

Catalyst SD-WANでのSNMPv3の設定

内容

[はじめに](#)

[背景](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[確認](#)

[参考資料](#)

はじめに

このドキュメントでは、SNMPv3の設定について説明し、セキュリティ（認証）、暗号化（プライバシー）、および制限（表示）について説明します。

背景

多くの場合、SNMPv3の設定は複雑で設定が困難なため、何を行う必要があるかわかるまで行いません。SNMPv3が存在する理由は、セキュリティ、暗号化、および制限の点でHTTPSと似ています。

前提条件

SD-WAN機能テンプレートおよびデバイステンプレートに関する知識。

SNMP MIB、SNMPポーリング、およびSNMPウォークに関する一般的な知識

要件

SD-WANコントローラ

Ciscoエッジルータ

使用するコンポーネント

20.9上のSD-WANコントローラ

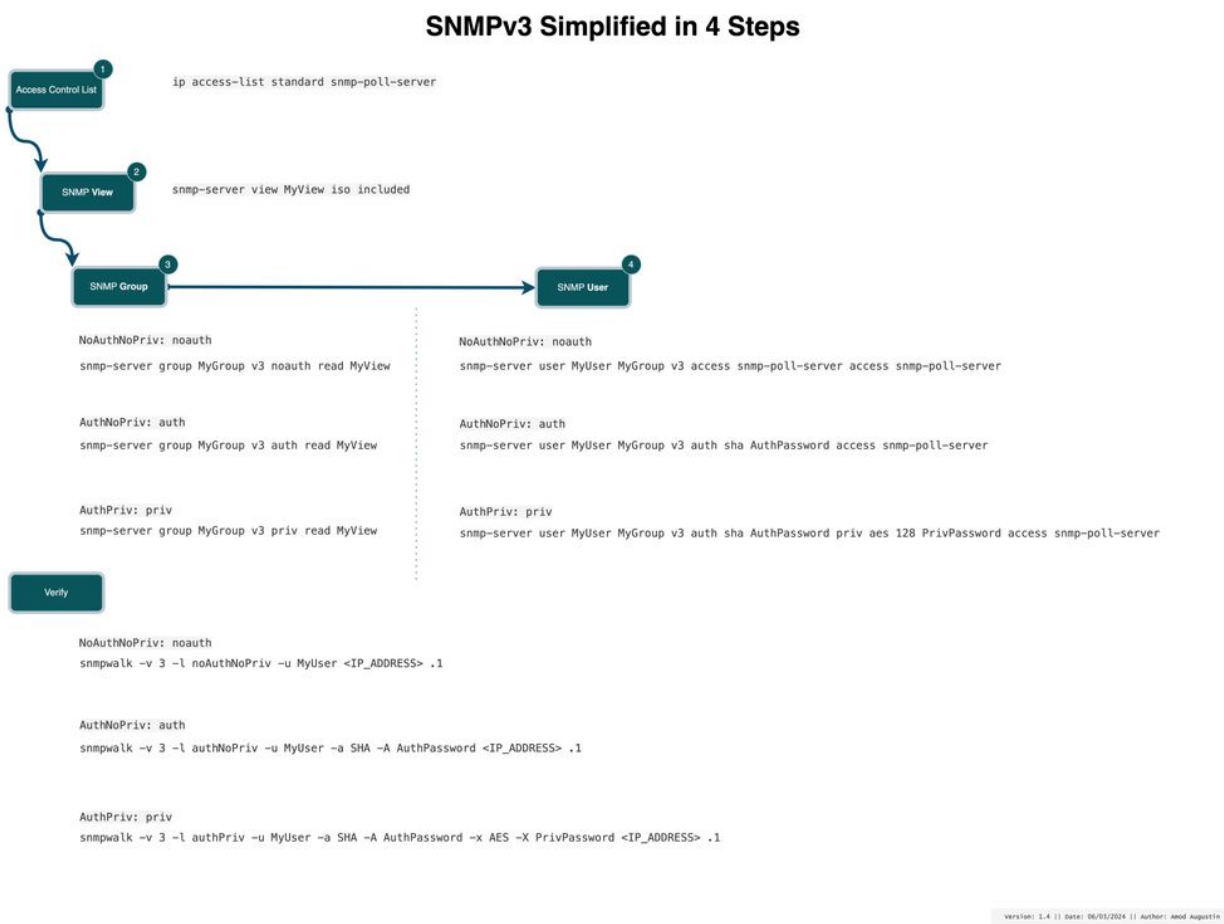
17.9上のCiscoエッジルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

この図は、CLIの観点からSNMPv3を設定するために必要なすべての要件を理解するのに役立ちます。



SNMPv3は4つのステップで簡素化

概念をCLIまたは機能テンプレートに簡単に適用できることを理解したら、さあ、飛び込もう。

ステップ 1 :

システムをポーリングできるユーザ (この例ではルータ) を許可するようにACLを設定します。

```
ip access-list standard snmp-poll-server
```

ステップ 2 :

SNMPビューを定義します。この用語はポーリング側がアクセスできるMIBを示しているので、これは制限事項です。

```
snmp-server view MyView iso included
```

ステップ 3 :

snmpグループを定義します。snmpグループは主に2つの部分で構成されます。a.セキュリティレベルb.制限 (ビュー)。

セキュリティ レベル:

- noAuthNoPriv: 認証およびプライバシーなし (暗号化なし)。
- authNoPriv : 認証は必要ですが、プライバシーはありません。
- authPriv : 認証とプライバシーの両方が必要です。

制約事項はステップ2で定義したものです。最後に、これらをまとめます。

```
!NoAuthNoPriv: noauth  
snmp-server group MyGroup v3 noauth read MyView
```

```
!AuthNoPriv: auth  
snmp-server group MyGroup v3 auth read MyView
```

```
!AuthPriv: priv  
snmp-server group MyGroup v3 priv read MyView
```

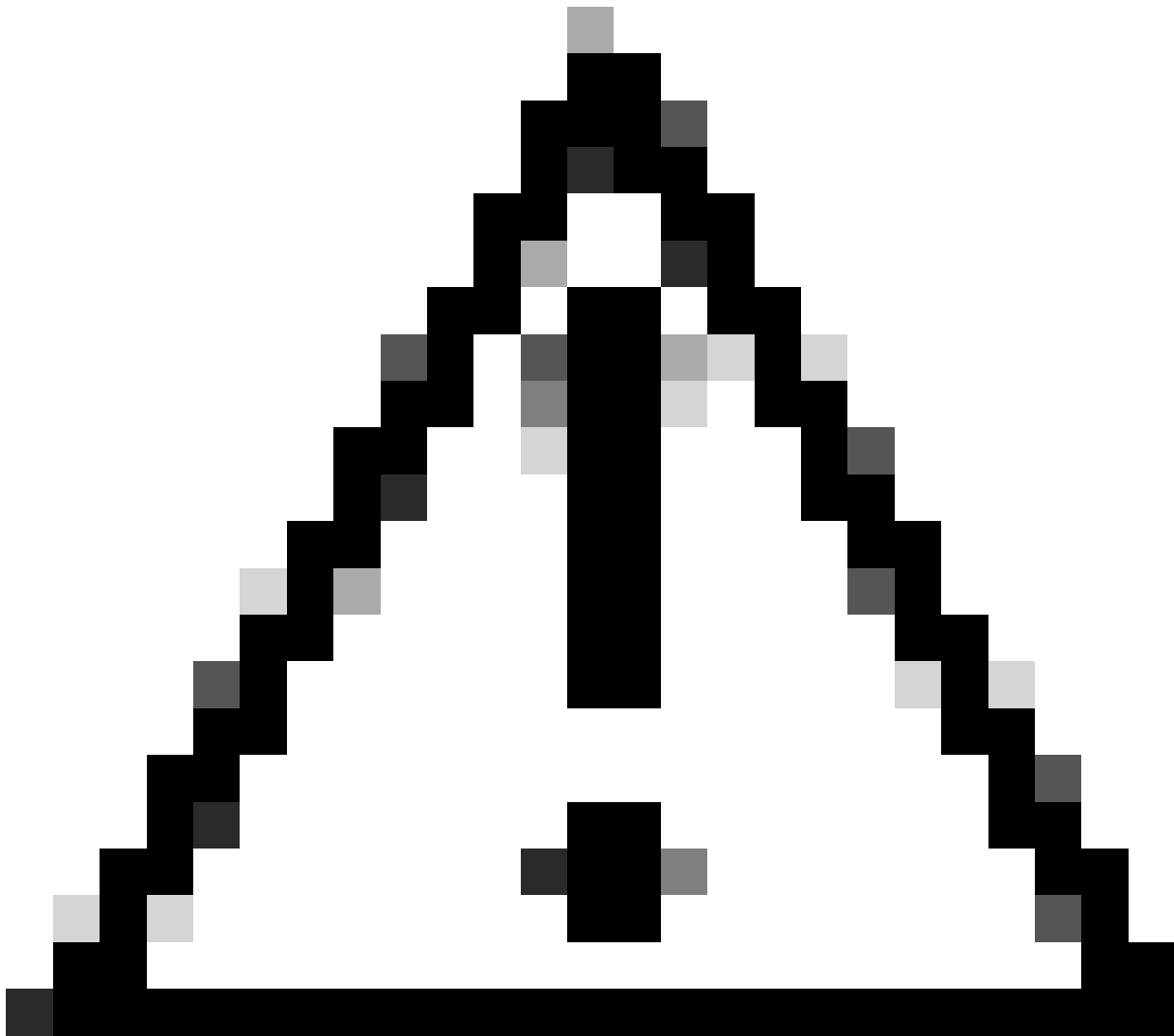
ステップ 4 :

このステップでは、グループをユーザに関連付け、各グループをそれぞれの認証とプライバシー (暗号化) を定義するユーザに関連付け、アクセスコントロールリストを使用してさらにセキュリティを強化できます。

```
!NoAuthNoPriv: noauth  
snmp-server user MyUser MyGroup v3 access snmp-poll-server
```

```
!AuthNoPriv: auth  
snmp-server user MyUser MyGroup v3 auth sha AuthPassword access snmp-poll-server
```

```
!AuthPriv: priv  
snmp-server user MyUser MyGroup v3 auth sha AuthPassword priv aes 128 PrivPassword access snmp-poll-server
```



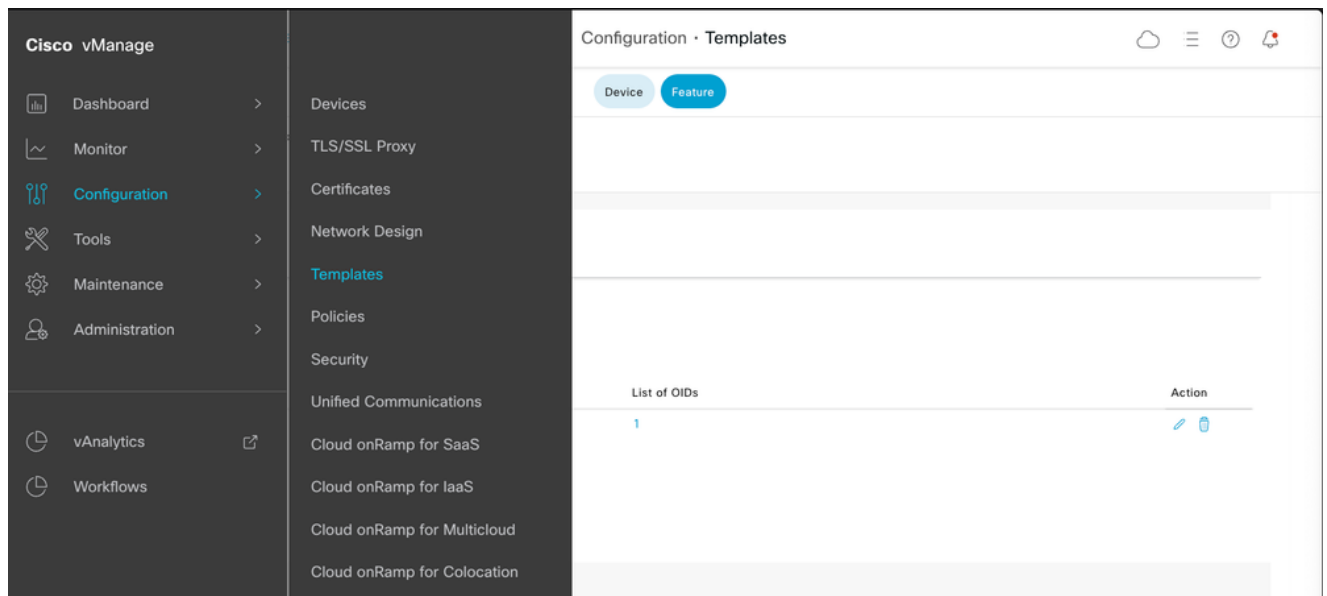
注意:snmp-server userを設定しようとしても、コンテキストヘルプは利用できず、実行コンフィギュレーションにも表示されません。これはRFC 3414に準拠するためです。完全なコマンドを入力すると、パーサーは設定を受け入れます

cEdge-RT01(config)# snmp-server user ? ^ % Invalid input detected at '^' marker.

Cisco Bug ID [CSCvn71472](#)

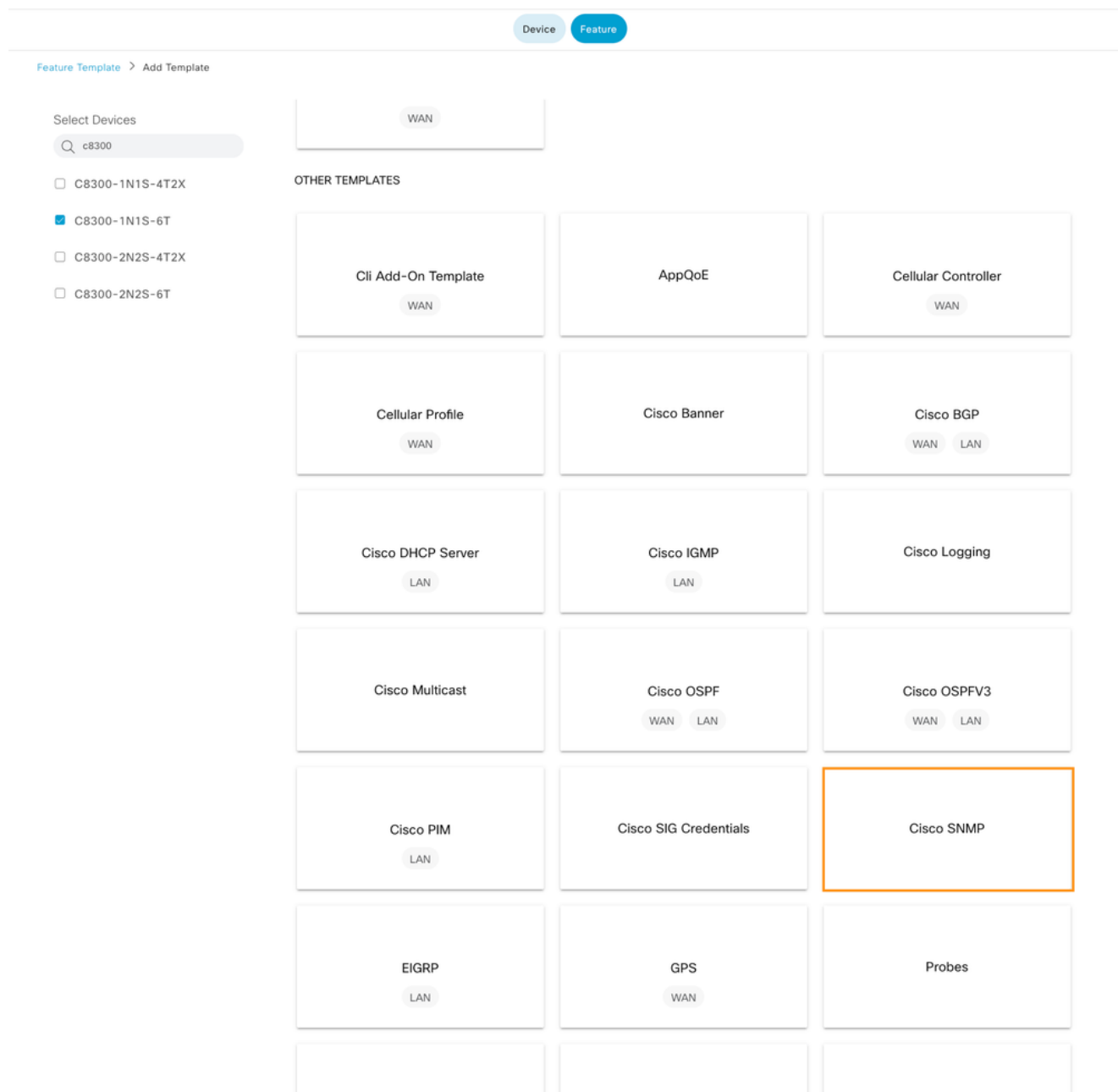
おめでとうございます。以上が必要なことです。CLIとその概念を理解したので、次にCatalyst SD-WAN ManagerでSNMP機能テンプレートを使用して設定する方法を説明します

Cisco vManage > Configuration > Templates > Featureの順に選択します



機能テンプレート

Other TemplateセクションにあるCisco SNMPに移動します



SNMP機能

SNMPビュー (制限) を定義します。これがステップ2です。

Device TypeC8300-1N1S-6T

Template NameCisco_SNMPv3

DescriptionCisco_SNMPv3

SNMP

SNMP Version

SNMP

Shutdown

Yes

No

Contact Person

Location of Device

SNMP VERSION

SNMP Version

V2

V3

VIEW & GROUP

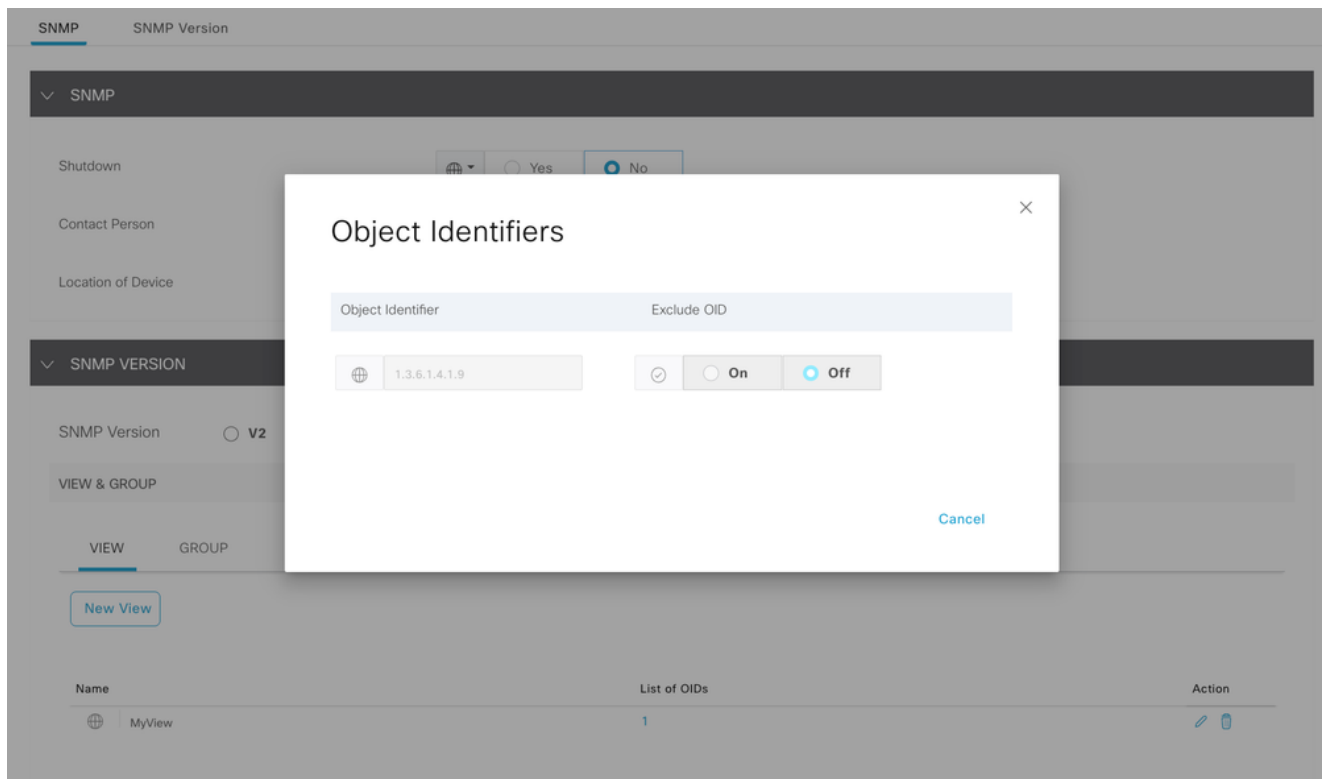
2

VIEWGROUP

New View

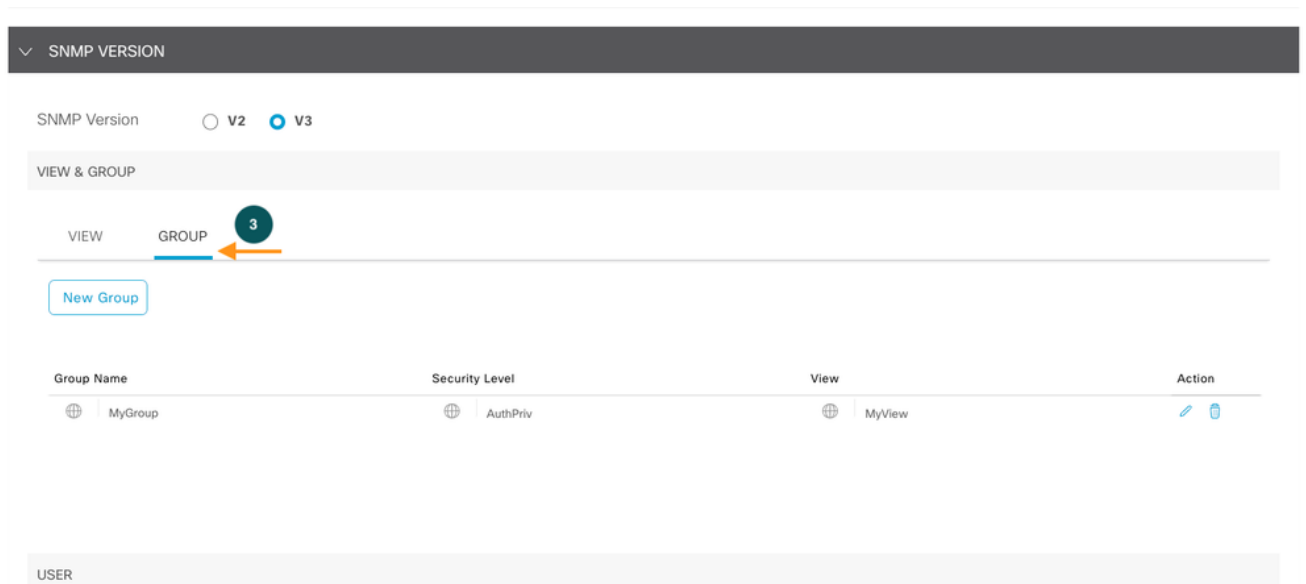
Name	List of OIDs	Action
MyView	1	

SNMP ビュー



SNMP OID(SNMP OID)

SNMPグループを定義します。これがステップ3です。



SNMPグループ

3 Update Group

Name

Security Level

View

Save Changes Cancel

SNMPグループ

ユーザグループを定義します。これは、認証および暗号化パスワードを定義するステップ4です。

Feature Template > Cisco SNMP > Cisco_SNMPv3

SNMP SNMP Version

VIEW GROUP

New Group

Group Name	Security Level	View	Action
MyGroup	AuthPriv	MyView	

USER

New User 4

Username	Authentication Type	Authentication Password	Privacy Type	Privacy Password	Action
MyUser	SHA		AES-CFB-128		
MyGroup					

SNMPユーザ

4

Update User

User

MyUser

Authentication Protocol

SHA

Authentication Password

.....

Privacy Protocol

AES-CFB-128

Privacy Password

.....

Group

MyGroup

Save Changes

Cancel

• TARGET SERVER

SNMPユーザ暗号化



注:SNMPグループのセキュリティレベルに基づいて、ユーザに関連付けられているそれぞれのフィールドが有効になります。

次に、デバイステンプレートに機能テンプレートをアタッチします。

Device

Feature

Basic Information

Transport & Management VPN

Service VPN

Cellular

Unified Communication

Additional Templates

Switchport

Additional Templates

AppQoS	Choose...
Global Template *	Factory_Default_Global_CISCO_Templ... ⓘ
Cisco Banner	Choose...
Cisco SNMP	Cisco_SNMPv3
ThousandEyes Agent	Choose...
TrustSec	Choose...
CLI Add-On Template	Choose...
Policy	Choose...
Probes	Choose...
Security Policy	Choose...

SNMP機能テンプレート

確認

```
Router#show snmp user
```

```
User name: MyUser
Engine ID: 800000090300B8A3772FF870
storage-type: nonvolatile    active    access-list: snmp-poll-server
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: MyGroup
```

snmpwalkがインストールされているマシンから、コマンドを実行して、各セキュリティレベルのSNMP応答を確認できます

```
!NoAuthNoPriv: noauth
snmpwalk -v 3 -l noAuthNoPriv -u MyUser
```

.1

```
!AuthNoPriv: auth
snmpwalk -v 3 -l authNoPriv -u MyUser -a SHA -A AuthPassword
```

.1

```
!AuthPriv: priv
```

```
snmpwalk -v 3 -l authPriv -u MyUser -a SHA -A AuthPassword -x AES -X PrivPassword
```

.1

-v : バージョン(3)

-l : セキュリティレベル

-A : 認証プロトコルパスフレーズ

-X : プライバシープロトコルパスフレーズ

参考資料

- [CiscoエッジルータでのSNMPv3トラップの設定](#)
- Tim Glen [によるSNMPv3の設定テンプレート](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。