page in the
 Crosswork Cloud UI
>>
 bgp router-id <router-id>
 address-family ipv4 unicast
 !
 address-family ipv6 unicast
 !
 neighbor <CDG-ipv4-address>
  remote-as <CDG-asn>    << This must match the ASN of the CDG in the Crosswork Cloud
UI. It should be a Private ASN number. >>

  ebgp-multihop 255
  description Cisco CrossWork Cloud CDG IPv4
  update-source <src-interface>
  address-family ipv4 unicast
   route-policy DROP in
   route-policy PASS out
 !
 neighbor <route-server-ipv6>
  remote-as <CDG-asn>   << This must match the ASN of the CDG in the Crosswork Cloud UI.
 It should be a Private ASN number. >>

  ebgp-multihop 255
  description Cisco CrossWork Route Server IPv6
  update-source <src-interface>
  address-family ipv6 unicast
   route-policy DROP in
   route-policy PASS out
!
route-policy PASS
 pass
end-policy
!
route-policy DROP
 drop
end-policy
!
```

ここで

- <asn> は、ネットワークの BGP AS 番号です。
- <router-id> は、ネットワークの BPG ルータ ID です。

- <CDG-asn>は、CDG の BGP ASN 番号です。これは、プライベートASN番号である必要があります
- <src-interface> は、ネットワークの BGP 送信元インターフェイスです。
- <CDG-ipv4-address> は CDG の IPv4 アドレスです。
- <CDG-ipv6-address> は CDG の IPv6 アドレスです。

# Cisco IOS XR デバイス用 Netflow の構成例

次のコードは、Cisco IOS XR デバイス用 Netflow の構成例です。

**IPv4 の例**：

```
flow exporter-map ccni
 packet-length 1468
 version v9
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
 !
 transport udp 2055
 source GigabitEthernet0/0/0/0
 destination 172.24.96.171  << this is the IP address of the CDG >>
!
flow monitor-map ccni
 record ipv4
 exporter ccni
 cache entries 1000000
 cache timeout active 12
 cache timeout update 15
!
sampler-map ccni-sampler
 random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0
 ipv4 address 172.24.96.141 255.255.255.128
 flow ipv4 monitor ccni sampler ccni-sampler ingress
```

IPv4 接続を介して NetFlow IPv6 レコードをエクスポートする例：

（注） この例では、192.0.2.169 が Crosswork Data Gateway の IPv4 アドレスです。

```
flow exporter-map ccni
 packet-length 1468
 version v9
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
 !
 transport udp 2055
 source GigabitEthernet0/0/0/0
 destination 192.0.2.169  << this is the IP address of the CDG >>
!
flow monitor-map ccni-ipv6
 record ipv6
```

```
 exporter ccni
 cache entries 1000000
 cache timeout active 12
 cache timeout update 15
!
sampler-map ccni-sampler
random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0
 ipv6 address 2001:100:100::1/64
flow ipv6 monitor ccni-ipv6 sampler ccni-sampler ingress
```

**IPv4 および IPv6 の適用例**：

```
flow exporter-map ccni
packet-length 1468
version v9
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
!
transport udp 2055
source GigabitEthernet 0/0/0/0
destination 172.24.96.171 << this is the IP address of the CDG >>
!
flow monitor-map ccni
  record ipv4
  exporter ccni
  cache entries 1000000
  cache timeout active 12
  cache timeout update 15
!
flow monitor-map ccni-ipv6
  record ipv6
  exporter ccni
  cache entries 1000000
  cache timeout active 12
  cache timeout update 15

sampler-map ccni-sampler
  random 1 out-of 1000
!
interface GigabitEthernet0/0/0/0

  ipv4 address 172.24.96.141 255.255.255.128
  ipv6 address 2001:100:100::1/64
  flow ipv4 monitor ccni sampler ccni-sampler ingress
  flow ipv6 monitor ccni-ipv6 sampler ccni-sampler ingress
```

# Cisco IOS XR デバイス用 IPFIX の構成例

次のコードは、Cisco IOS XR デバイス用 IPFIX の構成例です。

```
flow exporter-map ccni
 packet-length 1468
 version ipfix
  options sampler-table timeout 15
  template data timeout 15
  template options timeout 15
```

```
 !
 transport udp 2055
 source GigabitEthernet0/0/0/0
 destination 172.24.96.184
!
flow monitor-map ccni
 record ipv4
 exporter ccni
 cache entries 1000000
 cache timeout active 3
 cache timeout update 3
!
sampler-map ccni-sampler
 random 1 out-of 1000
!
interface TenGigE0/0/0/16
 description internal interface
 ipv4 address 182.1.0.1 255.255.255.0
 flow ipv4 monitor ccni sampler ccni-sampler ingress
!
interface TenGigE0/0/0/27
 description external interface
 ipv4 address 184.1.0.1 255.255.255.0
 flow ipv4 monitor ccni sampler ccni-sampler ingress
```

# トラフィック分析で使用される SNMP の識別子

Crosswork Cloud Traffic Analysis の特定の SNMP ビューを作成する場合、次のリストに、Crosswork Cloud Traffic Analysis が使用する SNMP オブジェクト識別子（OID）が含まれています。

- sysDescr：1.3.6.1.2.1.1.1.0
- sysObjectID：1.3.6.1.2.1.1.2.0
- sysUpTime：1.3.6.1.2.1.1.3.0
- sysName：1.3.6.1.2.1.1.5.0
- sysLocation：1.3.6.1.2.1.1.6.0
- ifDescr：1.3.6.1.2.1.2.2.1.2
- ifType：1.3.6.1.2.1.2.2.1.3
- ifSpeed：1.3.6.1.2.1.2.2.1.5
- ifOperStatus：1.3.6.1.2.1.2.2.1.8
- ifName：1.3.6.1.2.1.31.1.1.1.1
- ifHCSpeed：1.3.6.1.2.1.31.1.1.1.15
- ifHCInOctets：1.3.6.1.2.1.31.1.1.1.6
- ifHCOutOctets：1.3.6.1.2.1.31.1.1.1.10

# Crosswork Traffic Analysis 用の外部インターフェイスの指定

デバイスを追加したら、SNMP ステータスを確認し、1 つ以上のインターフェイスを外部インターフェイスとして設定する必要があります。Crosswork Cloud Traffic Analysis は、外部インターフェイスを指定するまでトラフィックデータを表示できません。

**ステップ 1** メインウィンドウで、[設定（Configure）] > [デバイス（Devices）] の順にクリックします。

**ステップ 2** [デバイス（Device）] 列に表示されているデバイス名をクリックします。

**ステップ 3** Crosswork Data Gateway とデバイス間に表示される SNMP の上にカーソルを合わせて、ステータスが [接続済み（Connected）] になっていることを確認します。

デフォルトでは、すべてのインターフェイスが内部インターフェイスとして指定されています。デバイスの外部インターフェイスを選択し、外部として指定する必要があります。

**ステップ 4** [トラフィック分析（Traffic Analysis）] タブをクリックしてから、[インターフェイス（Interfaces）] をクリックします。

**ステップ 5** 1 つ以上の外部インターフェイスを選択し、[外部の設定（Set External）] をクリックします。

Crosswork Cloud Traffic Analysis は、インターフェイスを外部インターフェイスとして認識します。

# Crosswork Trust Insights にデバイスを追加するための前提条件

Cisco IOS XR ルータを Crosswork Cloud Trust Insights に追加する前に、次のルータ設定を確認する必要があります。

- デバイスに IOS XR の必要なサポートされるイメージがあることを確認します。サポートされるイメージについては、『Cisco Crosswork Cloud Release Notes』[英語] を参照してください。
- 登録キーと証明書が IOS XR 内で適切に生成されていることを確認します。詳細については、Crosswork Trust Insights のルータ構成の確認 （11 ページ）を参照してください。
- 制限付き特権ユーザを設定していることを確認します。詳細については、Crosswork Trust Insights の制限付き権限のユーザの設定 （14 ページ）を参照してください。

# Crosswork Trust Insights のルータ構成の確認

Crosswork Cloud Trust Insights を使用する前に、Cisco IOS XR ルータが信頼情報にアクセスできるように正しく設定されていることを確認する必要があります。次の手順に従って、ルータが Crosswork Cloud Trust Insights に正しく設定されていることを確認します。

（注） 次の例は、Crosswork Cloud Trust Insights を有効にするために必要な最小限の Cisco IOS XR 構成です。その他の構成例については、Crosswork Cloud Trust Insights を有効にするプラットフォームに対応する構成ガイドを参照してください。構成ガイドへの直接リンクについては、関連ハードウェアのマニュアルを参照してください。

**ステップ 1** ルータにログインし、次のコマンドを入力します。

```
ios# show running-config
```

**ステップ 2** 出力に次の構成要素が含まれていることを確認します。

- ホストネーム
- DNS ドメイン名（DNS domain name）
- 有効化された SSH サーバ
- SSH で有効化された Netconf-yang
- インバウンド SSH アクセス用に設定され、到達可能な有効な IP インターフェイス
- 適切な静的デフォルトルートの設定

次の出力例は、表示される内容を示しています。

```
hostname xr9kv-001
domain name test.cisco.com
!
netconf-yang agent
 ssh
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 192.168.1.123 255.255.255.0
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 192.168.1.1
  !
!
ssh server v2
ssh server netconf vrf default
```

**ステップ 3** SSH でルータに到達できることを確認します。

**ステップ 4** system-root-key と system-enroll-key の両方のキーペアを生成するには、次の動作モードのコマンドを入力します。

```
RP/0/RP0/CPU0:xr9kv-001#crypto key generate rsa system-root-key
Tue Apr 21 22:45:55.400 UTC
The name for the keys will be: system-root-key
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keypair.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]

RP/0/RP0/CPU0:xr9kv-001#crypto key generate rsa system-enroll-key
Tue Apr 21 22:46:24.943 UTC
The name for the keys will be: system-enroll-key
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keypair.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [2048]:
Generating RSA keys ...
Done w/ crypto generate keypair
[OK]
RP/0/RP0/CPU0:xr9kv-001#
```

生成されたキーは Cisco IOS XR オペレーティングシステム内に安全に保存され、構成には表示されません。

**ステップ 5** Crosswork Cloud Trust Insights にルータを追加するために必要な証明書を生成して登録するには、次の構成を追加します。

```
crypto ca trustpoint system-trustpoint
 keypair rsa system-enroll-key
 ca-keypair rsa system-root-key
 ip-address 1.1.1.1
 subject-name CN=cisco.com
 lifetime certificate 720
 enrollment url self
 message-digest sha256
 lifetime ca-certificate 720
!
```

（注） 上記の例では、CA 証明書のライフタイムは 2 年（720 日）に設定され、登録証明書のライフタイムも 2 年に設定されています。

**ステップ 6** 署名操作と Crosswork Cloud Trust Insights への登録に必要な証明書を認証および登録するには、次のコマンドを入力します。

```
RP/0/RP0/CPU0:xr9kv-001#crypto ca authenticate system-trustpoint
Tue Apr 21 22:47:46.935 UTC
% The subject name in the certificate will include: xr9kv-001.test.cisco.com
  Serial Number  : 25:34
  Subject:
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
Issued By      :
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
  Validity Start : 22:47:47 UTC Tue Apr 21 2020
  Validity End   : 22:47:47 UTC Wed Apr 21 2021
  SHA1 Fingerprint:
  6C20DBEC569808F21A06E779A219C39B1F20E182
RP/0/RP0/CPU0:xr9kv-001#


RP/0/RP0/CPU0:xr9kv-001#crypto ca enroll system-trustpoint
```

```
Tue Apr 21 22:48:31.141 UTC

% The subject name in the certificate will include: CN=test.cisco.com
% The subject name in the certificate will include: xr9kv-001.test.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 144c478a
% The IP address in the certificate is 192.168.23.211
  Serial Number  : 25:35
  Subject:

serialNumber=144c478a,unstructuredAddress=192.168.1.123,unstructuredName=xr9kv-001.test.cisco.com,CN=test.cisco.com

  Issued By      :
 serialNumber=144c478a,unstructuredName=xr9kv-001.test.cisco.com
  Validity Start : 22:48:31 UTC Tue Apr 21 2020
  Validity End   : 22:48:31 UTC Sat Nov 07 2020
  SHA1 Fingerprint:
  8F44F8EE427F9D48B6E47CDF60B90537EF9F65B4
RP/0/RP0/CPU0:xr9kv-001#
```

**ステップ 7** 次の例に示すように、CLI 署名ユーティリティコマンドを使用して、登録証明書と登録キーを使用した証明操作が正常に行われていることを確認します。

（注） 「署名（signature）」フィールドに入力されている場合、登録証明書は Crosswork Cloud Trust Insights の準備が整っています。

```
RP/0/RP0/CPU0:xr9kv-001#show version | utility sign include-certificate
Tue Apr 21 22:49:24.632 UTC
{
"cli-output": "Cisco IOS XR Software, Version 7.0.2\nCopyright (c) 2013-2020 by Cisco Systems,
Inc.\n\nBuild Information:\n Built By : ahoang\n Built On : Fri Mar 13 22:27:54 PDT 2020\n
Built Host : iox-ucs-029\n Workspace : /auto/srcarchive15/prod/7.0.2/xrv9k/ws\n Version : 7.0.2\n
Location : /opt/cisco/XR/packages/\n Label : 7.0.2\n\ncisco IOS-XRv 9000 () processor\n
System uptime is 8 hours 58 minutes\n\n",
"signature-envelop": {
"signature-version": "01",
"digest-algorithm": "RSA-SHA256",
"pub-key-id": "2508",
"signature":
"F910CRigUmsBBQmnRUoiBYmg+TAWseO1Ey5eRBDwCkT+jHAiQdBhKXGl2MVza5JplrLayDdNbU+L4IvNAlFGegXR1G9IVcd/
RHbsIhhD8GvUTLOrYoIXyWw9b3L0PAbOjRTcbSe5Yr+4qf9XJJ1m88xjtJUgEE08jGz5lYgaBGGHMgS8KwAOmyBiwTaZcKaqYUIiLGqWfJ/
PtxsGv0fhJ+8/9FxjdJcWPLIwXAhQe2QkT15afAjV6LmShQu4TM+Dylad4n4A6YlWFz4sAfEWobl0dVGXPKzDI9UUJDYbdOU8j/
y6Bv9Eko8xYZJaDlUyNCjBWmLi28us9car/wbkfw==",
"signing-certificate": [
"MIIDNDCCAhygAwIBAwICCswDQYJKoZIhvcNAQELBQAwOzEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZXN4MThfNy5
jaXNjby5jb20xETAPBgNVBAUTCGVlZmY1MzRiMB4XDTIxMDIyMDA1NTYzNVoXDTIyMDIyMDA1NTYzNVowOzEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZ
XN4MThfNy5jaXNjby5jb20xETAPBgNVBAUTCGVlZmY1MzRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0n
LmZqLe9bJNdvpvOFmr8vQzDwZ9pcjtuRx7SOfafs+RasNTnaOot3IL76hayCCfvkCOK/Re/8tUpjDpLS/rtOx9J/adRIK
GjlpYoxK1PK4XxMubg5cOZFzVprQmwur8Rvhx6c2xB79KANqKYSEF4cgoLHMQ0YHkfcBAs9abnStYecUWOGHwnC3OalM1
x3pRe
4ZCY30mS5ZJa/C+21EL+MDCKPj+aUkOCw8ADJUX3qT+TWMf7aLrZj/hfmzDEgrahbv2A1F9QG+ooP53pjRXmN2k6Va67J
tGsZ7spYF8F5KcUF7AhZWvKxGOegS7sUMBu4EhF0eHLoB7Mz3sVGNHNQIDAQABo0IwQDAPBgNVHRMBAf8EBTADAQH/MA4
GA1UdDwEB/wQEAwIBxjAdBgNVHQ4EFgQUFWl+ShMwn/DK+ExWKWVm9JzwJNgwDQYJKoZIhvcNAQELBQADggEBAJvxdPpw
qF0+WHFxvfTzgr09ql7roJ92vao8M47v9xX2pMQFMQceU9tL3O/XZ6sDAg+FF7jyTAOVHgzbfG2OlVoAuDeElgsK5xrYE
RhWBk86IiWTasbrUSeHPNsXJgHK/RuudpB+w8pdOEYORKsVLfFH/u1Sfet33grRkiEvFxU8zj515mnjhVE/4GgeH9hF6T
pR3/1Xv6Afka74wJbikppNo/d2TH4KX6AJ6hKnkd1PGaTyZ
GF1UFOvtFXV5cAwaL0wfUft7qF2YNFr9i4lUuR4oi///c72eLLuL+c00c6hADUH3lJVRTcuaLbsrviz7yEGOD/7/MfYRf
oZ2wNIP2U=", "MIIDhjCCAm6gAwIBAwICCswwDQYJKoZIhvcNAQELBQAwOzEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZXN
4MThfNy5jaXNjby5jb20xETAPBgNVBAUTCGVlZmY1MzRiMB4XDTIxMDIyMDA1NTYzNloXDTIxMDkwODA1NTYzNlowazET
MBEGA1UEAwwKY2lzY28uY29tIDEmMCQGCSqGSIb3DQEJAhYXeHJ2OWtfZXN4MThfNy5jaXNjby5jb20xGTAXBgkqhkiG9
w0BCQgTCjEuNzQuMzIuMzcxETAPBgNVBAUTCGVlZmY1MzRiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtc
WkoBPwa5yPerZcRtbbUFVDtg7430PjvLzjHjWzmtY/CPea1
bZ3NPWTAUmS0Q+0D5VwqL+5SVkE9ZVwFoRoyMm2+wwbfBAxt0G2MYTdOttLulEP/H7ApVA/Y+pUGXYGsekRxu8Ipyi
```

```
Vesi57DQxgHlo2lk4EBsZsDv7oW9Osrtx7rib/kCyA5hTsEpw3oZ20Qp+91QY+vY7NUIQKx78RYkPiQNeOjQqibR0M1Rj
Glgo4ZTDI4IxsdgXm/xxiX3scTqu1q/XVY3v5uEjT2zao0nZAU6z3PQKDSyHDXg3yIDskFMj74HI6hUJsA1U+Qj+mw9DcK
aypjQ8y7ZchLeeQQIDAQABo2QwYjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwID+DAgBgNVHSUBAf8EFjAUBgg
rBgEFBQcDAQYIKwYBBQUHAwIwHQYDVR0OBBYEFHJJ3dCXoGGWD2yZ8JQ3f/A/8XqxMA0GCSqGSIb3DQEBCwUAA4IBAQBm
z5YfGTbNAXPHJCxA9w8HUHyr1MlKB6wMKT0AUoWBJ6HvXJXoA
H5cs7uF3Zw4QjY28HaaxkMPr6338VbGi3DnyIOf1Hc6/XRfNBi3eMYcSNyRRgtvQSmTzM7A3CrSOiFlMmdPCdYIeoFiMd
M3uIZzfMe1EnONetev1bs+Te29utYXzb6QWjW0oJZ6/6g4cauo6jkhC/SNsRh3b/+8YMzxAHgzRFg+rm/O6cYa3jNCopjR
JqeFfmNuISgU9LIszmkt3/4n4uiAj4aAqwAc7YG0dzwWdwiXUwj3Q7TrMS8R8AaLUN47nYzm0QfUwNbUDkST2XjIGV90J
vH3E2CnAX+j" ]
}
}
```

これにより、信頼情報を取得するためにルータが正しく設定されていることが確認されます。

**ステップ 8** 署名操作で問題が発生した場合は、次のコマンドを使用して既存の証明書とキーをクリアします。

```
# crypto key zeroize rsa <name of key>
# clear crypto ca certificates system-trustpoint
# crypto ca cancel-enroll system-trustpoint
```

**ステップ 9** 有効期限が切れる前に証明書を更新するには、次のコマンドを使用します。

```
# clear crypto ca certificate system-trustpoint
# crypto key zeroize rsa system-enroll-key
# crypto key generate rsa system-enroll-key
# crypto ca authenticate system-trustpoint
# crypto ca enroll system-trustpoint
```

（注） 証明書を更新する前に登録キーを再生成します。署名 CA 証明書および登録証明書のライフタイムは、**crypto ca trustpoint**の構成を使用して設定されます。

# Crosswork Trust Insights の制限付き権限のユーザの設定

Cisco IOS XR ルータの不正操作または構成変更を防ぐには、デバイスへのアクセスに使用するクレデンシャルに制限付きの権限を付与する必要があります。trust dossier コマンドと signing コマンドを実行するために必要な最小限の許可を可能にするために、デバイスに次の構成（推奨されるタスクグループとユーザの構成など）があることを確認します。

Cisco IOS XR リリース 7.3.1 以降のリリースでは、次のコマンドがサポートされています。

```
!
taskgroup alltasks-dossier
task read sysmgr
task read system
task read dossier
task read pkg-mgmt
task read basic-services
task read config-services
task execute dossier
task execute basic-services
!
```

Cisco IOS XR リリース 7.3.1 より前のリリースでは、次のコマンドがサポートされています。

```
!
taskgroup alltasks-dossier
 task read sysmgr
 task read system
```

```
 task read pkg-mgmt
 task read basic-services
 task read config-services
 task execute crypto
 task execute dossier
 task execute basic-services
!
usergroup dossier-group
 taskgroup alltasks-dossier
!
username dossier
 group dossier-group
 secret 10 <not shown here>
!
```

この構成により、次のものが作成されます。

- ドシエの収集および署名操作を有効にするために必要なすべてのタスクを定義する **alltasks-dossier** タスクグループ。必要に応じてタスクグループの名前を変更できます。
- タスク権限が割り当てられる **dossier-group** ユーザグループ。必要に応じて、ユーザグループ名を変更できます。
- 適切なタスクグループ権限を持つ **dossier** ユーザ。必要に応じて、ユーザの名前を変更できます。適切なクレデンシャル（秘密）を指定していることを確認します。

この構成を適用すると、Crosswork Cloud Trust Insights でこの情報を使用して新しいクレデンシャルグループを作成できます。詳細については、「クレデンシャルの作成」を参照してください。

# Trust Insights の信頼ドシエ情報

Crosswork Cloud Trust Insights にデバイスを追加すると、信頼情報を含むドシエが Crosswork Data Gateway 経由でルータから取得されます。信頼ドシエ（.json 形式）は SSH 経由で収集され、Crosswork Cloud Trust Insights 登録キーで署名されます。Crosswork Data Gateway が Crosswork Cloud Trust Insights に転送する信頼ドシエには、次の情報が含まれています。

- Cisco IOS のバージョンとプラットフォームの出力
- アンチリプレイナンス
- システム ハードウェア インベントリ
- ファイル システム インベントリ

（注） ファイル システム インベントリは、Cisco IOS XR リリース 7.9.1 以降のリリースでサポートされています。

- ハードウェアインベントリ用のセキュアな固有デバイス識別子（SUCI）証明書
- ソフトウェア パッケージ インベントリ

- リブート履歴
- ロールバック履歴

# Trust Insights のデバイスドシエのデータ収集

次の手順では、最新のデバイス情報を取得するためにアドホックドシエ収集を開始する方法について説明します。デフォルトでは、デバイスドシエ収集は 12 時間ごとに行われます。ドシエ収集頻度を変更する、または1つ以上のデバイスの収集を無効にするには、デバイスドシエ収集頻度の変更 （16 ページ）を参照してください。

**ステップ 1** メインウィンドウで、[トラストインサイト（Trust Insights）]>[設定（Configure）]>[デバイス（Devices）]の順にクリックします。

**ステップ 2** ドシエの収集を実施するデバイスの名前をクリックします。

**ステップ 3** [トラストインサイト（Trust Insights）] タブをクリックします。

**ステップ 4** [ドシエの収集（Collect Dossier）] をクリックします。

ドシエの収集が完了するまでに数分かかることがあることを示す Informational（情報提供）メッセージが表示され、[ドシエの収集（Collect Dossier）] ボタンの下に要求に関するテキストが表示されます。

ドシエ収集が完了すると、UI でのデバイスデータが更新されます。

# デバイスドシエ収集頻度の変更

1 つ以上のデバイスのドシエ収集頻度を変更できます。

（注） この手順は Crosswork Cloud Trust Insights デバイスにのみ適用されます。

**ステップ 1** メインウィンドウで、[トラストインサイト（Trust Insights）]>[設定（Configure）]>[デバイス（Devices）]の順にクリックします。

**ステップ 2** ドシエ収集の頻度を変更する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

**ステップ 3** [コレクション（Collection）] をクリックします。

（注） Crosswork Cloud は、Trust Insights デバイスのみを表示します。Trust Insights に属していないデバイスを選択した場合、そのデバイスは表示されません。

**ステップ 4** [有効（Enabled）]/[無効（Disabled）] トグルスイッチが [有効（Enabled）] に設定されていることを確認します。[無効（Disabled）] を選択すると、今後のドシエ収集が停止されます。

**ステップ 5** [頻度（Frequency）] ドロップダウンリストから、収集を実行する頻度を選択します。デバイスの [新しい頻度（New Frequency）] 列と [新しいステータス（New Status）] 列が適切に更新されることに注意してください。

**ステップ 6** [保存（Save）] をクリックします。

# Trust Insights 用の Crosswork Data Gateway およびデバイス接続のトラブルシューティング

次の手順では、Crosswork Data Gateway と Crosswork Cloud Trust Insights デバイス間の接続の問題を解決する方法について説明します。

**ステップ 1** メインウィンドウで、[デバイス（Devices）] をクリックしてから、Crosswork Data Gateway への接続を表示するデバイスをクリックします。

**ステップ 2** [ステータス（Status）] タブをクリックします。

**ステップ 3** Crosswork Data Gateway とデバイス間の接続がエラーを示す赤色で、ファイアウォールがある場合は、cdg.crosswork.cisco.com および crosswork.cisco.com を許可するように設定されていることを確認します。

Crosswork Data Gateway とデバイス間の接続をテストして修正します。

**ステップ 4** Crosswork Data Gateway とデバイス間の [SSH] の矢印が接続の正常性を示す緑色であることを確認します。

[SSH] の矢印が赤色の場合、Crosswork Data Gateway はデバイスに接続できません。次のエラーを修正します。

- ルータの SSH 構成が正しいことを確認します。詳細については、Crosswork Trust Insights のルータ構成の確認 （11 ページ） を参照してください。
- Crosswork Cloud Trust Insights で入力したクレデンシャルが、ルータに設定されているクレデンシャルと一致していることを確認します。[SSH] リンクにカーソルを合わせ、青色のハイパーリンクをクリックして、そのデバイスのクレデンシャルに移動します。

**ステップ 5** Crosswork Data Gateway とデバイス間の [トラストデータ（Trust Data）] の矢印が接続の正常性を示す緑色であることを確認します。

# デバイスの無効化

デバイスを無効にすると、情報の収集が一時的に停止します。以前に収集されたデバイスデータは保持されます。

または、デバイスを削除して、デバイスとそのデータを完全に削除することもできます。デバイスを削除した後は、そのデータを回復できません。デバイスの削除 （18 ページ） を参照してください。

**ステップ 1** メインウィンドウで、[モニタ（Monitor）]>[デバイス（Devices）] または [設定（Configure）]>[デバイス（Devices）] をクリックします。

**ステップ 2** 非アクティブ化にする 1 つ以上のデバイスの横にあるチェックボックスをオンにし、[無効化（Disable）] をクリックします。

デバイスが非アクティブ化されたことを示すメッセージが表示されます。

以前に非アクティブ化されたデバイスを再アクティブ化できます。デバイスを再アクティブ化した後、デバイスの詳細ページに統計情報が表示されるまでに最大 30 分かかる場合があります。

**ステップ 3** デバイスのデータ収集を再開するには、デバイスを選択し、[有効化（Enable）] をクリックします。

デバイスがアクティブ化されたことを示すメッセージが表示され、デバイスのデータ収集が再開されます。

# デバイスの削除

デバイスを削除すると、システムにより以前に収集されたすべてのデバイスデータが削除されます。デバイスを削除した後は、データを回復できません。

または、デバイスを無効にしてデータ収集を一時的に停止し、以前に収集したデバイスデータを保持することもできます。デバイスの無効化 （17 ページ）を参照してください。

**ステップ 1** メインウィンドウで、[モニタ（Monitor）]>[デバイス（Devices）] または [設定（Configure）]>[デバイス（Devices）] をクリックします。

**ステップ 2** 削除するデバイスの名前をクリックします。

**ステップ 3** [削除] をクリックします。

**ステップ 4** デバイスを削除することを確認するには、[削除（Remove）] をクリックします。

デバイスとその以前に収集されたデータが削除されます。

**ステップ 5** 最近削除されたデバイスを復元するには、削除されたデバイスの復元 （18 ページ）を参照してください。

# 削除されたデバイスの復元

以前に削除したデバイスを復元できます。デバイスを削除すると、Crosswork Cloud は必要に応じてすぐに再度追加できるように、デバイスを約 7 日間記憶します。

**ステップ 1** メインウィンドウで、[設定（Configure）]>[デバイスの削除（Removed Devices）] の順にクリックします。

デバイスを削除してから 7 日を超える場合、[削除済みデバイス（Removed Devices）] のリストに表示されないことがあります。デバイスの追加 （1 ページ）の説明に従って、デバイスを再度追加する必要があります。

**ステップ 2** 再度追加するデバイスの横にある [復元（Restore）] をクリックします。

デバイスが復元されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。