SecIntel on MX 設定ガイド

Juniper Networks .K.K

2020年7月31日

Juniper Networks | Engineering Simplicity

更新履歴

バージョン	更新日	更新内容
1.0	2020/7/31	初版公開

はじめに

本資料にある内容は、資料作成時点におけるものであり、事前の予告なしに内容を変更する場合があります。

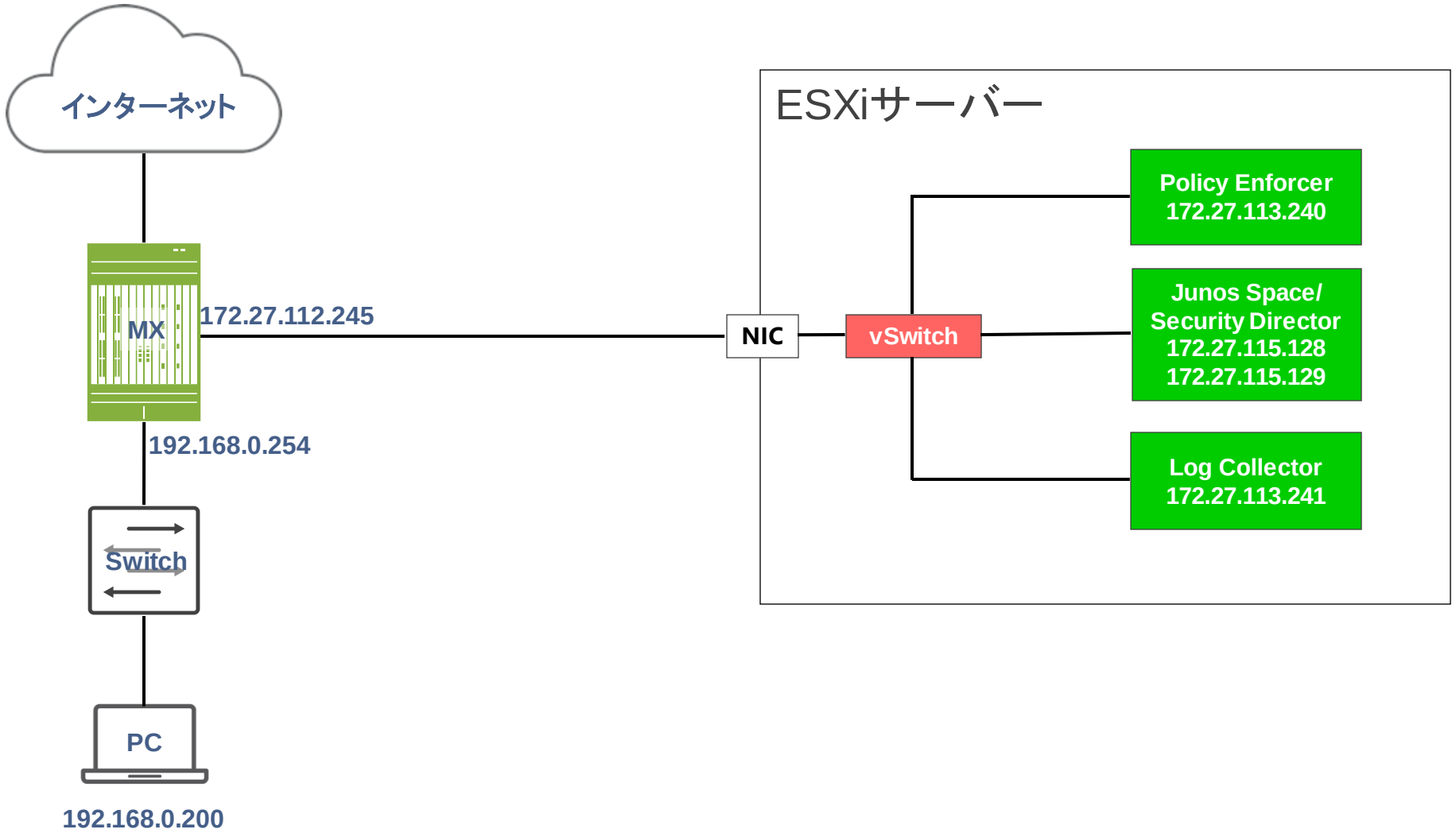
本資料は内容の正確さを保つために努めて作成しておりますが、本資料を利用することによって生じた損害について、当社は一切責任を負わないものとします。

また、本資料の内容と公式情報との間に差分がある場合、公式情報を正としてお取り扱いください。

本資料は下記のソフトウェア/サービスを用いてConnected Securityのセットアップを行っています。

- ESXi 6.0
- space-19.4R1.3.ova
- Security-Director-19.4R1.53.img
- Policy_Enforcer-19.4R1-975.ova
- Log-Collector-19.4R1.28.ova
- MX240(OS Version 19.4R1.10)

構成イメージ



Agenda

- 事前準備・設定
- Security Director設定
- MX設定
- MX確認コマンド一例

事前準備・設定

事前準備・設定

1. Junos Space、Log Collector、Policy Enforcerのデプロイ・各初期設定を行う
2. Junos SpaceにSecurity Directorをインストールする
3. Device Discovery ProfilesでMXを登録する
   （※MX側でIPアドレス・SNMPの事前設定が必要となります）
4. 登録したMXのOSバージョンに合わせたDMIスキーマをインストールする
5. Sky ATPアカウントを持っていない場合は下記ポータルサイトでアカウントを作成
   https://sky.junipersecurity.net/

   -アカウント作成方法は下記URLを参照
   https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/task/configuration/sky-atp-registering.html

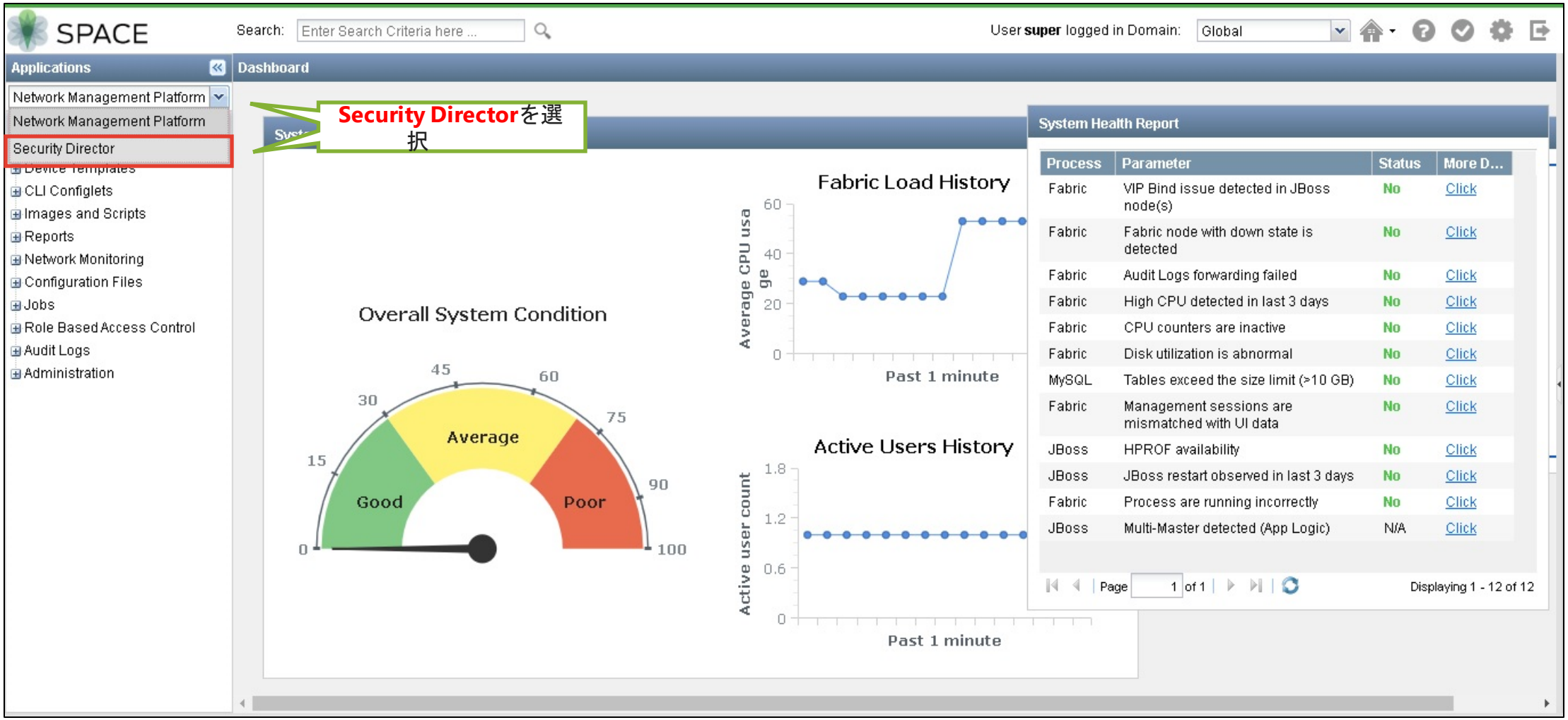
   ※本年からSky ATPはATP Cloudへ名称を変更させて頂きました。
   GUI上や各ドキュメント上の表記につきましては、ATP Cloud に随時変更させて頂く予定でございます。
   本マニュアルは、変更前の現在のGUI上の表記に合わせてSky ATP の名称で作成しております。

Security Director設定

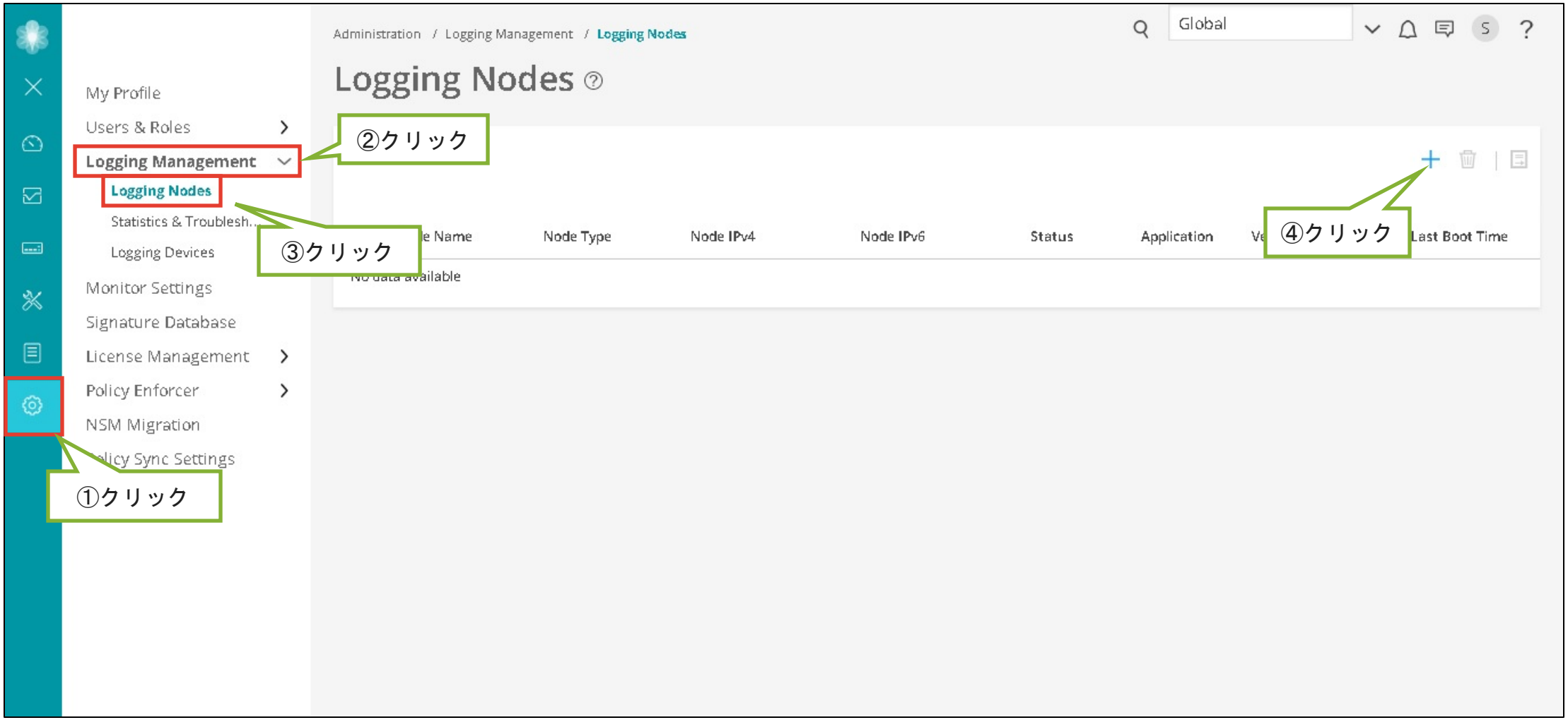
Security Director基本設定の流れ

1. Log Collectorの設定
2. Policy Enforcerの設定
3. Secure Fabricの設定
   -Secure Fabric：ネットワークデバイスの集合
4. Sky ATPの設定
   -アカウント作成済みのSky ATP/Realmの指定

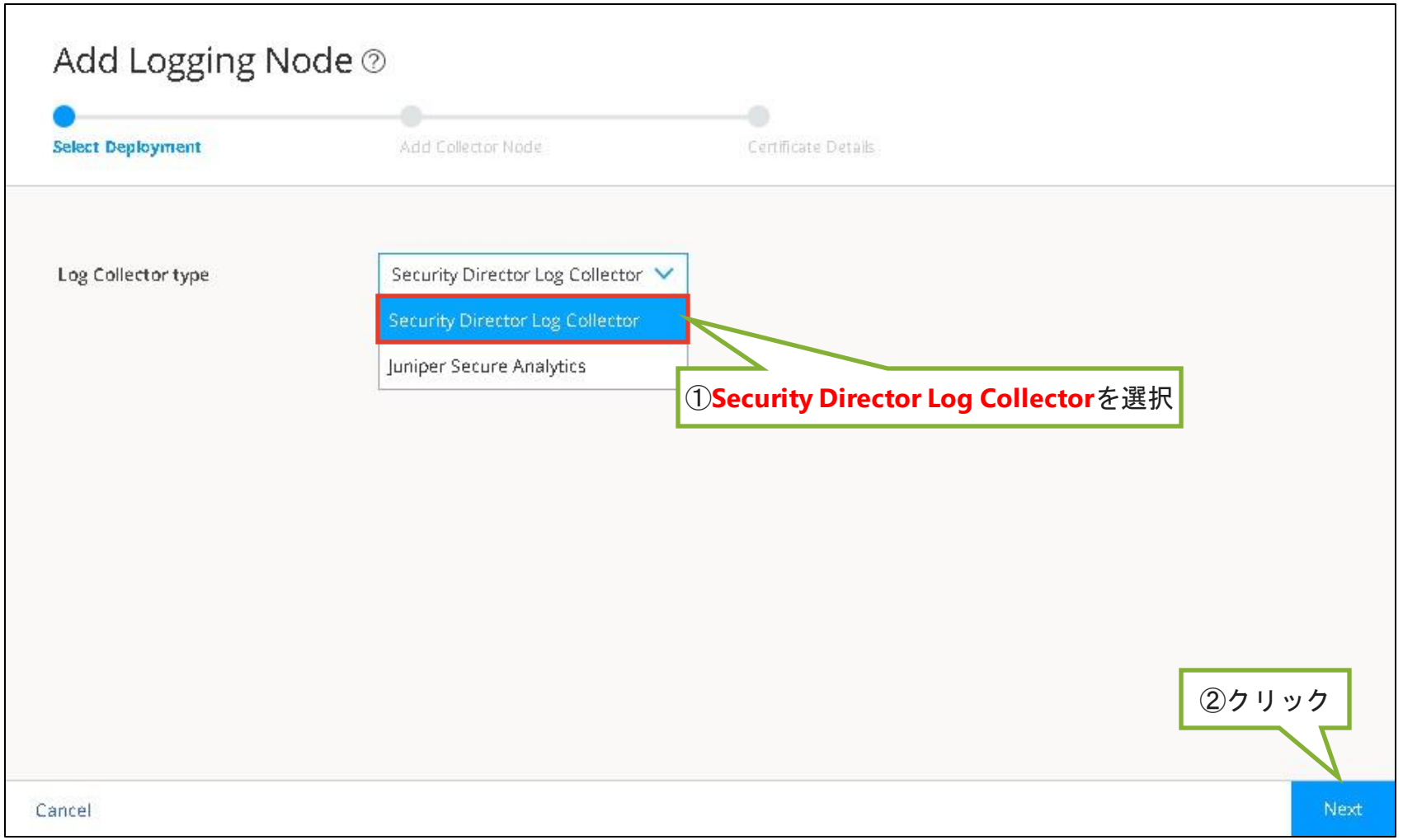
Log Collectorの設定



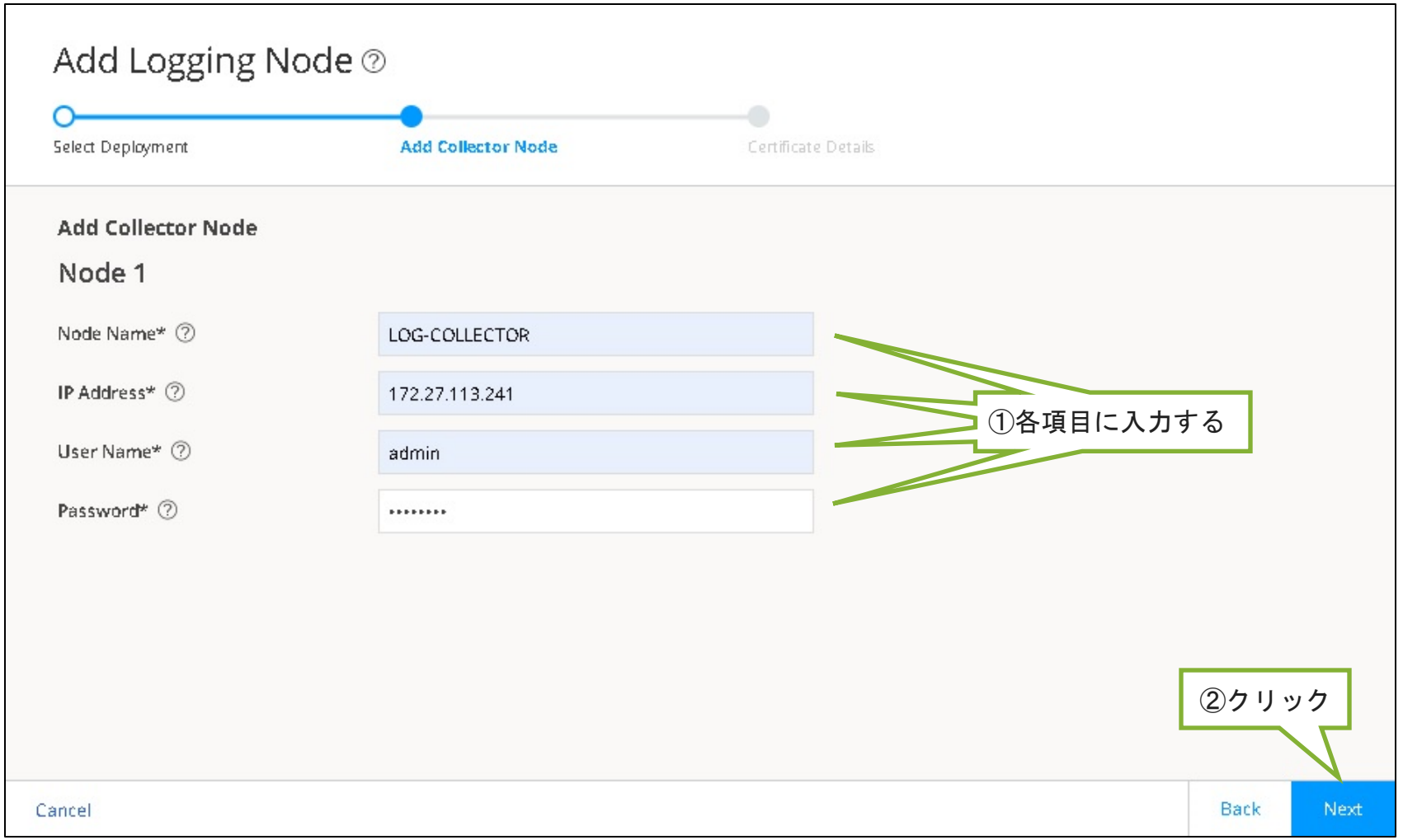
Log Collectorの設定



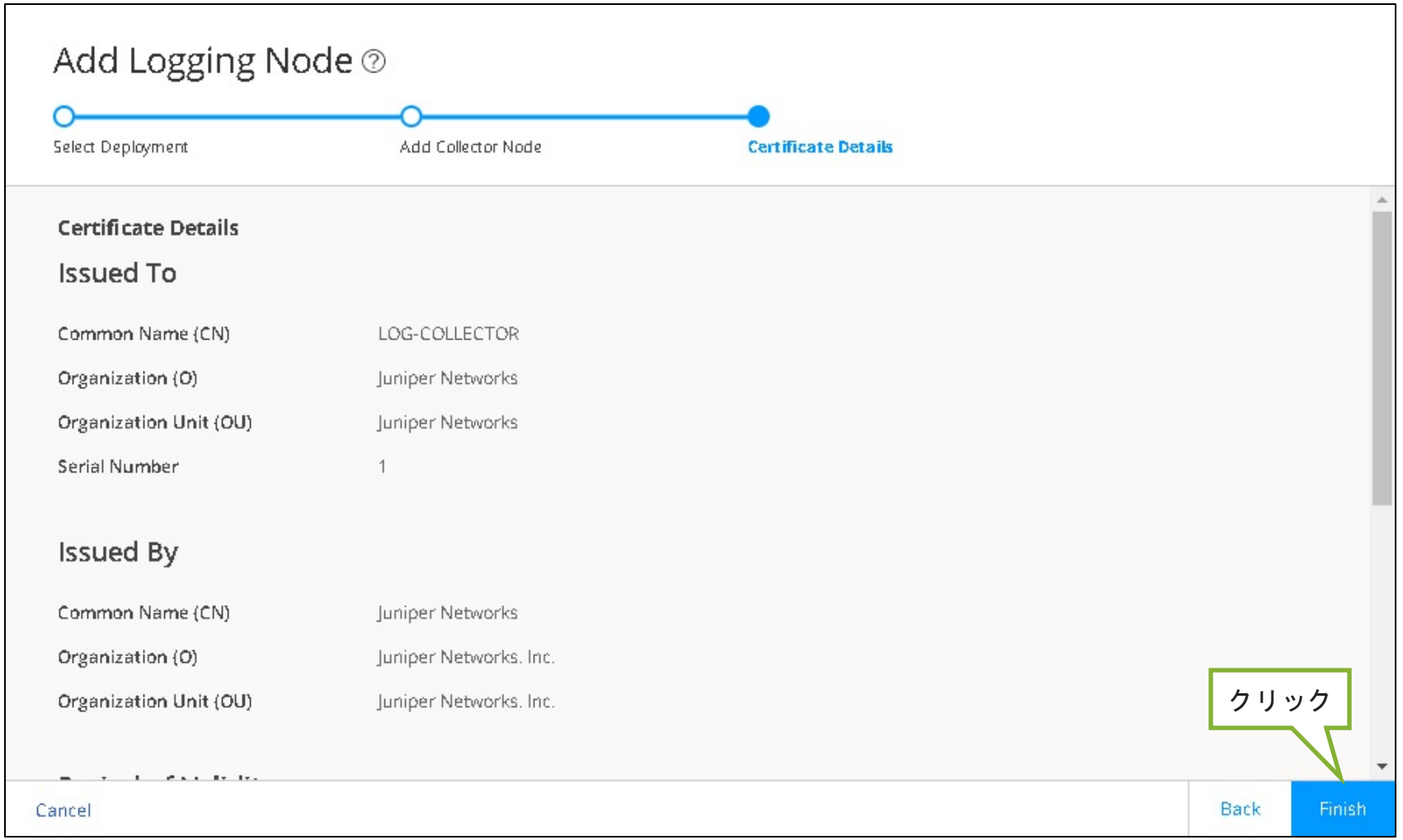
Log Collectorの設定



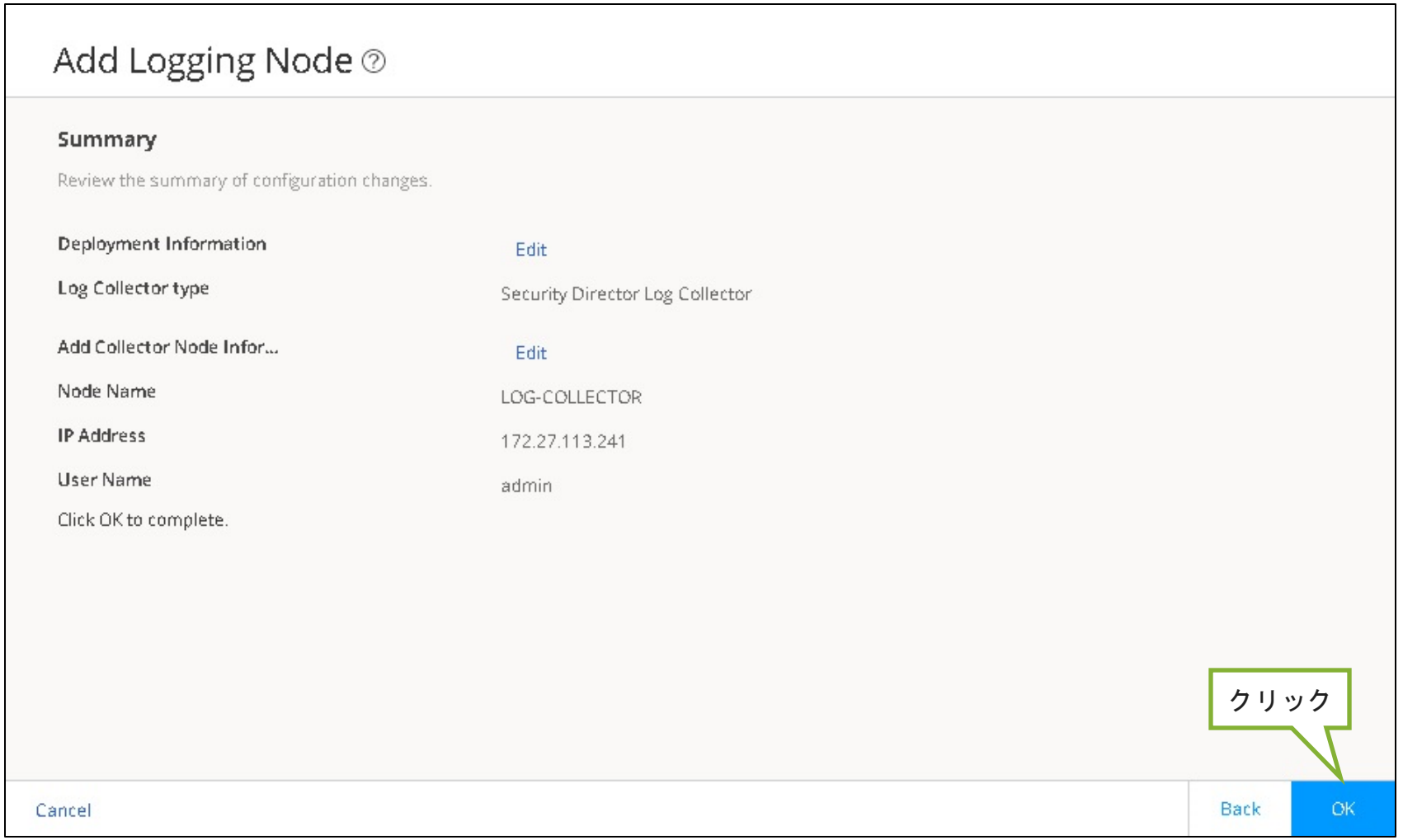
Log Collectorの設定



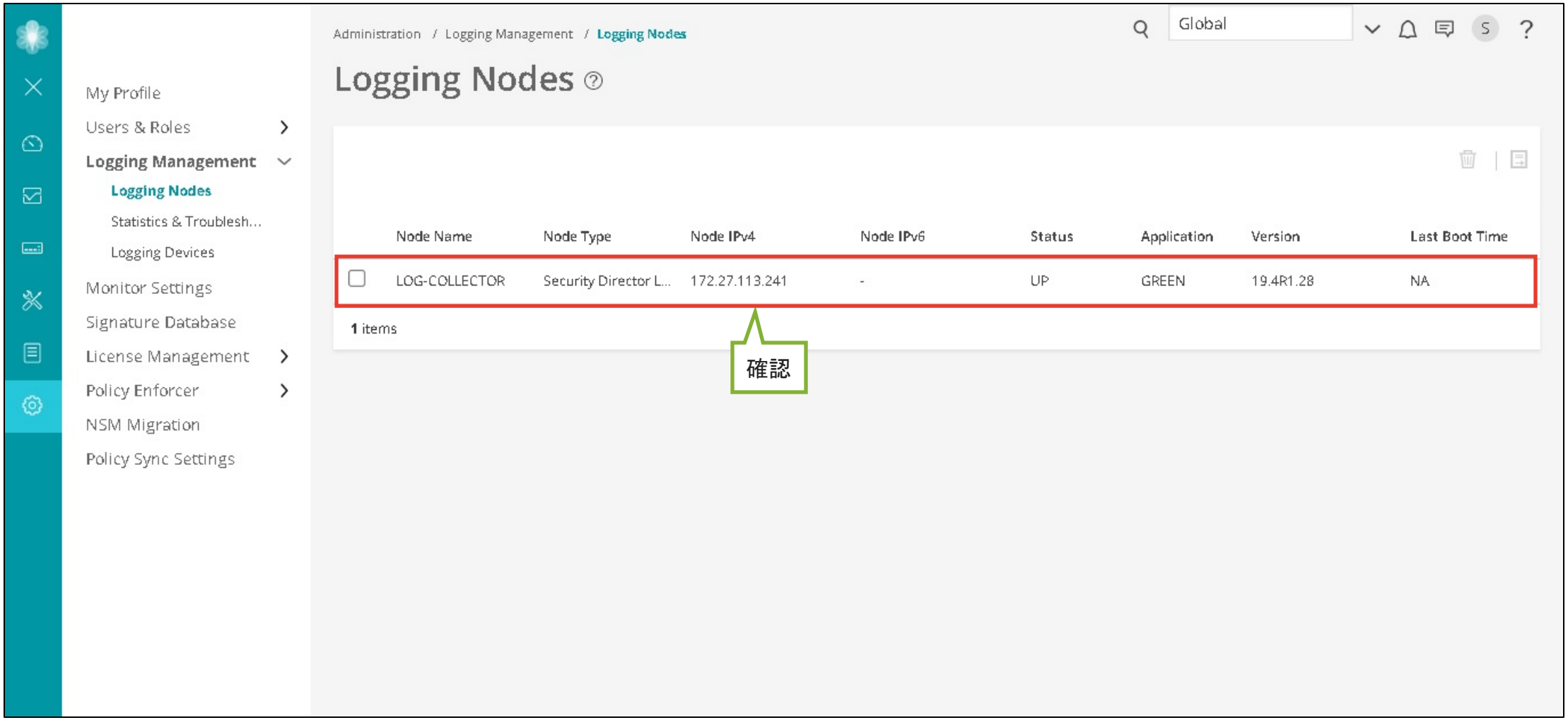
Log Collectorの設定



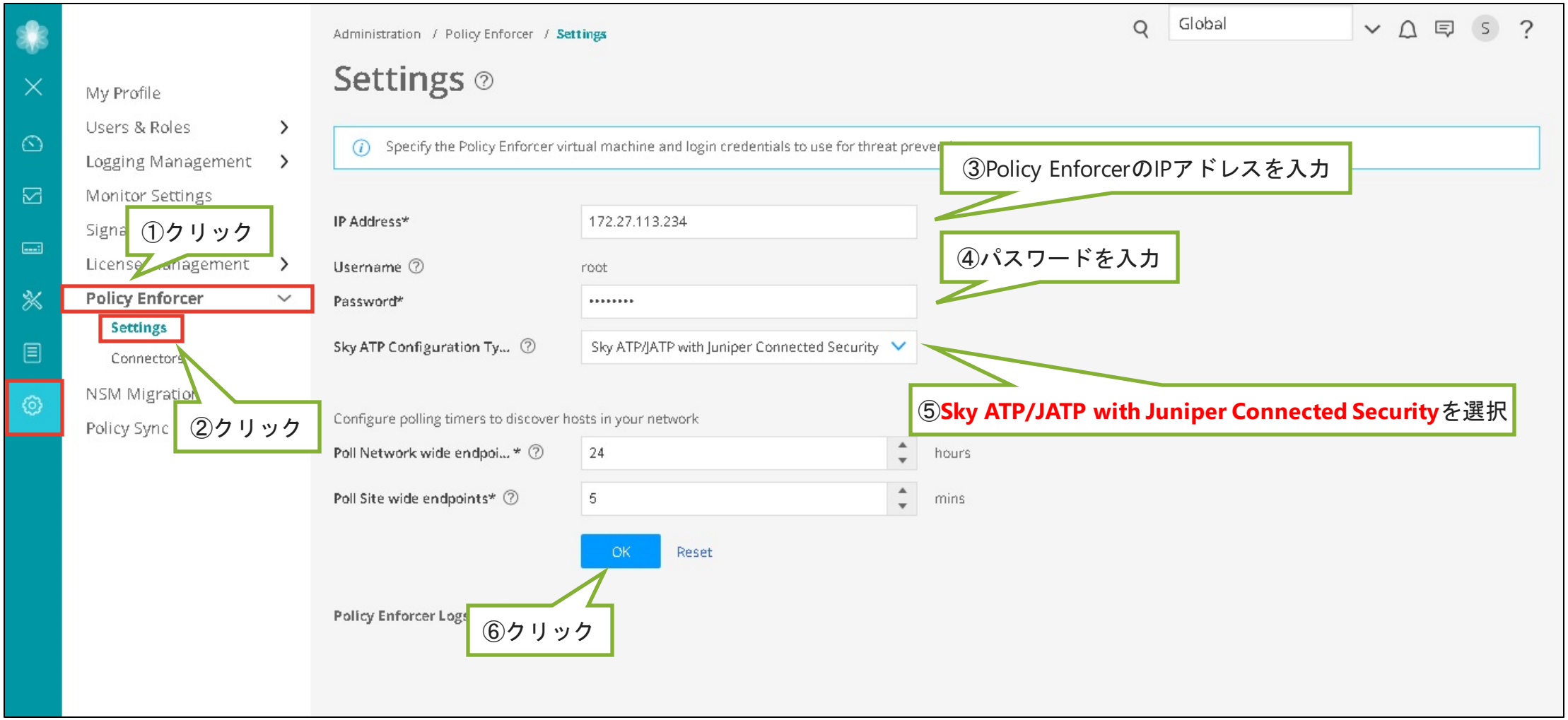
Log Collectorの設定



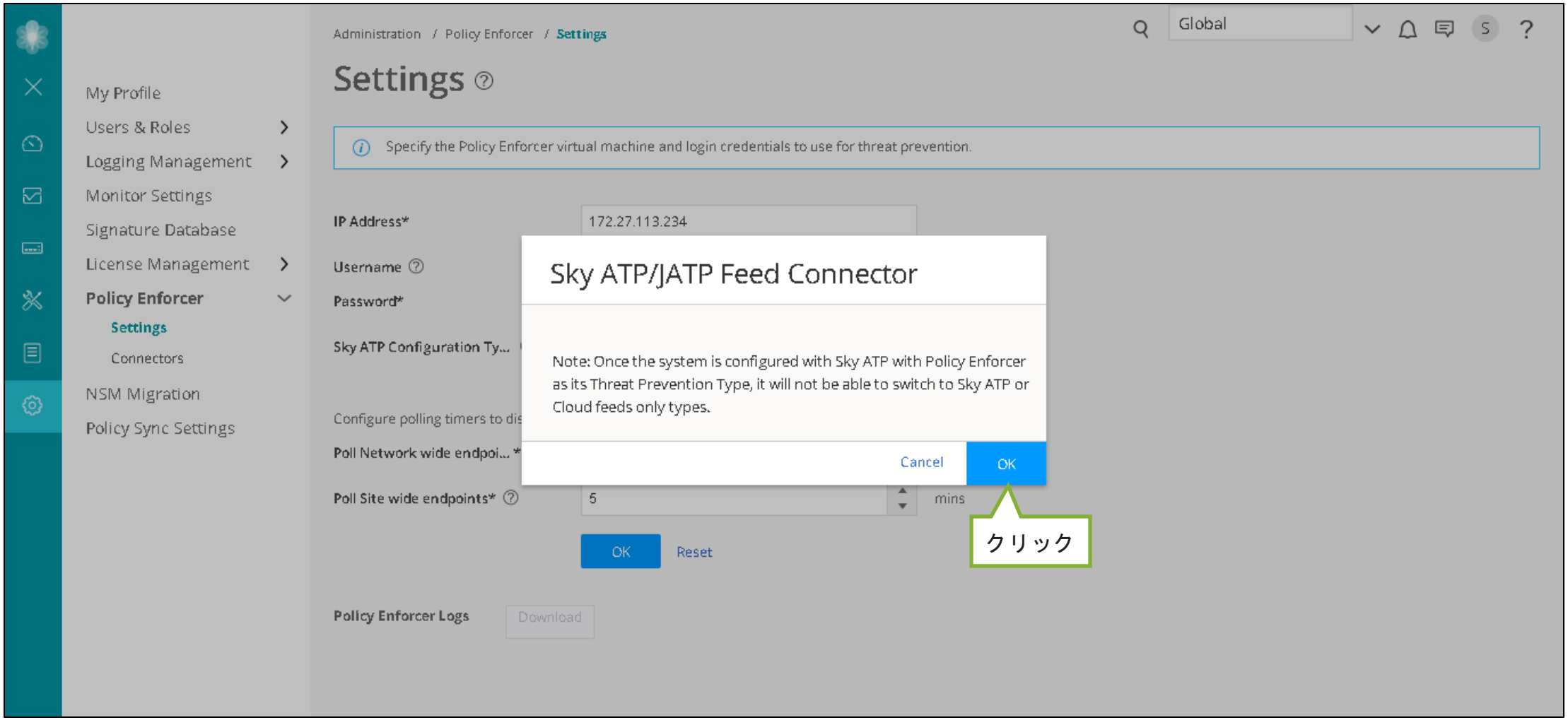
Log Collectorの設定



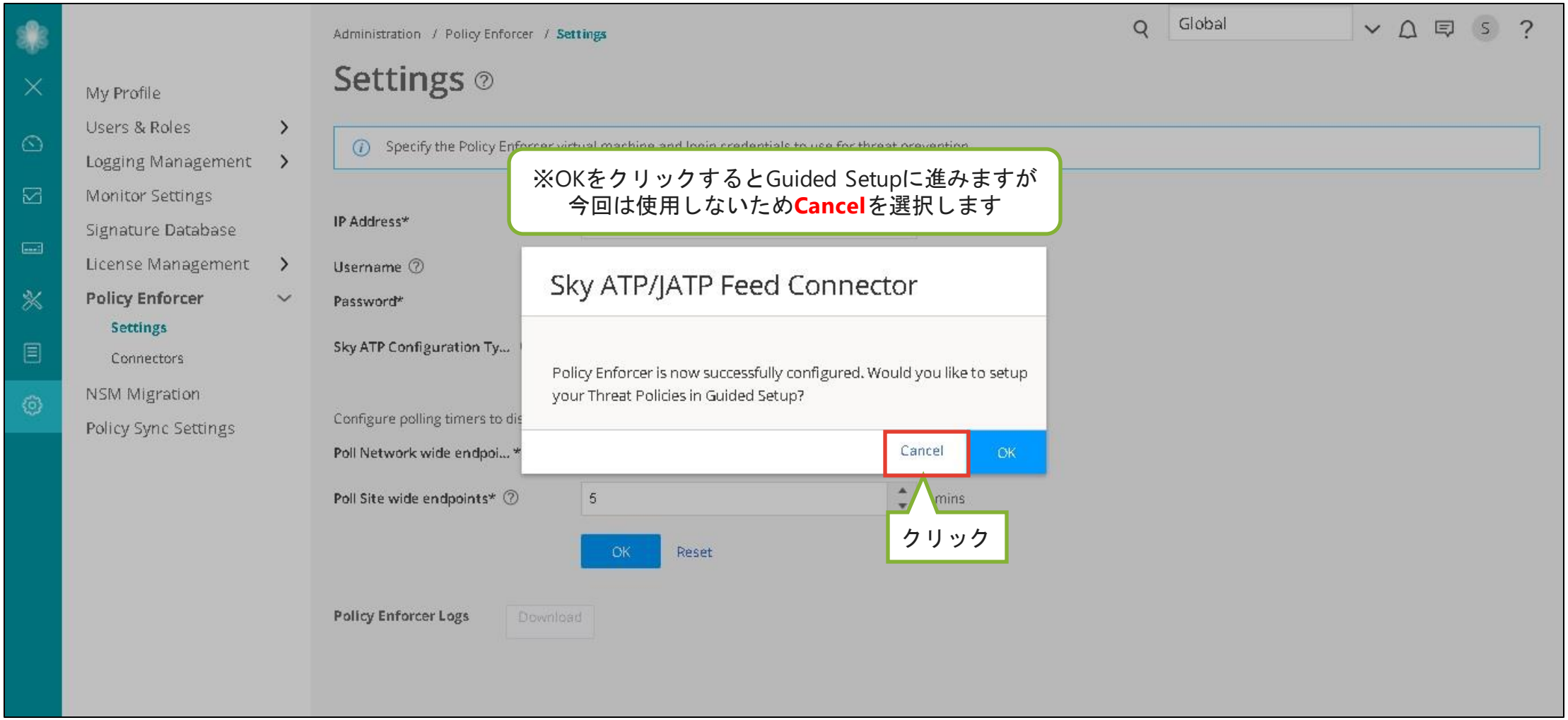
Policy Enforcerの設定



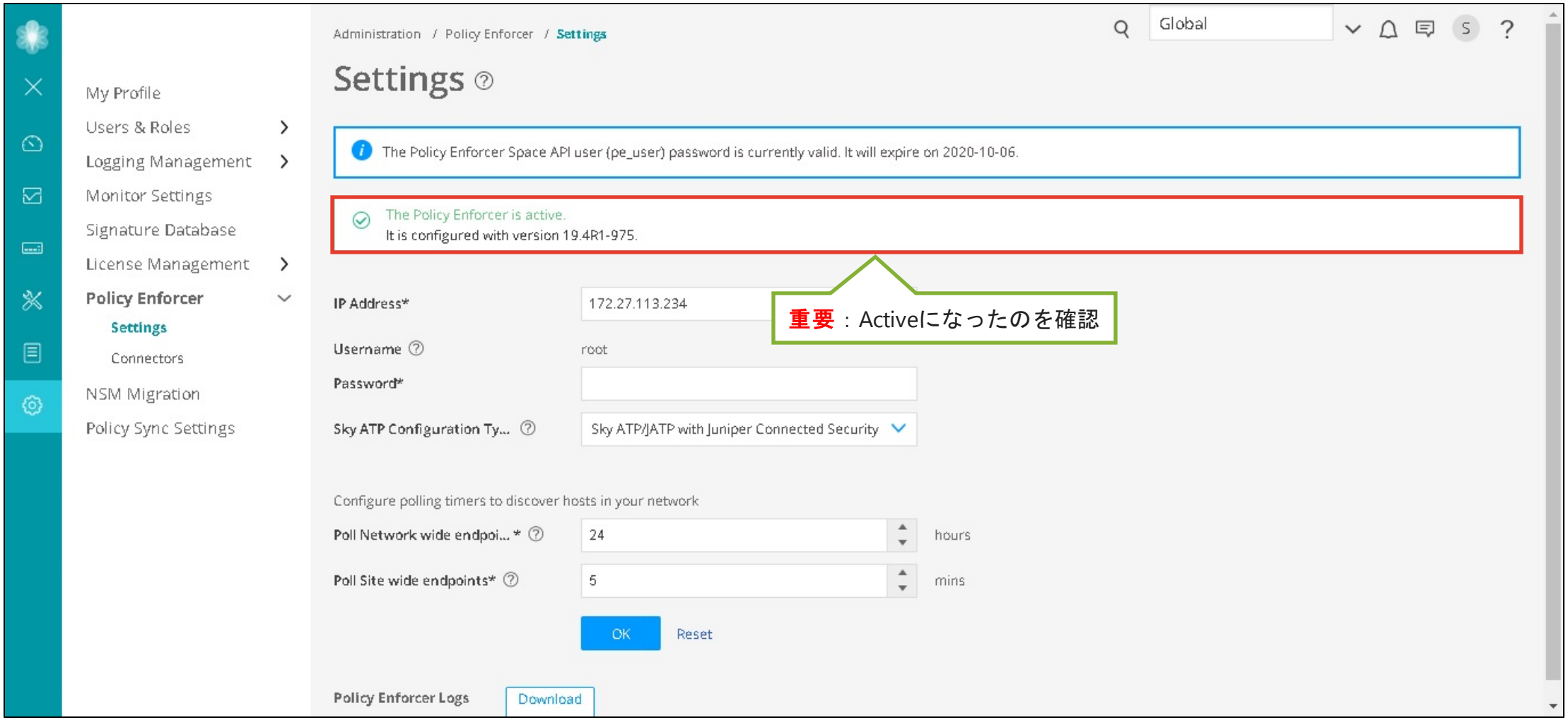
Policy Enforcerの設定



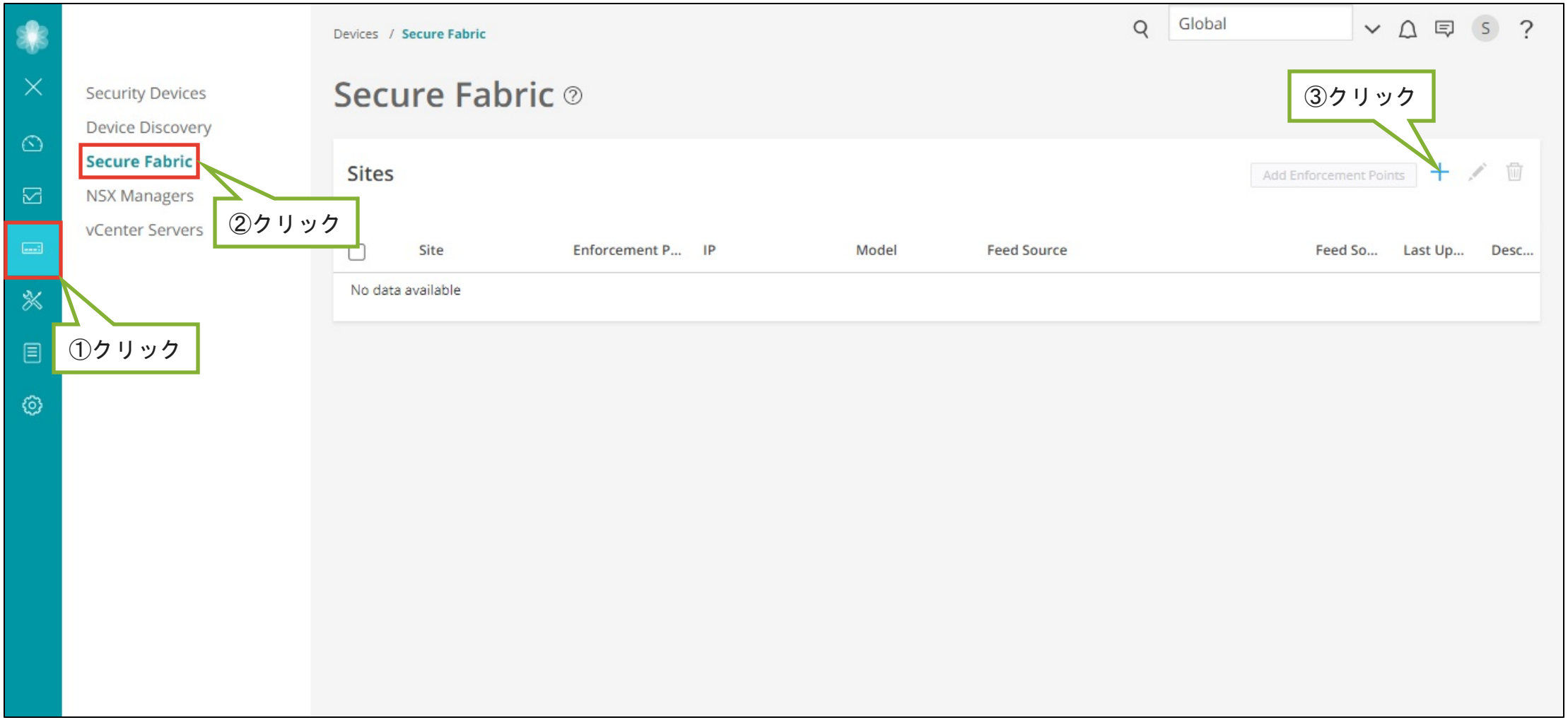
Policy Enforcerの設定



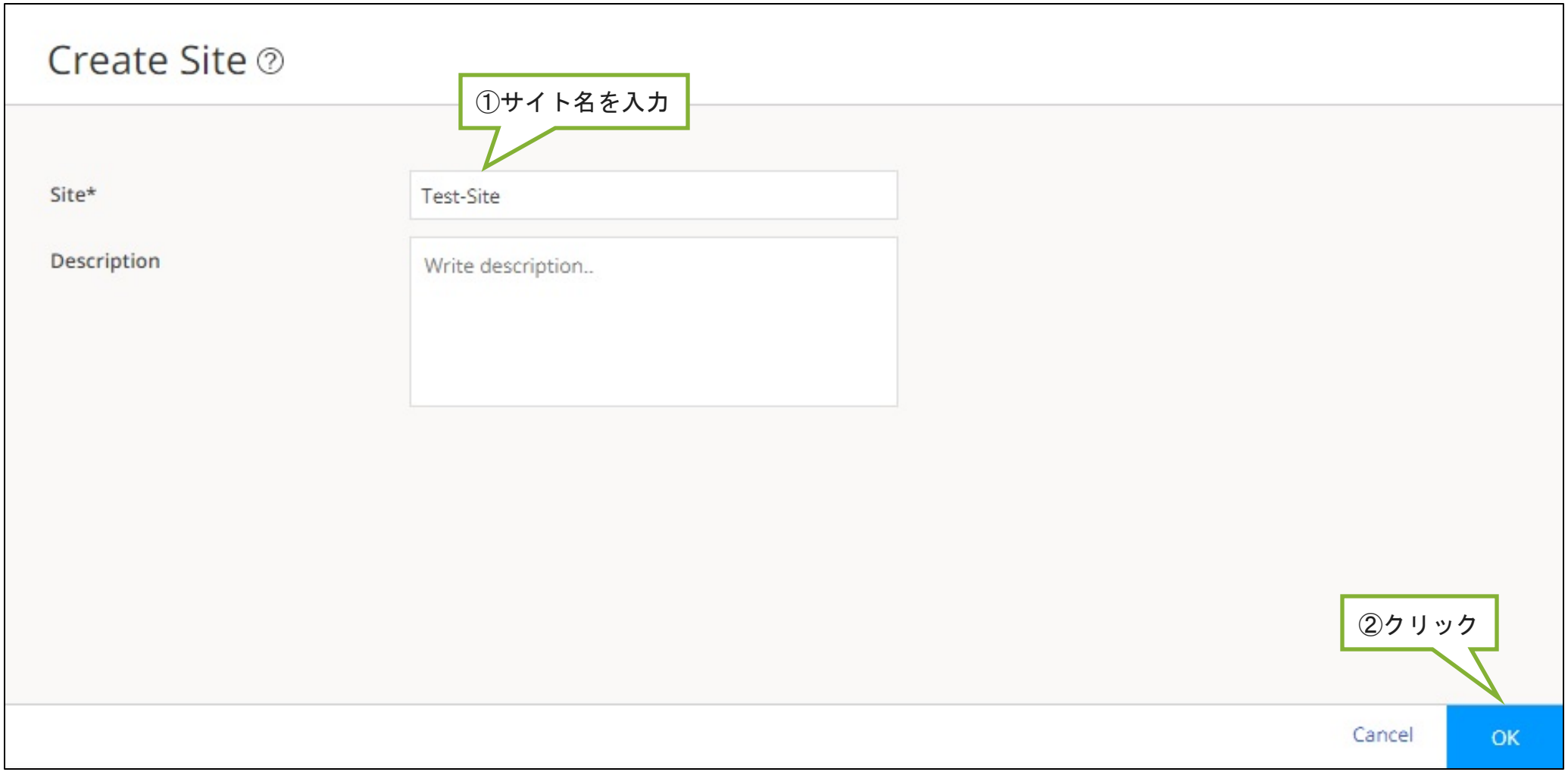
Policy Enforcerの設定



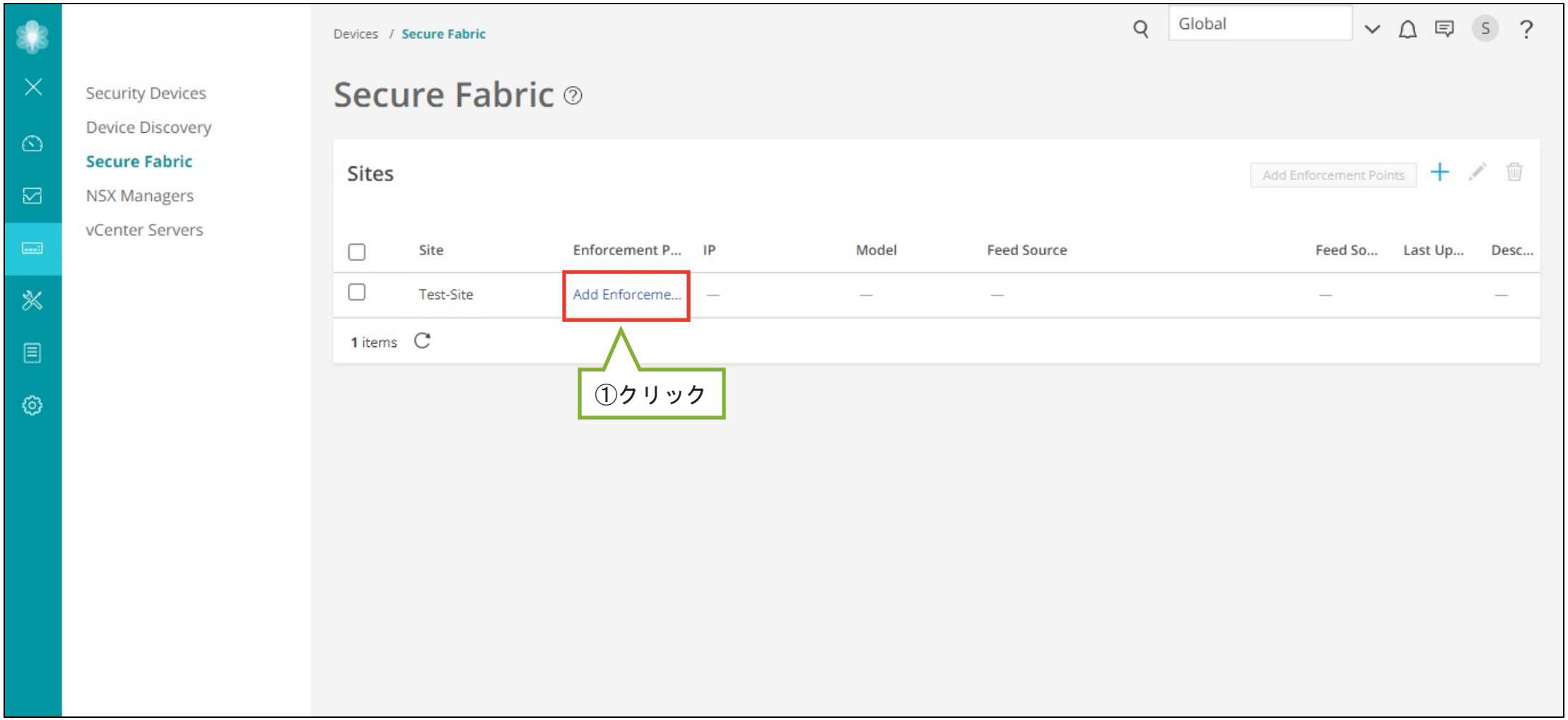
Secure fabricの設定



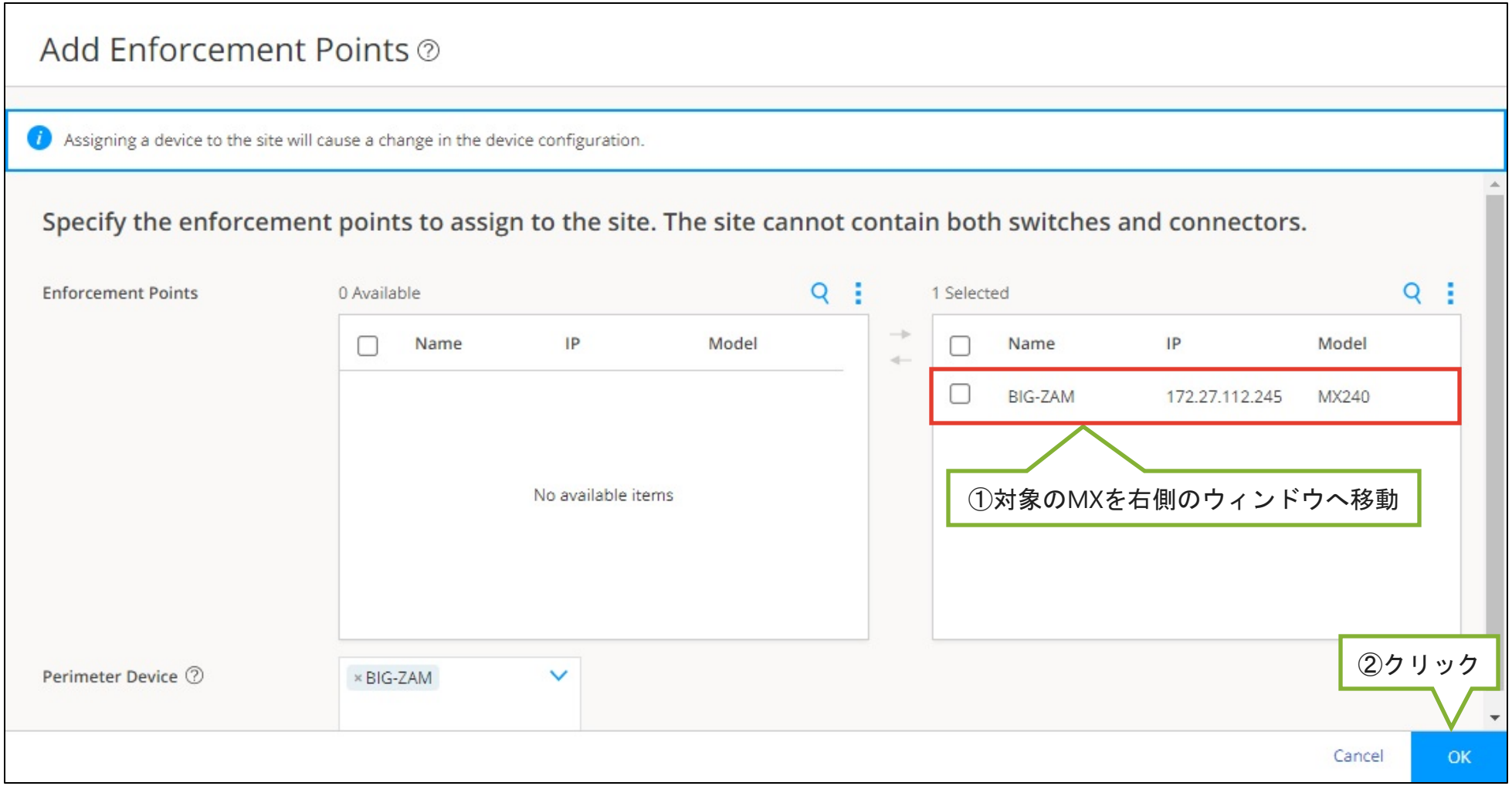
Secure fabricの設定



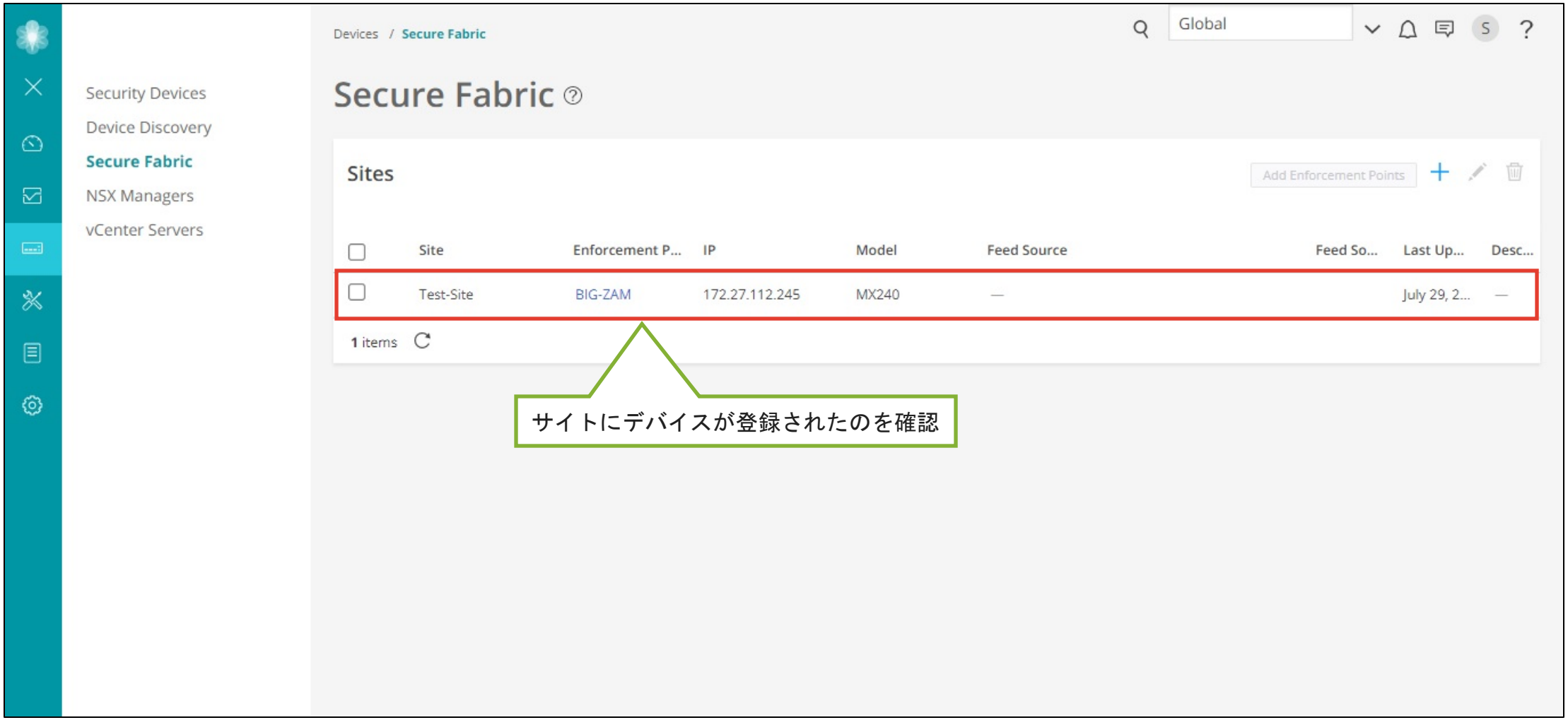
Secure fabricの設定



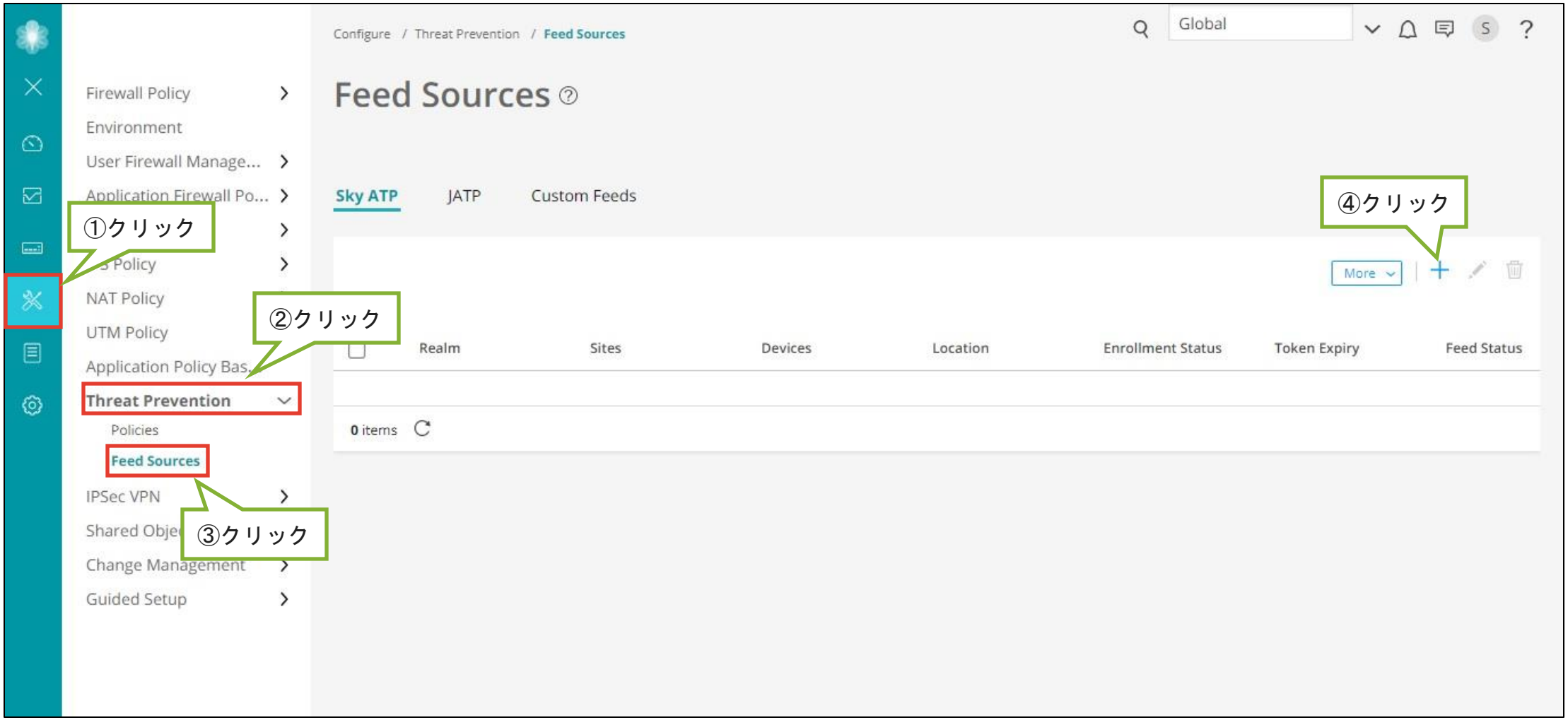
Secure fabricの設定



Secure fabricの設定



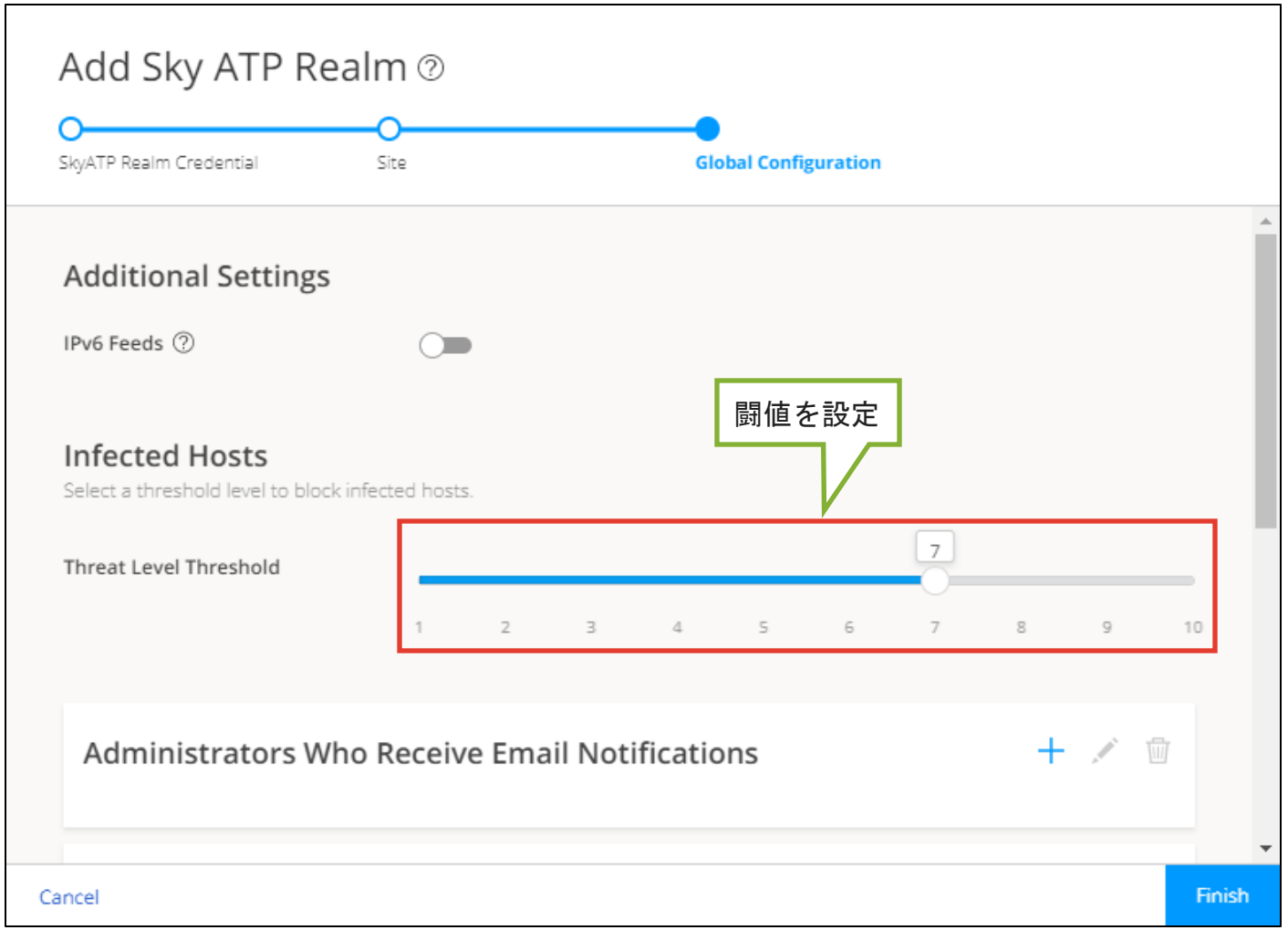
Sky ATPの設定



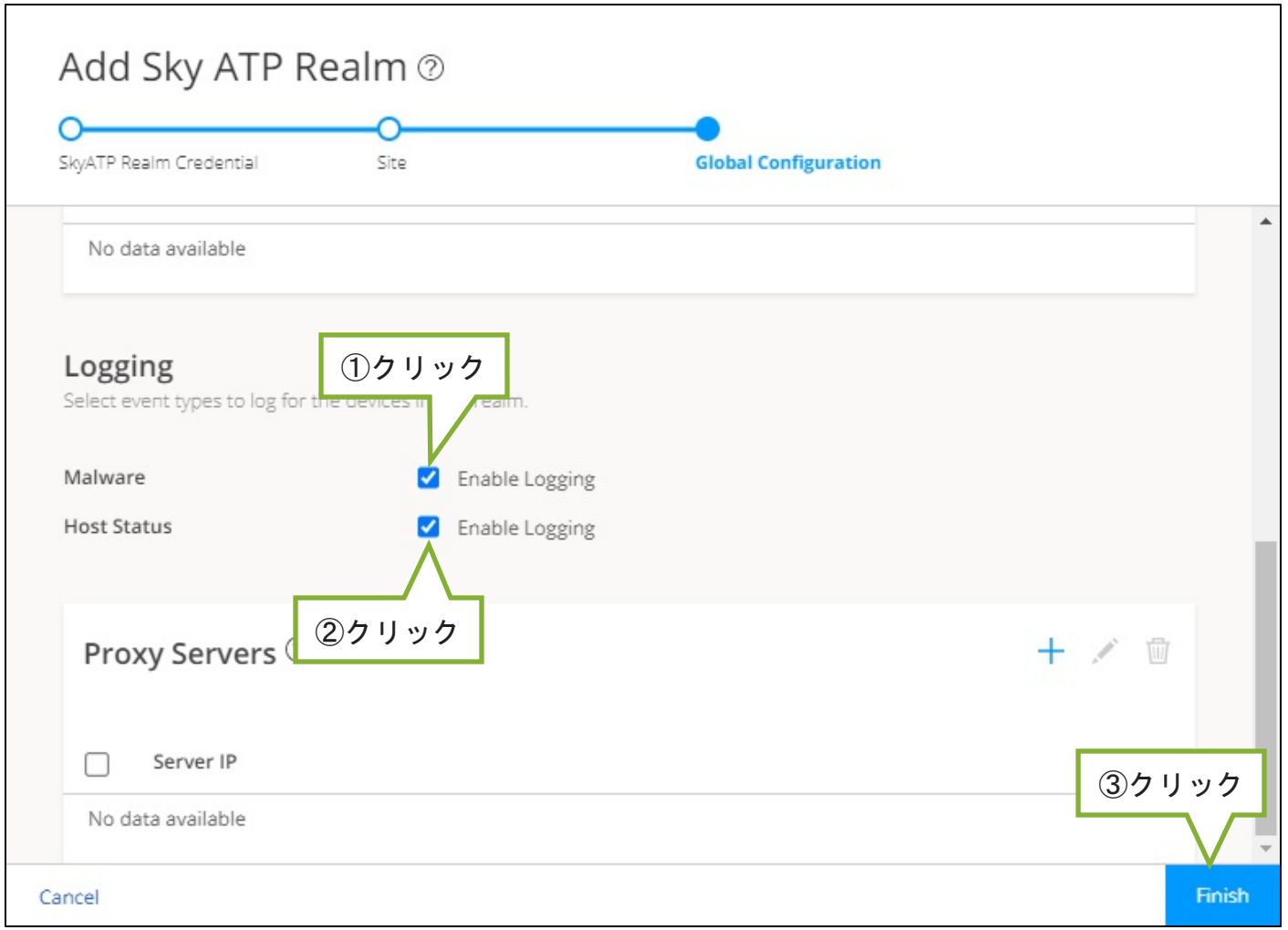
Sky ATPの設定

Sky ATPの設定

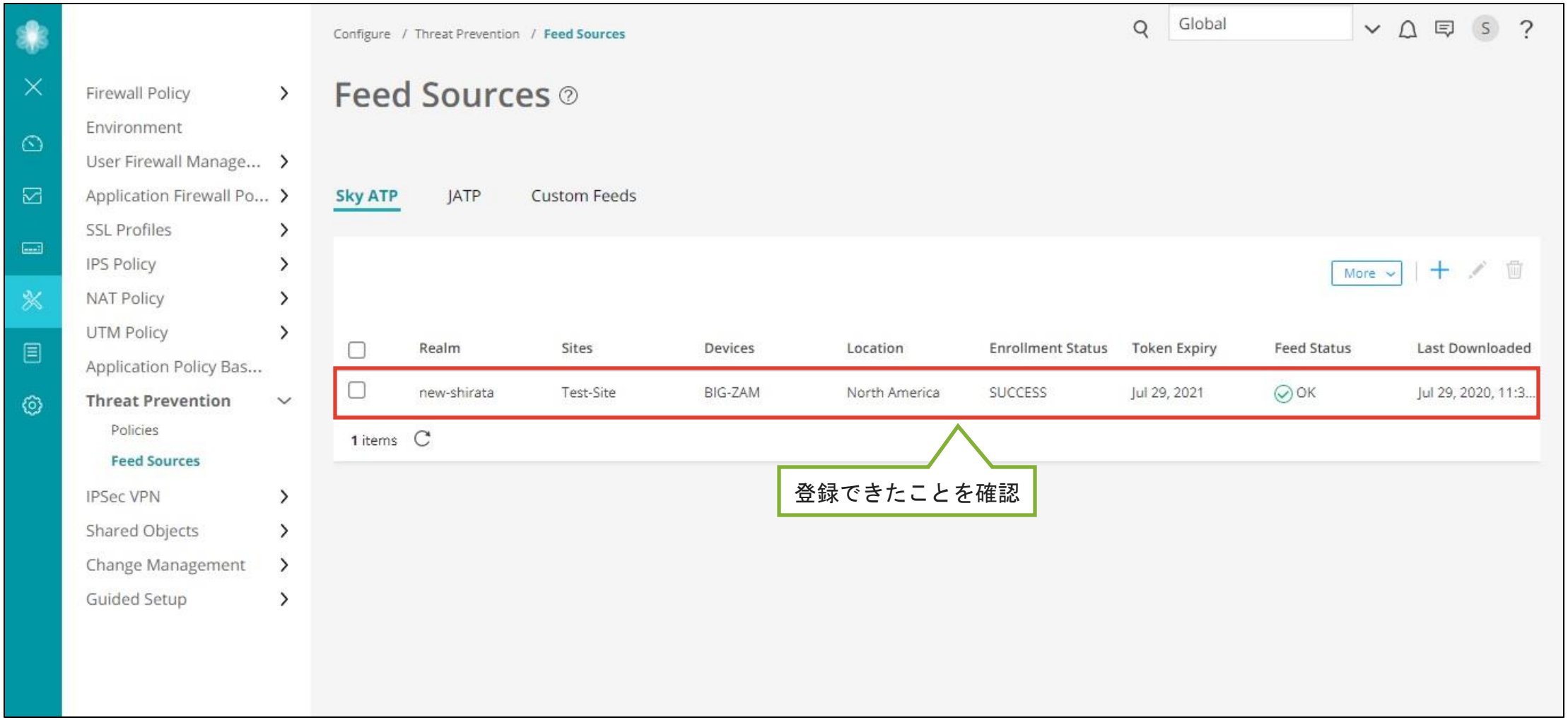
Sky ATPの設定



Sky ATPの設定



Sky ATPの設定



MX設定

MX設定

1. MXがNetConfを受け入れるようにする

```
system {
    services {
        netconf {
            ssh {
                port 830;
            }
        }
    }
}
```

MX設定

2. SecIntelの設定

```
services {
security-intelligence {
        url https://172.27.113.234:443/api/v1/manifest.xml; #Security Directorと連携時に自動入力
        authentication {
            auth-token 6XYNM4KKLPSI16FOC1LYKIDOD2K9GYK0; #Security Directorと連携時に自動入力
        }
        traceoptions {
            file secIntel.log size 1g;
            level all;
            flag feed;
        }
    }
}
```

MX設定

3. URL Filteringの設定

```
services {
    web-filter {
        profile Profile_Name { #任意のプロファイル名
            security-intelligence-policy {
                file-type txt; #txtのみサポート
                threat-level 1 { #threat-levelは1~10の各レベルごとに設定
                    threat-action {
                        accept; #アクションを指定*1
                    }
                }
            }
        }
    }
}

*1 threat-actionはlog、drop、drop-log、accept、log-and-sample、drop-and-sample、drop-log-and-sampleから選択
```

MX設定

4. URL Filter Templateの設定

```
services {
    web-filter {
        profile Profile_Name {
            url-filter-template Template_Name { #任意のテンプレート名
                client-interfaces xe-2/0/0.0; #URLフィルターを適応するインターフェイスを指定
                client-routing-instance inet.0;
            }
        }
    }
}
```

MX確認コマンド一例

MX確認コマンド一例

- Security-Intelligenceの概要の確認

```
> show services security-intelligence category summary

Category name      :CC
  Status           :Enable
  Description      :Command and Control data schema
  Update interval  :1800s
  TTL              :3456000s
  Feed name        :cc_ip_data
    Version        :20200723.4
    Objects number:144238
    Create time    :2020-07-29 12:44:12 JST
    Update time    :2020-07-29 13:06:49 JST
    Update status  :Store succeeded
    Expired        :No
    Options        :N/A
```

MX確認コマンド一例

- Security-Intelligenceの更新ステータスの確認

```
> show services security-intelligence update status

Current action         :Checking update interval of category CC.
Last update status     :Update interval of category CC is not reached.
Last connection status:succeeded
Last update time       :2020-07-29 13:22:04 JST
```

MX確認コマンド一例

- Policy Enforcerから受信した脅威レベルごとのフィルター数及びフィルターの保存場所の確認

```
> show services web-filter secintel-policy-status summary profile Profile_Name

URL Filtering SecIntel Policy Status:
Profile     : Profile_Name
C&C DB File : /var/db/url-filterd/urlf_si_cc_db.txt*1
Policy State: Ready
DB File Change Time : Wed Jul 29 12:28:18 2020
DB File Load Time   : Wed Jul 29 12:28:19 2020
C&C Prefix Count    : IPv4: 144238     IPv6: 0
Filters:
Threat level   Action              v4 Term Count    IPv4        v6 Term Count   IPv6

1              ACCEPT              192              57595       0               0
2              ACCEPT              26               7597        0               0
3              ACCEPT              4                1044        0               0
4              ACCEPT              4                1082        0               0
5              ACCEPT              5                1254        0               0
6              ACCEPT              170              50913       0               0
7              ACCEPT              5                1370        0               0
8              ACCEPT              5                1498        0               0
9              ACCEPT              4                971         0               0
10             ACCEPT              4                1119        0               0

*1 Secure Fabric上でSky ATPにサイトを登録すると、Sky ATPからC&C DBファイルをPolicy Enforcerへプッシュされ MXがそれを取得する
```


Thank you
JUNIPER NETWORKS
Engineering
Simplicity