

# Tenable と ServiceNow の統合ガイド

最終更新日: 2月 18, 2026



## 目次

Tenable for ServiceNow へようこそ .....	3
アプリケーションの依存関係 .....	3
アプリケーションのインストール .....	5
インストール後 .....	5
5.x バージョンアプリからのアップグレード .....	6
ユーザー設定 .....	10
ドメインで区切られていないインスタンスのユーザーアクセス許可 .....	10
ユーザーの作成 .....	13
ドメインで区切られていないインスタンスのユーザーアクセス許可 .....	13
接続エイリアスの作成 .....	15
SGC Central Guided Setup .....	22
接続を管理する .....	27
コネクタの作成 .....	29
コネクタ設定オプションのマトリクス .....	29
Tenable Vulnerability Management の設定 .....	33
ServiceNow ITSM Pro のインシデントルールのフィールド .....	36
Tenable Security Center の設定 .....	42
Tenable OT Security の設定 .....	47
設定のテスト .....	52
よくある質問 .....	53



## Tenable for ServiceNow へようこそ

Tenable のアプリケーションは、お客様が ServiceNow と Tenable Vulnerability Management、Tenable Security Center、Tenable OT Security を併用しやすいように設計されています。

Service Graph Connector for Tenable アプリケーションは、Tenable 資産を ServiceNow 構成管理データベース (CMDB) に統合します。資産は、ServiceNow の識別および調整エンジン (IRE) を通じて CMDB にインポートされます。このアプリケーションを設定した後、Tenable の資産データを CI として ServiceNow に取り込み、ServiceNow CI を資産として Tenable Security Center と Tenable Vulnerability Management にプッシュすることができます。

Tenable OT Security for VR アプリケーションは、Tenable の脆弱性の検出結果を ServiceNow Security Operations Vulnerability Response モジュールに統合します。このアプリケーションを設定した後、Tenable OT Security の脆弱性のすべての検出結果を ServiceNow Vulnerable Items (VI) に同期し、Tenable プラグインの詳細情報を ServiceNow Third-Party Vulnerabilities に同期します。

Tenable for ITSM アプリケーションは、Tenable の脆弱性の検出結果をカスタムテーブルに統合し、これらの脆弱性からインシデントを作成します。このアプリケーションを設定した後、Tenable の脆弱性のすべての検出結果をカスタム脆弱性テーブルに同期し、Tenable プラグインの詳細情報を 2 つ目のカスタムテーブルに同期します。

### アプリケーションの依存関係

- プラットフォームの互換性:
  - Tenable Vulnerability Management、Tenable Security Center 5.7+、または Tenable OT Security
  - ServiceNow China、Zurich
- 必須プラグイン:
  - ITOM Discovery License - 1.0.0
  - ITOM Licensing - 1.0.0
  - CMDB CI Class Models - 1.76.0
  - CMDB 共通統合 - 2.20.0



- SGC Central - 2.2.0
- (オプション -ドメインセパレーションを使用する場合は必須) Domain Separation
- (オプション - VR には必須) ServiceNow Vulnerability Response - 23.0.0
- (オプション - ITSM には必須) Incident - 1.0.0



## アプリケーションのインストール

システム管理者 (admin) ロールを持つユーザーが、ServiceNow Store からアプリケーションをインストールできます。

必要なユーザーロール: 管理者

ServiceNow Store からアプリケーションをインストールする方法

1. <https://store.servicenow.com> にアクセスします。
2. 検索タブで「Service Graph Connector for Tenable」アプリを検索します。
3. **[Service Graph Connector for Tenable]** をクリックします。
4. **[Get]** ボタンをクリックします。
5. ServiceNow アカウントの ServiceNow ID 認証情報を入力します。  
成功したことを示すメッセージが表示され、
6. インスタンスを開き、**[System Applications]** > **[All Available Applications]** > **[All]** に移動します。
7. フィルター基準と検索バーを使用してアプリケーションを検索します。
8. リストされているアプリケーションの横にある **[Install]** をクリックします。

## インストール後

Tenable for ITSM と「Tenable.ot for VR」のアプリがインストールされている場合、それぞれのアプリのクロススコープ権限レコードを作成できます。

ServiceNow Store からアプリケーションをインストールする手順

1. 地球アイコンをクリックして、**[Application scope]** を **[Service Graph Connector for Tenable]** に設定します。
2. 検索フィルターをクリックし、「sys\_scope\_privilege.list」と入力します。
3. **[Enter]** をクリックします。
4. 右上にある **[New]** ボタンをクリックします。  
**[Cross scope privilege New record]** フォームが表示されます。



5. 次の表の値を使用して6つのレコードを作成します。

シリアル番号	ターゲットの範囲	ターゲット名	ターゲットタイプ	操作	ステータス
1	Tenable for ITSM	x_tsirm_tio_itsm_vulnerability	テーブル	読み取り	許可
2	Tenable for ITSM	TenableITSMHelper	スクリプトを含む	API 実行	許可
3	Tenable for ITSM	TenableITSM	スクリプトを含む	API 実行	許可
4	Tenable for ITSM	TenableITSMScheduleHelper	スクリプトを含む	API 実行	許可
5	Tenable.ot for VR	TenableVRScheduleHelper	スクリプトを含む	API 実行	許可
6	Tenable.ot for VR	TenableVRHelper	スクリプトを含む	API 実行	許可

6. レコードを作成したら、[Schedule Import] レコードに移動し、[Execute] をクリックします。

## 5.x バージョンアプリからのアップグレード

Service Graph Connector for Tenable for Assets および Tenable Connector のアプリを使用している場合は、今後予期しない問題が発生しないよう、こちらに記載されている手順に従ってアップグレードしてください。このプロセスは、他のアプリケーションを対象としていません。

**必要なユーザーロール:** 管理者

ServiceNow からアプリケーションをアップグレードする場合



### 古い Tenable for ITSM および Tenable.ot for VR をアップグレードする

1. インスタンスにログインし、[System Applications] > [All Available Applications] > [All] に移動します。
2. フィルター条件と検索バーを使用して対象のアプリケーションを見つけます。
3. アプリケーションリストの横で、アップデートするバージョンを選択します。
4. [Update] をクリックします。

### 古い Tenable Connector および Service Graph Connector for Tenable for Assets アプリをインスタンスからアンインストールする

1. [System Applications] > [All Available Applications] > [All] に移動します。
2. インスタンスにインストールされているアプリケーションのリストが表示されます。
3. Tenable Connector および Service Graph Connector for Tenable for Assets を見つけて選択し、関連リンクにある [Uninstall] をクリックします。

### 古い Tenable アプリから作成されたレコードをアップデートする

1. [System definition] > [Scripts - Background] に移動します。
2. 次のスクリプトを実行します。



- 次のスクリプトを **global** スコープで実行します。

```
var cmdbGr = new GlideRecord("cmdb_ci");
cmdbGr.addQuery("discovery_source", "SG-TenableForAssets");
cmdbGr.query();
while(cmdbGr.next()) {
    cmdbGr.discovery_source = "SG-Tenable";
    cmdbGr.update();
}
var vrItemsGr = new GlideRecord("sn_vul_vulnerable_item");
vrItemsGr.addQuery("source", "Tenable.ot");
vrItemsGr.query();
while(vrItemsGr.next()) {
    vrItemsGr.source = "Tenable OT Security";
    vrItemsGr.update();
}
var thirdPartyVrGr = new GlideRecord("sn_vul_third_party_entry");
thirdPartyVrGr.addQuery("source", "Tenable.ot");
thirdPartyVrGr.query();
while(thirdPartyVrGr.next()) {
    thirdPartyVrGr.source = "Tenable OT Security";
    thirdPartyVrGr.update();
}
```

**注意:** このスクリプトは、Tenable に固有の cmdb\_ci、脆弱な項目、および脆弱性エントリテーブルのレコードを消去するためのものです。

- 次のスクリプトを **x\_tsirm\_tio\_itsm** スコープで実行します。

```
var itsmVulTvmGr = new GlideRecord("x_tsirm_tio_itsm_vulnerability");
ismVulTvmGr.addQuery("source", "Tenable.io");
ismVulTvmGr.query();
while(ismVulTvmGr.next()) {
    itsmVulTvmGr.source = "Tenable Vulnerability Management";
    itsmVulTvmGr.update();
}
var itsmVulTscGr = new GlideRecord("x_tsirm_tio_itsm_vulnerability");
ismVulTscGr.addQuery("source", "Tenable.sc");
ismVulTscGr.query();
while(ismVulTscGr.next()) {
    itsmVulTscGr.source = "Tenable Security Center";
    itsmVulTscGr.update();
}

var itsmPluginTvmGr = new GlideRecord("x_tsirm_tio_itsm_plugin");
ismPluginTvmGr.addQuery("source", "Tenable.io");
ismPluginTvmGr.query();
while(ismPluginTvmGr.next()) {
```



```
    itsmPluginTvmGr.source = "Tenable Vulnerability Management";
    itsmPluginTvmGr.update();
}
var itsmPluginTscGr = new GlideRecord("x_tsirm_tio_itsm_plugin");
ismPluginTscGr.addQuery("source", "Tenable.sc");
ismPluginTscGr.query();
while(ismPluginTscGr.next()) {
    itsmPluginTscGr.source = "Tenable Security Center";
    itsmPluginTscGr.update();
}
```

**注意:** このスクリプトは、Tenable Vulnerability and Tenable Plugin テーブルのデータを消去するためのものです。

- 次のスクリプトを `x_tsirm_tio_vr` スコープで実行します。

```
var vrAdditionalFindingsGr = new GlideRecord("x_tsirm_tio_vr_ve_info");
vrAdditionalFindingsGr.addQuery("source", "Tenable.ot");
vrAdditionalFindingsGr.query();
while(vrAdditionalFindingsGr.next()) {
    vrAdditionalFindingsGr.source = "Tenable OT Security";
    vrAdditionalFindingsGr.update();
}
```

**注意:** このスクリプトは、Tenable Plugin Additional Info テーブルのデータを消去するためのものです。

## ユーザー設定

必要に応じて、ユーザーにロール特権を割り当てることができます。ロールは、ドメインで区切られたインスタンスとドメインで区切られていないインスタンスに応じて指定されます。

**注意:** `x_tsirm_tio_now.import_set_admin` ロールは、すべての Tenable アプリのインポート設定テーブルへのアクセスに使用されます。Tenable では、このロールをユーザーに付与することを推奨していません。

### ドメインで区切られていないインスタンスのユーザーアクセス許可

ユーザー	ロール	アクセス許可	説明
システム管理者	admin	統合アプリケーションプラグインのインストール ユーザーの作成 アプリケーションログ 接続エイリアスの作成 コネクタの作成 設定 定期ジョブの設定 リソース モニターの処理 サポート	このユーザーロールは ServiceNow インスタンスの管理者であり、統合固有のアクションをすべて実行する権限があります。
Tenable アプリケーション管理者	canvas_user cmdb_inst_admin connection_admin x_tsirm_tio_itsm.admin x_tsirm_tio_now.admin x_tsirm_tio_vr.admin	コネクタの作成 設定 定期ジョブの設定 リソース モニターの処理 サポート	このユーザーロールはアプリケーションの管理者であり、コネクタの作成、設定の変更、定期ジョブの設定が許可されています。
Tenable アプリケーションユーザー	canvas_user cmdb_inst_admin x_tsirm_tio_itsm.user	設定の読み取りアクセス コネクタ、定期ジョブへの読み取りアクセス	このユーザーロールは設定の読



	x_tsirm_tio_now.user x_tsirm_tio_vr.user	サポート	み取り専用に限 定されます。こ れらのユーザー は、設定を作成 または変更する ことはできませ ん。
--	---	------	--

ドメインで区切られているインスタンスのユーザーアクセス許可

ユーザー	ロール	アクセス許可	説明
システム管 理者	admin x_tsirm_tio_now.domain_ separation_admin	統合アプリケーションプ ラグインのインストール ユーザーの作成 アプリケーションログ 接続エイリアスの作成 コネクタの作成 設定 定期ジョブの設定 リソース モニターの処理 サポート	このユーザーロー ルは ServiceNow イ ンスタンスの管 理者であり、統 合固有のアク ションをすべて実 行する権限があ ります。
Tenable ア プリケーショ ン管理者	canvas_user cmdb_inst_admin connection_admin x_tsirm_tio_itsm.admin x_tsirm_tio_now.domain_ separation_admin x_tsirm_tio_vr.admin	コネクタの作成 設定 定期ジョブの設定 リソース モニターの処理 サポート	このユーザーロー ルはアプリケー ションの管理者 であり、コネクタ の作成、設定の 変更、定期ジョ ブの設定が許 可されていま す。
Tenable ア プリケーショ ンユーザー	canvas_user cmdb_inst_admin x_tsirm_tio_itsm.user	設定の読み取りアクセ ス コネクタ、定期ジョブへ	このユーザーロー ルは設定の読



	x_tsirm_tio_now.user x_tsirm_tio_vr.user	の読み取りアクセス サポート	み取り専用に限 定されます。こ れらのユーザー は、設定を作成 または変更する ことはできませ ん。
--	---	-------------------	--



## ユーザーの作成

ServiceNow プラットフォームでは、さまざまな Tenable ユーザーロールを作成し、割り当てることができます。

必要なユーザーロール: 管理者

### ドメインで区切られていないインスタンスのユーザーアクセス許可

ユーザー名 (例)	ロール
admin	canvas_user cmdb_inst_admin connection_admin x_tsirm_tio_itsm.admin x_tsirm_tio_now.domain_separation_admin x_tsirm_tio_vr.admin

Tenable ユーザーを作成してロールを割り当てる方法

1. [Organization] > [Users] の順にクリックします。
2. [Users] モジュールをクリックします。  
[Users] リストが表示されます。
3. [New] をクリックします。  
[New User] フォームが表示されます。
4. フォームに入力します。

注意: 次の表にある User ID タイトルとメールアドレスの値は、サンプルです。

フィールド	説明
User ID	ServiceNow プラットフォームインスタンスにおけるロールの一意のユーザー ID。(例: "tenable_admin")



First Name	このユーザーの名前。
Last Name	このユーザーの姓。
Title	このユーザーのジョブタイトルまたはロール(例:「Tenable 管理者」)。
Password	このロール用に作成された一意のパスワード。
Email	このユーザーの一意のメールアドレス。

5. **[Submit]** をクリックします。

**注意:** **[New User]** フォームを送信した後に、ロールを割り当てることができます。

6. **[User ID]** 列の **[Users]** リストで、作成した新しいユーザーの名前をクリックします。

新しいユーザーレコードが表示され、レコードのフォームビューに **[Set Password]** ユーザーインターフェースが表示されます。

7. **[Set Password]** ユーザーインターフェースアクションをクリックします。

新しいポップアップが表示されます。

8. **[Generate]** をクリックします。

**注意:** これにより、作成したユーザーに対して一意のパスワードが生成されますが、これは最初のログイン時に変更する必要があります。

9. 生成されたパスワードをコピーして、安全に保存します。

10. ポップアップを閉じます。

11. **[User ID]** 列の **[Users]** リストで、作成した新しいユーザーの名前をクリックします。

12. **[Role]** セクションで、**[Edit]** をクリックします。

13. **[Edit Member]** フォームの **[Collection]** フィールドにロールを追加します。

14. **[Collection]** 列で、[User Permissions For Domain Separated Instances](#) テーブルに記載されているロールを選択し、**[Roles List]** に移動します。

15. **[Save]** をクリックします。



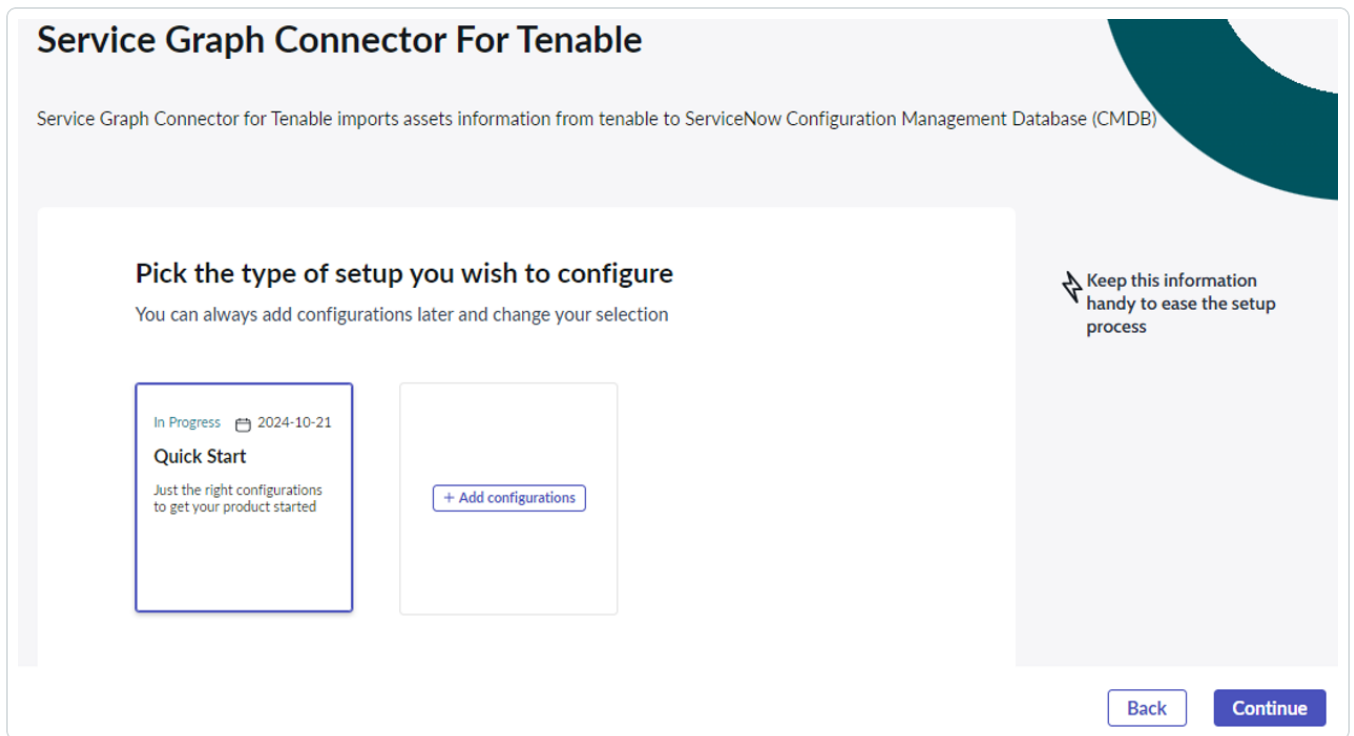
## 接続エイリアスの作成

ガイド付き設定で接続エイリアスを作成できます。

必要なユーザーロール: 管理者

接続エイリアスを作成する方法

1. ServiceNow インスタンスにログインします。
2. [Tenable Connector for Assets] > [Guided Setup] に移動します。
3. 設定タイプを選択します。



4. [Continue] をクリックします。
5. [Prerequisite] ページで [Update the max length of credential field] タブを選択し、ユーザーインターフェースに表示される手順に従います。

< Prerequisite ▾

Update the max l...

Update the max length for credential field Mandatory

System Administrator role required for this step. Contact to **System Administrator** to change the length of dictionary field.

- Follow the steps to update the length of user\_name in order to store the api key.
  - Open the user\_name record
  - Switch to the **'Global'** scope.
  - Update the **max length** value to **255**.
  - Save the record and switch back to the **'Service Graph Connector for Tenable'** scope.

Make sure to complete the task before checking 'Mark as complete' to proceed

Dictionary Entries View: Advanced | sys\_dictionary Table | name Search

Actions on selected rows... | x New ?

All > Table starts with discovery\_credentials > Column name starts with user\_name

Table	Column name	Type	Reference	Default value	Display	Text index
name	element	internal_type	reference	default_value	display	text_
discovery credenti	user name	Search	Search	Search	Search	Search

Mark as complete

- [Mark as Complete]** チェックボックスにチェックを入れます。
- [Continue]** をクリックします。
- [Configure Authentication Information]** タブを選択し、ユーザーインターフェースの手順に従います。

< **Configure the Connection and Credentials** ▼

Configure Authent...

🔒 Test Connection\*

🔒 Configure Tenabl...

**Configure Authentication Information** Mandatory

Prerequisite: Make the application scope as "Service Graph Connector for Tenable".

**Steps:**

1. [Click Here](#) [This will navigate the user to the connection page].
2. Select the appropriate **connection alias** record.
3. Click on the **Edit** button.
4. Fill out all of the required fields.
5. Click on the **Edit Connection** button.

Make sure to complete the task before checking 'Mark as complete' to proceed

Mark as complete

Cancel Continue

9. **[Mark as Complete]** チェックボックスにチェックを入れます。
10. **[Continue]** をクリックします。
11. **[Test Connection]** タブを選択し、ユーザーインターフェースの手順に従います。



### < Configure the Connection and Credentials ▾

- ✓ Configure Authe...
- Test Connection\***
- Configure Tenabl...

**Test Connection** Mandatory

- Choose tenable connector record for which you want to test the connection.
- Activate the connector and update the record.
- Open the same record and click on the **Test Connection** button.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x\_tsirm\_tio\_now\_tenable\_connector Name | name Search

Actions on selected rows... | x **New** ?

Name	Active	Connection Alias	Healthy	Updated
name	active	connection_alias	healthy	sys_updated_on
Tenable Operational Technology Connector	● true	x_tsirm_tio_now.Tenable_Operational_Tech...	● true	2024-10-21 04:00:56
Tenable Security Center Connector	● true	x_tsirm_tio_now.Tenable_Security_Center	● true	2024-10-21 03:58:34

Mark as complete Cancel Continue

12. Tenable から資産をフェッチするには、[Configure Tenable Schedule Import] タブを選択し、ユーザーインターフェースに表示された手順に従います。

### < Configure the Connection and Credentials ▾

- ✓ Configure Authe...
- ✓ Test Connection\*
- Configure Tenable...**

**Configure Tenable Scheduled Import to fetch assets from Tenable** Mandatory

- Open existing tenable record that you have configured. Make sure connector is in healthy state.
- Configure scheduled import from related list to fetch assets on a scheduled basis.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x\_tsirm\_tio\_now\_tenable\_connector Name | name Search

Actions on selected rows... | x **New** ?

Name	Active	Connection Alias	Healthy	Updated
name	active	connection_alias	healthy	sys_updated_on
Tenable Operational Technology Connector	● true	x_tsirm_tio_now.Tenable_Operational_Tech...	● true	2024-10-21 04:00:56
Tenable Security Center Connector	● true	x_tsirm_tio_now.Tenable_Security_Center	● true	2024-10-21 03:58:34
Tenable Vulnerability				2024-10-21

Mark as complete Cancel Continue



13. [Mark as Complete] チェックボックスにチェックを入れます。

14. [Continue] をクリックします。

## 複数インスタンスの追加 (オプション)

1. [Tenable Connector for Assets] > [Add Multiple Instances]の順にクリックします。
2. [Add Another Connections] タブを選択し、ユーザーインターフェースに表示された手順に従います。

**Add Multiple Instances** Close

Activities

- Add Another Connections
- **Test New Connections**
- Configure Tenable Scheduled Import ...

In Progress Priority

### Test New Connections

• create new connector record and test the connection.

Tenable Connectors Name Search Actions on selected rows... New

Name	Active	Service Graph Connection	Healthy	Updated
Tenable Operational Technology Connector	● true	Tenable Operational Technology	● false	2025-07-21 23:08:48
Tenable Security Center Connector	● false	Tenable Security Center	● true	2025-07-18 04:49:07
Tenable Vulnerability Management Connector	● true	Tenable Vulnerability Management	● true	2025-07-21 23:08:47

1 to 3 of 3

Mark as complete Skip

3. [Mark as Complete] チェックボックスにチェックを入れます。

4. [Continue] をクリックします。

5. [Test New Connections] タブを選択し、ユーザーインターフェースの手順に従います。



< **Add Multiple Instances** ▾

✓ Add Another Con...  
✓ Test New Conne...  
Configure Tenabl...

**Configure Tenable Scheduled Import to fetch assets from Tenable** Mandatory

- Open existing tenable record that you have configured. Make sure connector is in healthy state.
- Configure scheduled import from related list to fetch assets on a scheduled basis.

Make sure to complete the task before checking 'Mark as complete' to proceed

Tenable Connectors | x\_tsirm\_tio\_now\_tenable\_connector | Name | name | Search

Actions on selected rows... | x | New ?

All

<input type="checkbox"/>	Name <sup>▲</sup> name	Active active	Connection Alias connection_alias	Healthy healthy	Updated sys_updated_on
<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>	<input type="text" value="Search"/>
<input type="checkbox"/>	<a href="#">Tenable Operational Technology Connector</a>	<span style="color: green;">●</span> true	<a href="#">x_tsirm_tio_now.Tenable_Operational_Tech...</a>	<span style="color: green;">●</span> true	2024-10-21 04:00:56
<input type="checkbox"/>	<a href="#">Tenable Security Center Connector</a>	<span style="color: green;">●</span> true	<a href="#">x_tsirm_tio_now.Tenable_Security_Center</a>	<span style="color: green;">●</span> true	2024-10-21 03:58:34
<input type="checkbox"/>	<a href="#">Tenable Vulnerability</a>				2024-10-21

Mark as complete Cancel Continue

9. **[Mark as Complete]** チェックボックスにチェックを入れます。

10. **[Continue]** をクリックします。

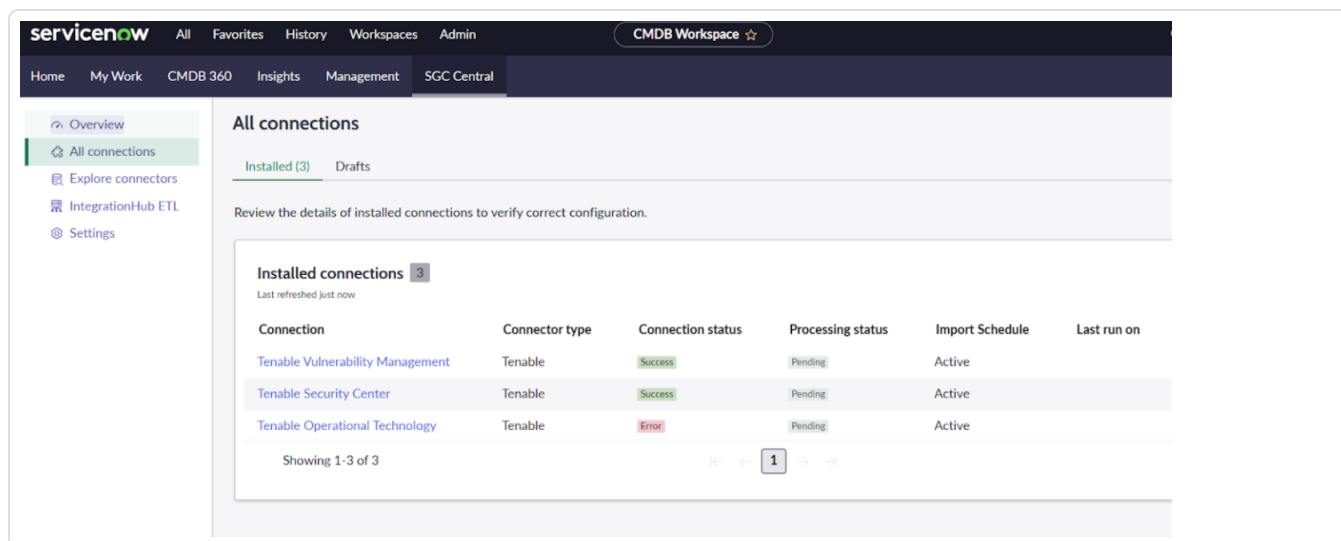
# SGC Central Guided Setup

ガイド付き設定で接続エイリアスを作成できます。

必要なユーザーロール: 管理者

## デフォルトの接続を設定する方法

1. [ワークスペース] > [CMDB ワークスペース] > [SGC Central]に移動します。



2. [All Connections]をクリックします。

ここで、インストールされている接続のリストを表示します。

3. 既存のレコードを更新します。

**注意:** 既存の設定が進行中の場合は、[ドラフト]タブをクリックしてTenableの設定を再開し、以下のマルチインスタンス設定セクションに記載されている手順に従ってマルチインスタンスを構成します。

4. いずれかの接続をクリックします。
5. URL、アクセスキー、秘密鍵を入力します。



Home My Work CMDB 360 Insights Management SGC Central

SGC Central > Tenable Vulnerability Management

### Tenable Vulnerability Management

Connector type Last run on Connection state Processing state Parent import schedule  
Tenable - Success Pending Active

Details Data sources Import schedules Errors

#### Details

Connection Name \*  
Tenable Vulnerability Management Connection

Connection URL \*  
https://cloud.tenable.com

Access Key \*  
access key

Secret Key \*  
.....

Use MID Server

Update and test connection

6. [Update and test connection] (更新してテスト接続)をクリックします。

接続テストが完了すると、[接続が検証されました]という成功メッセージが表示されます。

7. [データソース] タブをクリックしてデータソースの詳細を表示します。

SGC Central > Tenable Vulnerability Management

### Tenable Vulnerability Management

Connector type Last run on Connection state Processing state Parent import schedule  
Tenable - Success Pending Active

Details Data sources Import schedules Errors

#### Data sources 4

Last refreshed just now

Data Source	Type	Format	Updated	SQL statement	Last run datetime
SG-Tenable TVM - 3	File	JSON	2025-07-20 23:25:34		
SG-Tenable TVM - 2	File	JSON	2025-07-20 23:25:34		
SG-Tenable TVM - 4	File	JSON	2025-07-20 23:25:34		
SG-Tenable TVM - 1	File	JSON	2025-07-20 23:25:34		

Showing 1-4 of 4

1

20 rows per page

8. スケジューラを実行するには、[スケジュールのインポート] タブをクリックします。

## マルチインスタンス

1. [All Connections]に移動します。

2. [接続の作成]をクリックします。



3. **[Tenable]**を選択します。
4. **[接続の作成]**をクリックします。

**注意:** 手順に記載されているように、認証情報フィールドの最大長を更新する前提条件の手順を実行します。(すでに更新されている場合は、**[完了としてマーク]**をクリックします)。

5. **接続エイリアス**を選択します。
6. **[続行]**をクリックします。
7. 接続名、URL、トークンを入力します。
8. **[接続を作成してテストする]** ボタンをクリックします。

成功したことを示すメッセージが表示され、

**注意:** 接続の作成中に「認証情報の保存に失敗しました」というアラートが表示された場合は、無視できます。

9. 4件のスケジュールデータのインポートを確認します。
10. **[続行]**をクリックします。

Scheduled Data Import	Parent	Run	Data source	Active	Updated
Parent: (4) Show all					
SG-Tenable TOT - 4	(empty)	Periodically	SG-Tenable TOT - 4	true	2024-08-16 04:48:26
SG-Tenable TOT - 2	(empty)	Periodically	SG-Tenable TOT - 2	true	2024-08-16 04:46:39
SG-Tenable TOT - 1	(empty)	Periodically	SG-Tenable TOT - 1	true	2024-08-16 04:43:46
SG-Tenable TOT - 3	(empty)	Periodically	SG-Tenable TOT - 3	true	2024-08-16 04:47:08

11. **[Confirm Connection]** タブに移動し、**[View All Connections]** をクリックして追加されたすべての接続を表示します。



12. Tenable Connectorを作成するには、[Next] モジュールに移動し、以前に作成した SG Connection Record の [New] をクリックします。
13. 必要な設定の詳細を指定します。

SGC Central > Create Tenable connection

Create Connection For Te... ▾ i ^

- Prerequisites Complete
- Update the max length for credential field
- Configure the Connection a... 2/4
- Select SG connection alias template
- Configure and test connection
- Configure import schedule
- Confirm connection setup
- Create and Configure the Te... 0/2**
- Create and Configure the Tenable connector
- Configure Tenable Scheduled Import to fetch assets from...

In Progress

### Create and Configure the Tenable connector

- Choose tenable connector record for which you want to test the connection or Create new connector record.
- Select appropriate tenable SG Connection
- Activate the connector and update the record.
- Open the same record and click on the **Test Connection** button.

Tenable Connectors Name ▾ Search

Actions on selected rows... **New**

Name	Active	Service Graph Connection	Healthy	Updated
Tenable Operational Technology Connector	true	Tenable Operational Technology	false	2025-07-21 23:08:48
Tenable Security Center Connector	false	Tenable Security Center	true	2025-07-18 04:49:07
Tenable Vulnerability Management Connector	true	Tenable Vulnerability Management	true	2025-07-21 23:08:47

1 to 3 of 3

Mark as complete Skip

14. [Test Connection] をクリックします。
15. Connector Record を開いて Tenable Schedule Import Job を作成します。
16. [New] をクリックします。
17. 必要な設定の詳細を指定します。
18. [今すぐ実行] をクリックして、データを手動で収集します。
19. [Mark as Complete] をクリックします。



**Create Connection For Te...**

- Prerequisites Complete
  - Update the max length for credential field
- Configure the Connection a... 2/4
  - Select SG connection alias template
  - Configure and test connection
  - Configure import schedule
  - Confirm connection setup
- Create and Configure the Te...** 1/2
  - Create and Configure the Tenable connector
  - Configure Tenable Scheduled Import to fetch assets from...**

**Configure Tenable Scheduled Import to fetch assets from Tenable**

In Progress Priority

- Open existing tenable record that you have configured. Make sure connector is in healthy state.
- Configure scheduled import from related list to fetch assets on a scheduled basis.

**Tenable Connector**  
Tenable Operational Technology Connector

Active  Healthy

Scheduled Job Run As: System Administrator

Logging Level: Errors Only (Recommended)

**Asset Settings** | ITSM Settings | VR Settings

Pull Asset Chunk Size:  Push Asset Record Limit:

[SN Utils] Versions (0)

**Tenable Scheduled Imports (2)** | Tenable Jobs (2)

for text  Search     Actions on selected rows...

Connector = Tenable Operational Technology Connector

<input type="checkbox"/>	Name	Active	Tenable Product	Tenable Application
<input type="checkbox"/>	<a href="#">Tenable Operational Technology Connector - Pull Plugins</a>	true	tot	vr
<input type="checkbox"/>	<a href="#">Tenable Operational Technology Connector - Pull Vulnerabilities</a>	true	tot	vr

1 to 2 of 2



## 接続を管理する

必要なユーザーロール: 管理者

既存の接続を作成または更新し、接続をテストできます。接続 モジュールは、さまざまなシステムコンポーネント間の接続を管理および監視するのに役立ちます。

このモジュールの主なフィールドは次のとおりです。

Name	説明
Name	各接続の一意の識別子。
Active	接続が現在アクティブであるか非アクティブであるかを示します。
接続エイリアス	接続を参照するために使用される代替名または識別子。
メッセージ	接続に関連する関連情報または通知が含まれます。
ステータス	成功、保留中、失敗などの接続の現在の状態。
ステータスコード	接続認証情報を使用するのAPI呼び出しから返される応答ステータスコード。
提案	問題に対処するための推奨事項またはアクション。
アプリケーション	接続が作成されるアプリケーションスコープ。
更新日	接続レコードが最後に変更された日時です。

ステータスフィールドは接続の動作状態を示し、次の値を持つことができます。

Name	説明
Success	接続は正常に動作しており、データの送信または意図された機能の実行に成功しています。
Error	接続に問題があります。これにより、パフォーマンスに影響を与えたり、想定通りの動作を妨げたりする可能性があります。

コネクタを管理するには



1. ServiceNow インスタンスにログインします。
2. [Tenable Connector for Assets] > [Connectors] に移動します。  
[Tenable Connector] が表示されます。
3. [New] をクリックするか、既存の接続を選択して更新します。

Service Graph Connections は、関連する Tenable コネクタと同期したままです。[テスト接続] をクリックすると、そこでのステータスが更新され、この接続をサービスグラフ接続として使用するすべてのコネクタは、テスト接続の結果に基づいて正常または非正常としてマークされます。同様に、Tenable コネクタから [テスト接続] アクションを実行すると、テストの結果もそこに反映され、それに応じてステータスが更新されます。



## コネクタの作成

Tenable 製品の必須の接続と任意の接続を作成することができます。

必要なユーザーロール: 管理者

## コネクタ設定オプションのマトリクス

Tenable 製品	モジュール	ジョブタイプ
Tenable OT Security (ICP)	Asset	Pull Assets
	VR	Pull Plugins Pull Vulnerabilities
Tenable Security Center	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities
	SGC for Tenable	Pull Queries
Tenable Vulnerability Management	Asset	Pull Assets Push Assets
	ITSM	Pull Vulnerabilities

### コネクタを作成する方法

1. ServiceNow インスタンスにログインします。
2. [Tenable Connector for Assets] > [Connectors] に移動します。  
[Tenable Connector] が表示されます。
3. [New] をクリックします。  
[New User] フォームが表示されます。

Tenable Connector  
New record View: TenableStandard\*

Choose Connection Alias same as Tenable product.

\* Name

\* Tenable Product -- None --

\* Connection Alias

Active  Healthy

Scheduled Job Run As  Logging Level Errors Only (Recommended)

Asset Settings VR Settings ITSM Settings

Pull Asset Chunk Size  Push Asset Record Limit

Submit

4. [Name] フィールドにコネクタの名前を入力します。
5. [Tenable Product] ドロップダウンボックスから、[Tenable Vulnerability Management]、[Tenable Security Center]、[Tenable OT Security (ICP)] のいずれかを選択します。
6. 選択した Tenable Product 用の Service Graph Connection を選択します。
7. [任意の接続](#)に進むか、[Submit] をクリックします。

## 任意の接続

1. [Tenable Connector for Assets] > [Add Multiple Instances] の順にクリックします。
2. [Mark as Complete] チェックボックスにチェックを入れます。
3. (オプション) [Scheduled Job Run As] ボックスで、データのインポート者となるユーザーのユーザー名を入力します。
4. (オプション) ドロップダウンボックスから [Logging Level] を選択します。

**注意:** Tenable は [Errors Only] レベルの使用を推奨しています。

5. (オプション) [Asset Settings] タブ



Asset Settings	VR Settings	ITSM Settings
Pull Asset Chunk Size	<input type="text" value="1,500"/>	Push Asset Record Limit
		<input type="text" value="10,000"/>

名前	説明	デフォルト値
Pull Asset Chunk Size	プルされるレコードのページあたりの数。[Pull Assets] ジョブタイプに使用されます。	1500
Push Asset Record Limit	プラットフォームで一度にプッシュされるレコードの総数。[Push Assets] ジョブタイプに使用されます。	10000

注意: [VR Settings] と [ITSM Settings] のタブは、プラグインがアクティブ化されている場合にのみ表示されます。

## 6. (オプション) [VR Settings] タブ

Asset Settings	VR Settings	ITSM Settings
TOT Vulnerability Chunk Size	<input type="text" value="200"/>	TOT Plugin Chunk Size
		<input type="text" value="200"/>

名前	説明	デフォルト値
TOT Vulnerability Chunk Size	プルされる脆弱性のページあたりの数。[TOT Pull Vulnerabilities] ジョブタイプに使用されます。	200 (最大数でもある)
Push Asset Record Limit	プラットフォームで一度にプッシュされるレコードの総数。[Push Assets] ジョブタイプに使用されます。	10000

## 7. (オプション) [ITSM Settings] タブ



Asset Settings	VR Settings	ITSM Settings	
TSC Vulnerability Chunk Size	<input type="text" value="1500"/>	TVM Vulnerability Asset Chunk Size	<input type="text" value="50"/>

名前	説明	デフォルト値
TSC Vulnerability Chunk Size:	プルされる脆弱性の ページあたりの数。 <b>[TSC Pull Vulnerabilities]</b> ジョ ブタイプに使用されま す。	1500
TVM Vulnerability Asset Chunk Size	すべての脆弱性がプ ルされる資産の数。 <b>[TVM Pull Vulnerabilities]</b> ジョ ブタイプに使用されま す。	50

**注意:** Tenable はこのフィールドのデフォルト値を  
変更しないことを推奨しています。値を大きくす  
ると、一度にプルされるデータ量も増加します。  
そのために、そのデータの読み取り中に問題が  
発生する可能性があります。

8. **[Submit]** をクリックします。

次のステップ

- [Tenable Vulnerability Management の設定](#)
- [Tenable Security Center の設定](#)
- [Tenable OT Security の設定](#)



# Tenable Vulnerability Management の設定

必要なユーザーロール: 管理者

ServiceNow で Tenable Vulnerability Management を設定する方法

1. ServiceNow インスタンスにログインします。
2. [Tenable Connector for Assets] > [Connectors] に移動します。  
[Tenable Connector] が表示されます。
3. 接続先の Tenable 製品が Tenable Vulnerability Management である既存のコネクタに移動します。
4. [Module] ドロップダウンボックスから、[Asset] または [ITSM] を選択できます。

注意: デフォルトでは、コネクタの名前が入力されています。

注意: 資産モジュールでは、Tenable ジョブタイプとして [Pull Assets] または [Push Assets] を選択できます。ITSM モジュールでは、Tenable ジョブタイプとして [Pull Vulnerabilities] を選択できます。

## 資産モジュール、Tenable ジョブタイプ > Pull Assets

**Pull Assets 定期ジョブ**は、Tenable Vulnerability Management から ServiceNow に資産をフェッチし、資産の詳細情報を CMDB の各テーブル (Incomplete IP Identified Device、Unclassed Hardware、Computer、Network Adaptor、IP Address) と**カスタムテーブル** (Tenable Asset Attributes) に保存します。

名前	説明	デフォルト値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内



Last Run	インポートが最後に実行された日時。	該当なし
Edit Run Schedule	<p>定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。</p> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p><b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</p> </div> <ul style="list-style-type: none"> <li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li> <li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは <b>[Run]</b> の選択によって異なります。</li> </ul>	<p>選択した場合、デフォルト値は <b>[Daily]</b>。</p>

### 資産モジュール、Tenable ジョブタイプ > Push Assets

**Push Assets 定期ジョブ**は、資産を ServiceNow から Tenable Vulnerability Management にプッシュします。

Name	説明	デフォルト値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内
Last Run	インポートが最後に実行された日時。	該当なし
Edit Run Schedule	定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。	有効な場合、デフォルト値は



	<p><b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</p> <ul style="list-style-type: none"> <li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li> <li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは <b>[Run]</b> の選択によって異なります。</li> </ul>	<b>[Daily]</b> 。
--	--	------------------

5. **[Conditions]** > **[Configuration Item Source Table]** ドロップダウンで、Tenable Vulnerability Management に資産をエクスポートするためにクエリをかけるテーブルを選択します。
6. **[Conditions]** > **[Conditions]** ドロップダウンで、選択したフィルター条件を **[Configuration Item Source Table]** で適用します。
7. **[ITSM Module]** を選択した場合は、以下のパラメーターを設定します。

#### ITSM モジュール、Tenable ジョブタイプ > Pull Vulnerabilities

**Pull Vulnerabilities 定期ジョブ**は、Tenable Vulnerability Management から ServiceNow に脆弱性をフェッチし、それらの脆弱性を**カスタムテーブル** (Tenable Vulnerability) に保存します。

名前	説明	デフォルト値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内
Last Run	インポートが最後に実行された日時。	該当なし
Last run - Fixed	修正したインポートが最後に実行された日時。統合では、この日時以降の脆弱性をフェッチしま	該当なし



	す。	
Run Fixed Query on Initial Run	初回のインポートで修正済みの脆弱性をプルします。	無効
Included Severities	インポートする脆弱性の深刻度を指定します。	デフォルトではこの値は空で、深刻度が「高」と「重大」の脆弱性のみがフェッチされます。
Edit Run Schedule	<p>定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。</p> <div style="border: 1px solid blue; padding: 5px;"><p><b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</p></div> <ul style="list-style-type: none"><li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li><li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは [Run] の選択によって異なります。</li></ul>	選択した場合、デフォルト値は [Daily]。

**注意:** [Name] テキストボックスは、コネクタの名前とジョブタイプに基づいて自動的に入力されます。

8. [Submit] をクリックします。

次のステップ

- [設定のテスト](#)に進みます。

## ServiceNow ITSM Pro のインシデント ルールのフィールド



ServiceNOW と Tenable Vulnerability Management の統合により、インシデントルールフィールドが生成され、次の資産属性が ServiceNow ITSM Pro にプッシュされます。

## インシデントルールのフィールドと資産属性

ラベル	Name
cvssV4Supplemental	u_cvssv4supplemental
seolDate	u_seoldate
epssScore	u_epssscore
recastRiskRuleComment	u_recastriskrulecomment
acceptRiskRuleComment	u_acceptriskrulecomment
hostUUID	u_hostuuid
acrScore	u_acrscore
エージェント UUID	u_agent_uuid
First Found	u_first_found
IP	u_ips
オペレーティングシステム	u_operating_system
Plugin Modification Date (プラグイン修正日)	u_plugin_modification_date
優先順位	u_priority
Scan (スキャン)	u_scan
severity_modification_type	u_severity_modification_type
XREF	u_xref
説明	u_description
indexed	u_indexed
Netbios Name (Netbios 名)	u_netbios_name



ラベル	Name
プラグインファミリータイプ	u_plugin_family_type
Port Port	u_port_port
risk_accepted	u_risk_accepted
severity_default_id	u_severity_default_id
VPR Context	u_vprcontext
Configuration Item	u_ci
Hostname (ホスト名)	u_hostname
Last Found Date	u_last_found_date
Plugin Description (プラグインの説明)	u_plugin_description
プラグインの概要	u_plugin_synopsis
リポジトリID	u_repository_id
SC Unique	u_scunique
Tenable プラグイン ID	u_tenable_plugin
FQDN	u_fqdn
last_fixed	u_last_fixed
pluginName	u_pluginname
Plugin Publication Date (プラグイン公開日)	u_plugin_publication_date
再開されました	u_reopened
Scan Started At	u_scan_started_at
状態	u_state
vulnUniqueness	u_vulnuniqueness
vulnUUID	u_vulnuuid



## インシデントルールフィールドと資産属性 (cont'd)

ラベル	Name
cvssV4BaseScore	u_cvssv4basescore
cgiScanEnabled	u_cgiscanenabled
keyDrivers	u_keydrivers
assetExposureScore	u_assetexposurescore
thoroughScanEnabled	u_thoroughscanenabled
paranoidScanEnabled	u_paranoidscanenabled
finding_id	u_finding_id
BIOS UUID	u_bios_uuid
hasBeenMitigated	u_hasbeenmitigated
最終見つかりました	u_last_found
プラグイン CVE	u_plugin_cve
Plugin Solution	u_plugin_solution
Repository Data Format (リポジトリデータフォーマット)	u_repository_data_format
UUID をスキャン	u_scan_uuid
サブステート	u_substate
資産ホスト名	u_asset_hostname
First Found Date	u_first_found_date
ジョブタイプ	u_job_type
出力	u_output
Plugin Name (プラグイン名)	u_plugin_name



ラベル	Name
製品タイプ	u_product_type
Scan Completed At	u_scan_completed_at
ソース名	u_source_name
デバイスタイプ	u_device_type
IP	u_ip
operatingSystem	u_operatingsystem
Plugin ID (プラグイン ID)	u_plugin_id
Port Protocol	u_port_protocol
変更されたリスク	u_risk_recasted
深刻度 ID	u_severity_id
VPR Score (VPR スコア)	u_vpr_score
ソース	u_source
Connector	u_connector
hostUniqueness	u_hostuniqueness
MAC アドレス	u_mac_address
Plugin Family (プラグインファミリー)	u_plugin_family
Ports (ポート)	u_port
リポジトリ名	u_repository_name
深刻度	u_severity
uniqueness	u_uniqueness
添付ファイル	u_attachment
cvssV4Vector	u_cvssv4vector



ラベル	Name
cvssV4ThreatScore	u_cvssv4threatscore
cvssV4ThreatVector	u_cvssv4thretvector



# Tenable Security Center の設定

必要なユーザーロール: 管理者

ServiceNow で Tenable Security Center を設定する方法

1. ServiceNow インスタンスにログインします。
2. [Tenable Connector for Assets] > [Connectors] に移動します。  
[Tenable Connector] が表示されます。
3. 接続先の Tenable 製品が Tenable Security Center である既存のコネクタに移動します。
4. [Module] ドロップダウンボックスから、[Asset]、[ITSM]、または [SGC for Tenable] を選択できます。

注意: デフォルトでは、コネクタの名前が入力されています。

注意: 資産モジュールでは、Tenable ジョブタイプとして [Pull Assets] または [Push Assets] を選択できます。ITSM モジュールでは、Tenable ジョブタイプとして [Pull Vulnerabilities] を選択できます。

## 資産モジュール、Tenable ジョブタイプ > Pull Assets

**Pull Assets 定期ジョブ**は、Tenable Security Center から ServiceNow に資産をフェッチし、資産の詳細情報を CMDB の各テーブル (Incomplete IP Identified Device、Unclassed Hardware、Computer、Network Adaptor、IP Address) と **カスタムテーブル** (Tenable Asset Attributes) に保存します。

名前	説明	デフォルト値
TSC Query	選択されたフィルターを使用して、Tenable Security Center から脆弱性または資産をプルします。	無効
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効



Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内
Last Run	インポートが最後に実行された日時。	該当なし
Edit Run Schedule	<p>定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。</p> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p><b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</p> </div> <ul style="list-style-type: none"> <li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li> <li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは [Run] の選択によって異なります。</li> </ul>	<p>選択した場合、デフォルト値は [Daily]。</p>

### 資産モジュール、Tenable ジョブタイプ > Push Assets

**Push Assets 定期ジョブ**は、資産を ServiceNow から Tenable Security Center にプッシュします。Tenable Security Center では、データは定期ジョブの作成時に指定したグループにプッシュされます。指定されたグループがまだない場合は、プラットフォームで新しいグループが作成されます。

名前	説明	デフォルト値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内



Last Run	インポートが最後に実行された日時。	該当なし
Edit Run Schedule	<p>定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。</p> <div style="border: 1px solid blue; padding: 5px;"><p><b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</p></div> <ul style="list-style-type: none"><li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li><li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは <b>[Run]</b> の選択によって異なります。</li></ul>	有効な場合、デフォルト値は <b>[Daily]</b> 。

5. **[Conditions]** > **[Configuration Item Source Table]** ドロップダウンで、Tenable Security Center に資産をエクスポートするためにクエリをかけるテーブルを選択します。

**注意:** デフォルトでは、この値は `cmdb_ci` に設定されています。グループタイプが **[Static IP Address]** の場合、**[Configuration Item Source Table]** は「CMDB CI IP アドレス」の親テーブルである必要があります。

6. **[Condition]** > **[Group Name]** テキストボックスに、グループの名前を入力します。

**注意:** この名前のグループは、資産レコードのプッシュ中に Tenable Security Center に作成されます。これらのレコードは、プラットフォームのグループ名に基づいて識別できます。

7. **[Condition]** > **[Group Type]** ドロップダウンで、プッシュするデータのタイプに基づいて、**[DNS]** または **[Static IP Address]** を選択します。

**注意:** **[Static IP Address]** を選択した場合、**[IP Version]** と **[IP's To Send]** オプションを設定する必要があります。一意の IP アドレスのみが Tenable Security Center に保存されます。ただし、Tenable ジョブの **[Total Record]** フィールドには、プラットフォームに実際に保存されているレコード数よりも多くのレコードが表示される場合があります。この不一致は、プラットフォームでは一意性をチェックするのに対して、ジョブでは一意性をチェックしないために発生します。定期ジョブでは、最初に選択されたテーブルからレコードが取得され、次に `cmdb_rel_ci` テーブルの親子関係がチェックされます。この関係が成立していない場合、IP はプラットフォームにプッシュされません。この関係が成立している場合、子 IP がプラットフォームにプッシュされます。

8. [Conditions] > [Conditions] ドロップダウンで、選択したフィルター条件を [Configuration Item Source Table] で適用します。
9. [ITSM Module] を選択した場合は、以下のパラメーターを設定します。

### ITSM モジュール、Tenable ジョブタイプ > Pull Vulnerabilities

Pull Vulnerabilities 定期ジョブは、Tenable Security Center から ServiceNow に脆弱性をフェッチし、それらの脆弱性をカスタムテーブル (Tenable Vulnerability) に保存します。

名前	説明	デフォルト値
TSC Query	選択されたフィルターを使用して、Tenable Security Center から脆弱性または資産をプルします。	無効
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内
Last Run	インポートが最後に実行された日時。	該当なし
Last run - Fixed	修正したインポートが最後に実行された日時。統合では、この日時以降の脆弱性をフェッチします。 <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">注意: このフィールドは [Fixed] ジョブモード用です。</div>	該当なし
Run Fixed Query on Initial Run	初回のインポートで修正済みの脆弱性をプルします。	無効
Edit Run Schedule	定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。 <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">注意: 実行頻度は高く設定しないでください。ジョブが過密にな</div>	選択した場合、デフォルト値は



	<p>り、パフォーマンスの問題が発生する可能性があります。</p> <ul style="list-style-type: none"><li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li><li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは <b>[Run]</b> の選択によって異なります。</li></ul>	<b>[Daily]</b> 。
--	--	------------------

**注意:** [Name] テキストボックスは、コネクタの名前とジョブタイプに基づいて自動的に入力されます。

10. **[Submit]** をクリックします。

次のステップ

- [設定のテスト](#)に進みます。

# Tenable OT Security の設定

必要なユーザーロール: 管理者

ServiceNow で Tenable OT Security を設定する方法

1. ServiceNow インスタンスにログインします。
2. [Tenable Connector for Assets] > [Connectors] に移動します。  
[Tenable Connector] が表示されます。
3. 接続先の Tenable 製品が Tenable OT Security である既存のコネクタに移動します。
4. [Module] ドロップダウンボックスから、[Asset] または [VR] を選択できます。

注意: デフォルトでは、コネクタの名前が入力されています。

注意: 資産モジュールでは、Tenable ジョブタイプとして [Pull Assets] を選択できます。VR モジュールでは、Tenable ジョブタイプとして [Pull Vulnerabilities] を選択できます。[Pull Plugins Tenable Job Type] は、[Pull Vulnerabilities] ジョブによって自動的に作成されます。

## 資産モジュール、Tenable ジョブタイプ > Pull Assets

**Pull Assets 定期ジョブ**は、Tenable OT Security から ServiceNow に資産をフェッチし、資産の詳細情報を CMDB の各テーブル (IP Address、Network Adapter、OT Control Systems、Incomplete IP Identified Device、Operational Technology (OT)、Network Gear、Industrial Sensors) と **カスタムテーブル** (Tenable Asset Attributes) に保存します。

名前	説明	デフォルト値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内



Last Run	インポートが最後に実行された日時。	該当なし
Edit Run Schedule	<p>定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。</p> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p><b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</p> </div> <ul style="list-style-type: none"> <li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li> <li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは <b>[Run]</b> の選択によって異なります。</li> </ul>	<p>選択した場合、デフォルト値は <b>[Daily]</b>。</p>

5. **[VR Module]**を選択した場合は、次のパラメーターを設定します。

**注意:** このモジュールが表示されるのは、「Tenable.ot for VR」統合がインストールされている場合のみです。

#### VR モジュール、Tenable ジョブタイプ > Pull Plugins

**Pull Plugins 定期ジョブ**は、Tenable OT Security から ServiceNow に資産をフェッチし、プラグインの詳細情報をカスタムテーブル (Plugin Import and Tenable Plugin Additional Info) に保存します。

**注意:** この定期ジョブは、**Pull Vulnerabilities** ジョブが作成されると自動的に作成されます。

名前	説明	デフォルト値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効



Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内
Last Run	インポートが最後に実行された日時。	該当なし
Last run - Fixed	修正したインポートが最後に実行された日時。統合では、この日時以降の脆弱性をフェッチします。  <b>注意:</b> このフィールドは <b>[Fixed]</b> ジョブモード用です。	該当なし
Run Fixed Query on Initial Run	初回のインポートで修正済みの脆弱性をプルします。	無効
Edit Run Schedule	定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。  <b>注意:</b> 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。  <ul style="list-style-type: none"> <li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li> <li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは <b>[Run]</b> の選択によって異なります。</li> </ul>	選択した場合、デフォルト値は <b>[Daily]</b> 。

## VR モジュール、Tenable ジョブタイプ > Pull Vulnerabilities

**Pull Vulnerabilities 定期ジョブ**は、Tenable OT Security から ServiceNow に脆弱性をフェッチし、ServiceNow テーブル **Vulnerable Item** に脆弱性を保存します。

名前	説明	デフォルト
----	----	-------



		値
Active	選択されている場合、この定期ジョブが設定されたスケジュールで実行されます。	無効
Initial Run - Historical Data	データをプルするために遡る日数です。	過去 365 日以内
Last Run	インポートが最後に実行された日時。	該当なし
Last run - Fixed	修正したインポートが最後に実行された日時。統合では、この日時以降の脆弱性をフェッチします。 <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">注意: このフィールドは [Fixed] ジョブモード用です。</div>	該当なし
Run Fixed Query on Initial Run	初回のインポートで修正済みの脆弱性をプルします。	無効
Edit Run Schedule	定期ジョブの実行設定を変更する場合は、このボックスを選択します。次のオプションを設定する必要があります。 <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">注意: 実行頻度は高く設定しないでください。ジョブが過密になり、パフォーマンスの問題が発生する可能性があります。</div> <ul style="list-style-type: none"><li>• <b>Run:</b> インポートを実行する頻度。可能な値は Daily、Weekly、Monthly、Periodically、Once、On Demand、Business Calendar: Entry Start、Business Calendar: Entry End です。</li><li>• <b>Repeat Interval/Time:</b> インポートを実行する時刻 (hh/mm/ss) を設定します。これは [Run] の選択によって異なります。</li></ul>	選択した場合、デフォルト値は [Daily]。

注意: [Name] テキストボックスは、コネクタの名前とジョブタイプに基づいて自動的に入力されます。

6. [Submit] をクリックします。

次のステップ



- [設定のテスト](#)に進みます。



## 設定のテスト

ServiceNow MID サーバーアプリケーションは、ServiceNow プラットフォームと外部アプリケーション、データソース、サービス間のデータ通信とデータ移動をサポートします。1つの環境に複数のMIDサーバーを設定して、一部のサーバーは開発とテスト専用、他は本番専用にすることができます。

設定チェック:

- Tenable Security Center が社内ネットワークのファイヤーウォールの後ろにある場合は、MIDサーバーを使用してデータにアクセスする必要があります。
- Tenable オペレーショナルテクノロジーの場合、MIDサーバーは必須です。
- ServiceNowドキュメントの [MIDサーバー](#) セクションを参照してください。
- お使いのシステムがMIDサーバーシステム要件を満たしていることを確認します。詳細は、ServiceNowドキュメント [MIDサーバーのシステム要件](#) を参照してください。



## よくある質問

### ServiceNow Store からアプリケーションをインストールできないのはなぜですか？

1. システム管理者 (admin) ロールを持っていることを確認します。
2. [System Applications] > [All Available Applications] > [All] に移動します。
3. アプリケーションが [Installed] タブに表示されていることを確認します。

### ユーザーを新規作成するにはどうすればよいですか？

- [ユーザー管理](#)にある手順を実行します。

### ECC キューのタイムアウトに関連するエラーが表示されるのはなぜですか？

1. sys\_properties.LIST に移動します。
2. 指定された値で次のシステムプロパティを更新します。
  - a. glide.http.outbound.max\_timeout.enabled = false
  - b. glide.http.outbound.max\_timeout.enabled = false
  - c. glide.http.outbound.max\_timeout = 60 (または要件に応じて時間を長くします)
3. スケジュールされたスクリプトを再実行します。

### 接続エイリアスを作成できないのはなぜですか？

- システム管理者 (admin) ロールを持っていることを確認します。

### コネクタを作成できないのはなぜですか？

1. システム管理者 (admin) ロールまたはアプリケーション管理者ロールがあることを確認します。

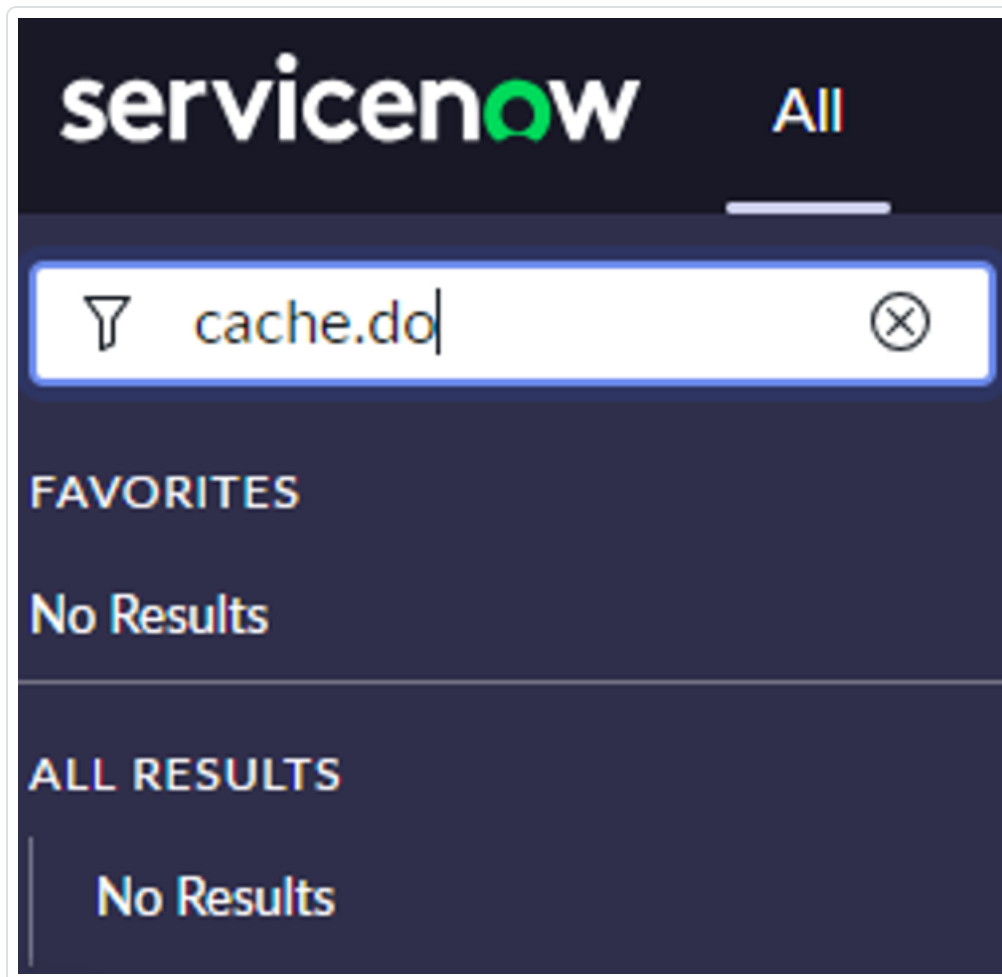
### コネクタが正常でないのはなぜですか？



1. 認証情報と接続エイリアスのエンドポイントをチェックします。エンドポイントの後に「/」を追加しないようにしてください。
2. (TSC および TOT の場合) MID が実行されていることを確認します。(TOT では必須)

## [Tenable Scheduled Import Form] ビューにオプションが表示されないのはなぜですか？

1. ブラウザからキャッシュを消去するか、Incognito から [Scheduled Import Job] を作成します。
2. ServiceNow インスタンスからキャッシュを消去します。
  - a. ServiceNow インスタンスにログインします。
  - b. フィルタータブで「cache.do」と入力します。



- c. [Enter] をクリックします。

- d. 次のページで [Clear Cache] をクリックします。

[Clear Cache](#)

---

**Servlet Memory**  
Max memory: 1980.0  
Allocated: 1980.0  
In use: 1695.0  
Free percentage: 14.0

---

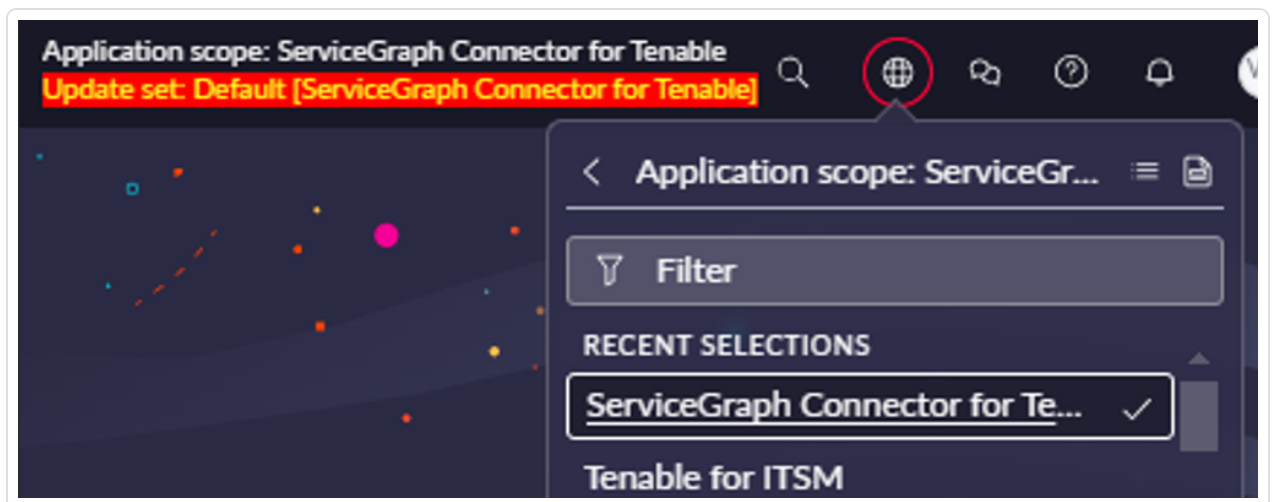
After Cache Flush

---

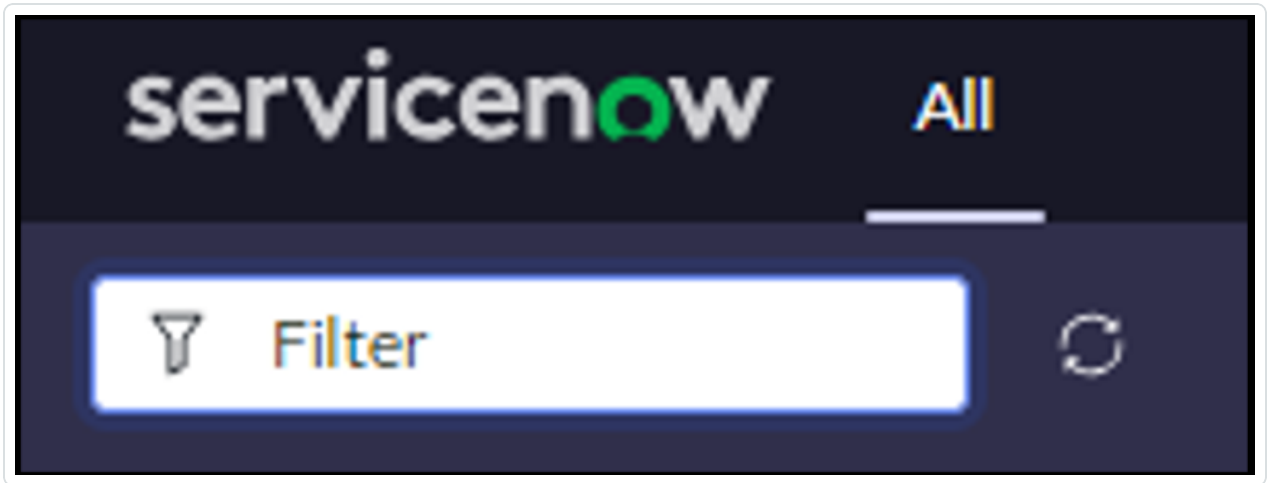
**Servlet Memory**  
Max memory: 1980.0  
Allocated: 1980.0  
In use: 1264.0  
Free percentage: 36.0

## 定期ジョブの実行後にジョブが作成されないのはなぜですか？

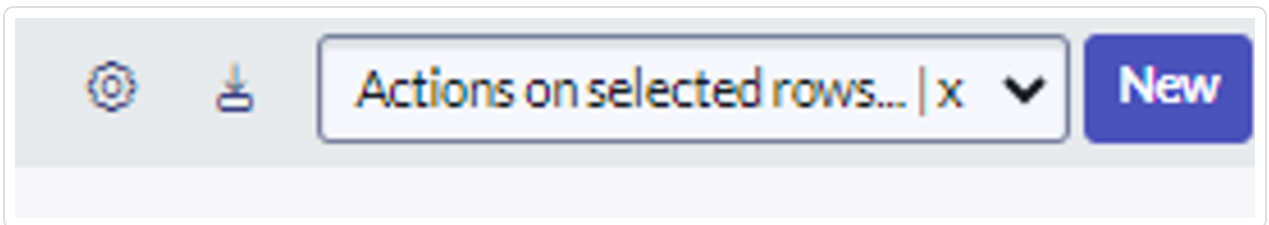
1. 不足しているクロススコープ特権レコードを手動で作成します。
  - a. ここから、[Application scope] を [Service Graph Connector for Tenable] に設定します。



- b. [Filter] をクリックし、「sys\_scope\_privilege.list」と入力します。



- c. [Enter] をクリックします。
- d. 右上にある [New] ボタンをクリックします。



以下のフォームが表示されます。

- e. 次の値で6つのレコードを作成します。

シリアル番号	ターゲットの範囲	ターゲット名	ターゲットタイプ	操作	ステータス
1	Tenable for	x_tsirm_tio_itsm_	テーブル	読み	許可



	ITSM	vulnerability	ル	取り	
2	Tenable for ITSM	TenableITSMHelper	スクリプトを含む	API 実行	許可
3	Tenable for ITSM	TenableITSM	スクリプトを含む	API 実行	許可
4	Tenable for ITSM	TenableITSMScheduleHelper	スクリプトを含む	API 実行	許可
5	Tenable.ot for VR	TenableVRScheduleHelper	スクリプトを含む	API 実行	許可
6	Tenable.ot for VR	TenableVRHelper	スクリプトを含む	API 実行	許可

f. [Schedule Import record] に移動し、[Execute] をクリックします。

2. すべてのスレッドが埋まっているかどうかをチェックします。

a. [User Administration] > [All Active transaction] に移動します。

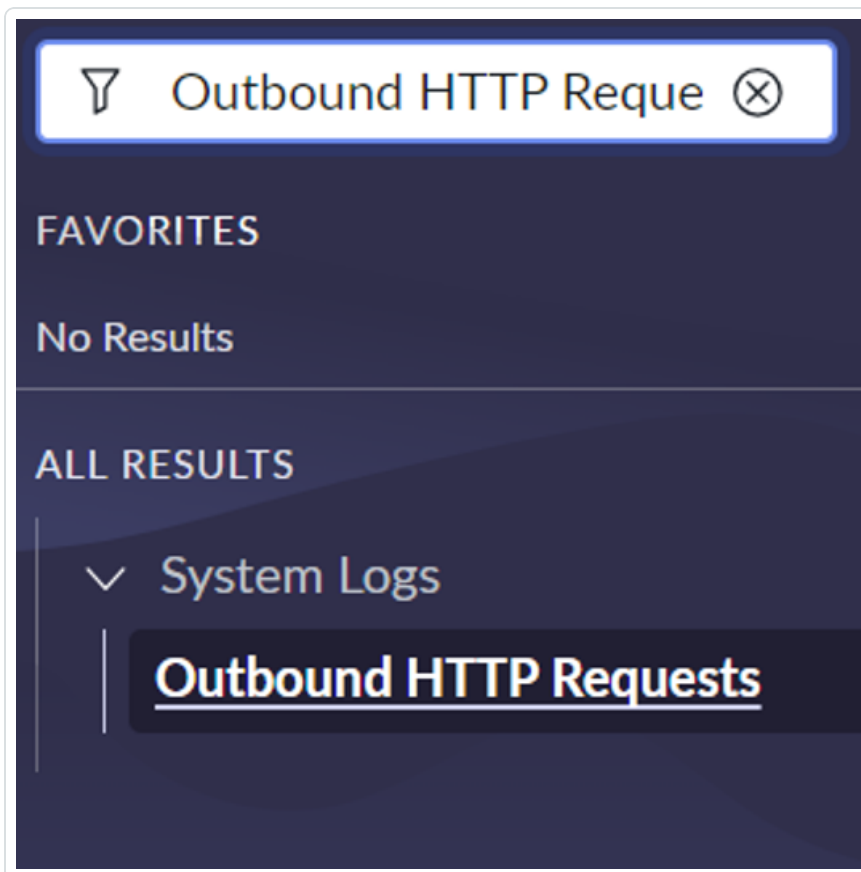
b. すべてのスレッドが埋まっていることを確認します。その場合、使用されていないスレッドを削除してください。

c. [Scheduled Data] インポートフォームをリロードします。

**統合が失敗する、またはデータがテーブルに取り込まれないのはなぜですか？**



1. コネクタの設定をチェックし、正常であることを確認します。
2. ユーザーが適切なロールを持っていることを確認します。[この](#)ページを参照して、Tenableプラットフォームでユーザーに必要なロールを確認します。
3. [Application Logs] を確認します。
4. エラーがAPI呼び出しに関連するものである場合は、次の手順に従います。
  - a. **sys\_properties** テーブルから次の3つのシステムプロパティを有効にし ([Filters] セクションで「sys\_properties.LIST」と入力できます)、統合を再度実行します。
    - glide.outbound\_http\_log.override -> 値を「true」に設定
    - glide.outbound\_http\_log.override.level -> 値を「all」に設定
    - glide.outbound\_http.content.max\_limit -> 値を「1000」に設定
  - b. [System Logs] の [Outbound HTTP Requests] モジュールで、API呼び出しのリクエストと応答の詳細を含むHTTPリクエストをチェックします。





## 「Request method or request URL not found from undefined」というエラーが表示されるのはなぜですか？

1. [Flow Designer] > [Actions]に移動します。
2. [Rest] ステップを開き、実行をチェックします。API のエラーの可能性がります。
3. 定期ジョブを再実行してください。

## インポートジョブを使用してデータを取得してからファイルサイズを拡大する中に、「例外: SyntaxError: 空の JSON 文字列」が発生しました。操作の手順

1. システム管理者 (admin) ロールを持っていることを確認します。
2. sys\_properties に移動します。
3. com.glide.attachment.max\_get\_size および com.glide.attachment.max\_sizeの値を増加します。値をバイト単位で入力します。

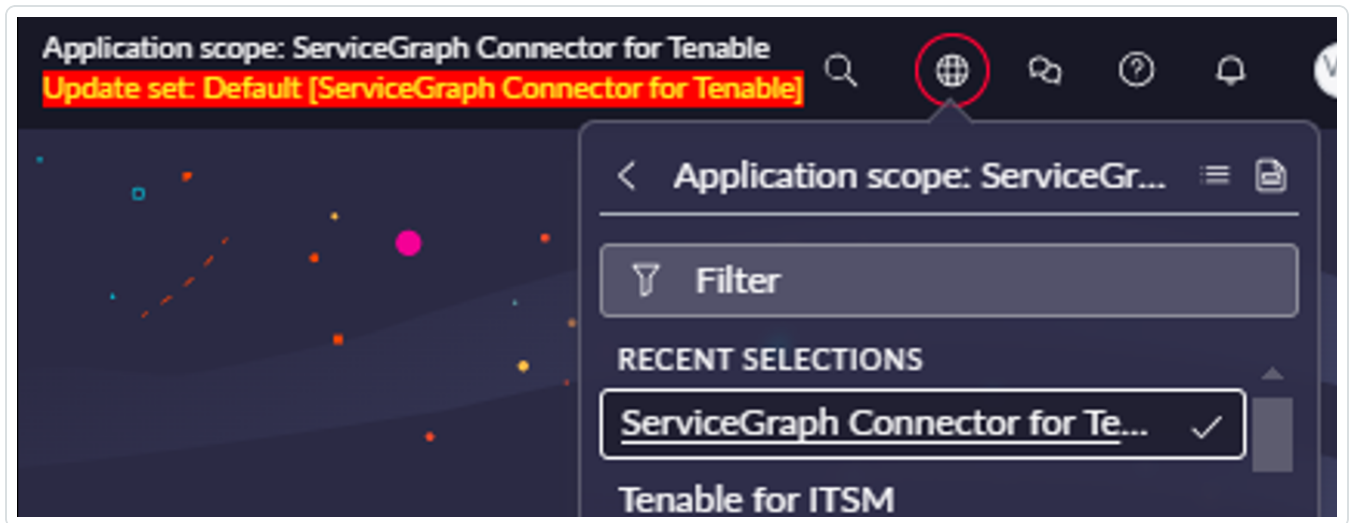
注意:プロパティが存在しない場合は、[グローバルスコープ] で新しく作成します。(例: com.glide.attachment.max\_get\_size = 31457280 および com.glide.attachment.max\_size = 4096 です)。

## MID サーバーを検証できないのはなぜですか？

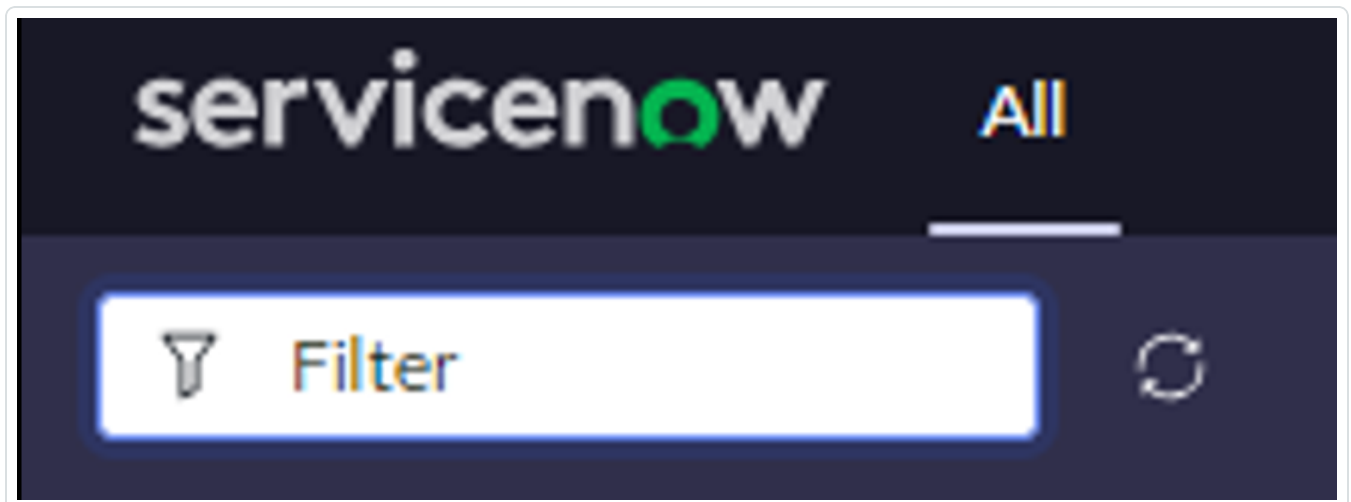
1. [MID Server] > [MID Security Policy] に移動します。
2. [Intranet and Internet Records] を開き、[Certificate Chain Check]、[Hostname Check]、[Revocation Check] のチェックボックスをオフにします。

## ITSM または VR のデータソースをアクティブ化/非アクティブ化するにはどうすればよいですか？

1. 次の場所から [Application scope] を [ServiceGraph Connector for Tenable] に設定します。



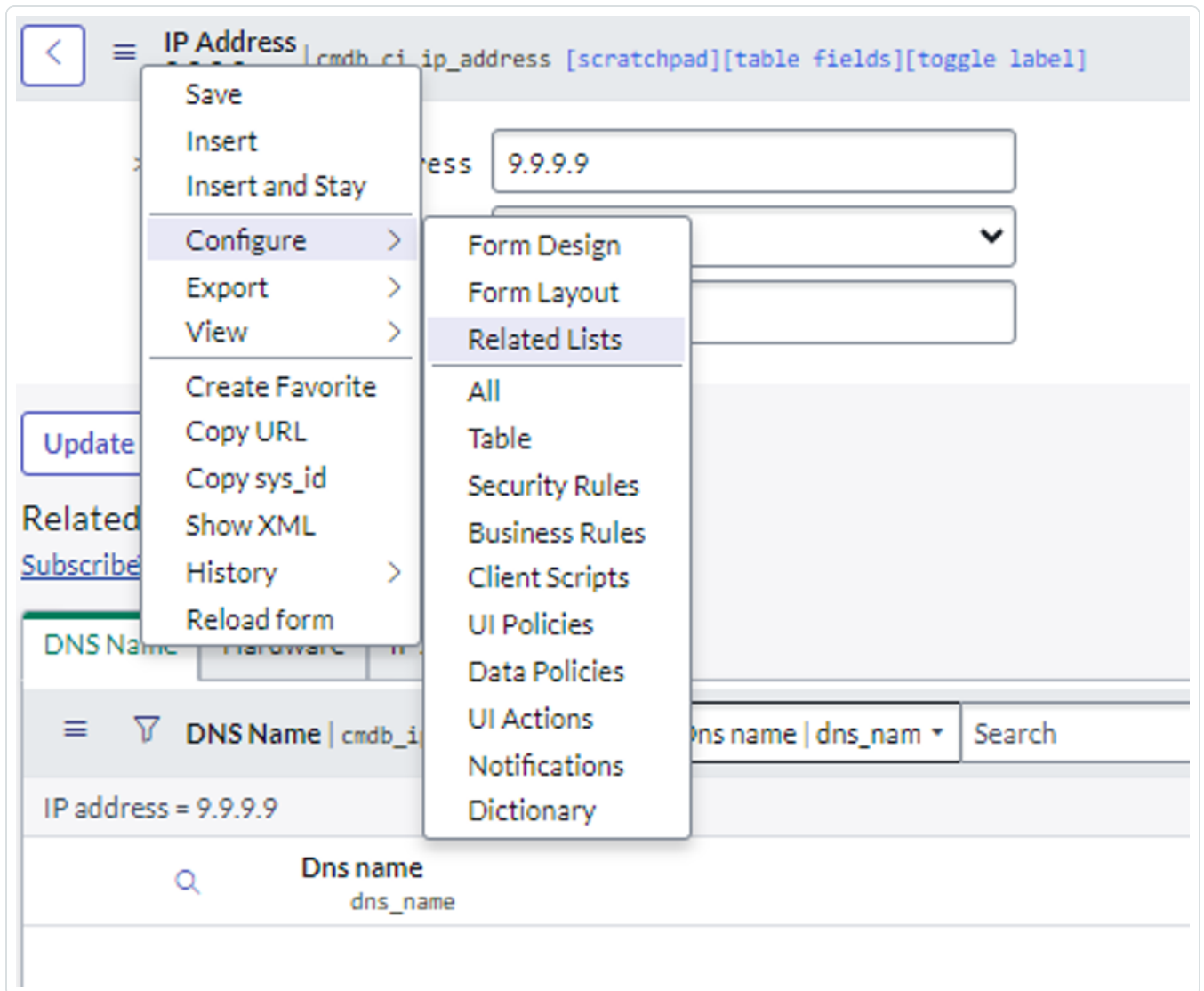
2. [Filter] をクリックします。



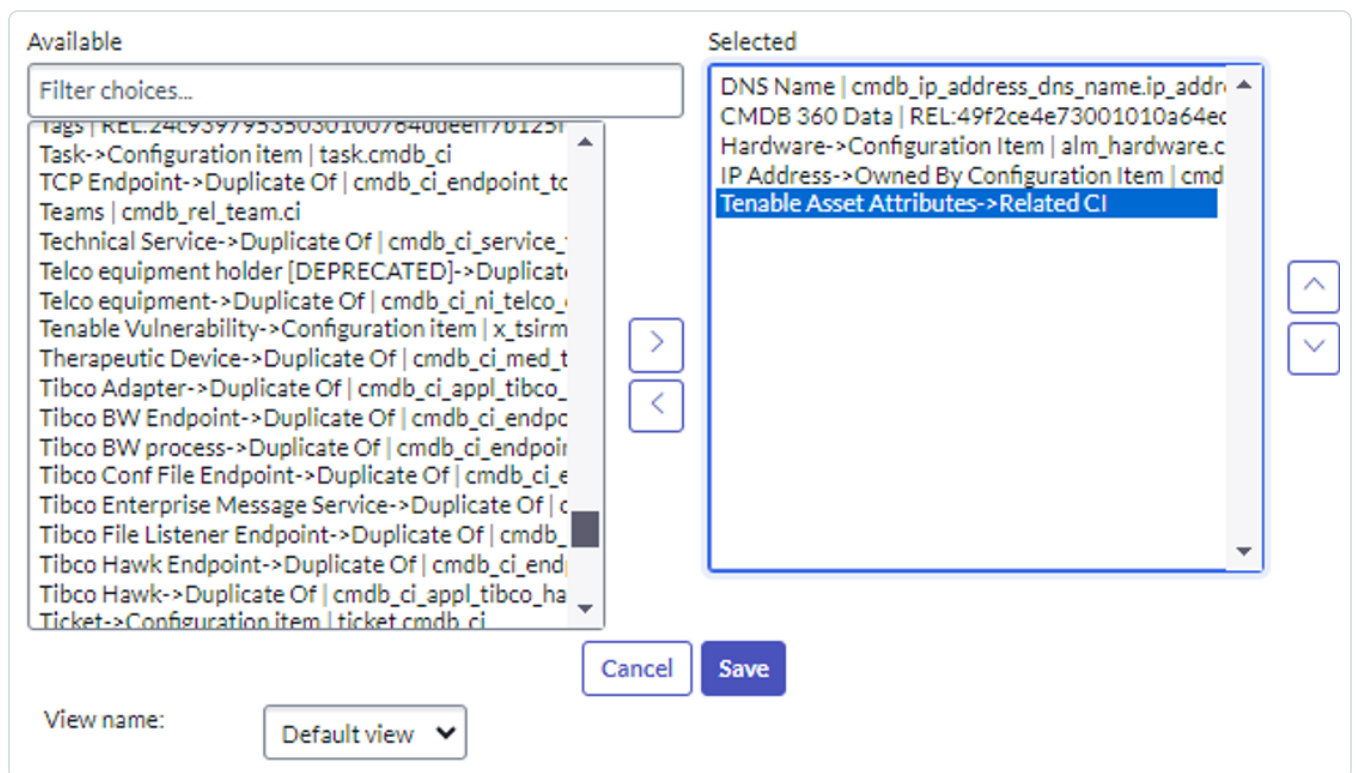
3. 「x\_tsiirm\_tio\_now\_data\_source\_registry.list」と入力します。
4. [Enter] をクリックします。
5. 適切なフィルターを適用した後、[Active] 列でレコードの値を設定します。

資産レコードの関連リストに Tenable 資産属性を表示するにはどうすればよいですか？

1. [Asset] レコードの左上にある [Additional Actions] ボタンをクリックします。
2. [Configure] > [Related Lists]に移動します。



3. [Tenable Asset Attributes] オプションを選択し、[Selected] リストにプッシュします。



4. [Save] をクリックします。

5. これで資産の [Tenable Asset Attributes] 関連リストが表示されます。

## Xanadu のガイド付き設定で [Mark as Complete] をクリックすると、統合が別のセクションの手順にリダイレクトされるのはなぜですか？

- これは現在、Xanadu で確認されている問題です。この問題の詳細については、ServiceNow コミュニティページをチェックしてください。

## 既存の接続レコードが SG 接続モジュールの表ビューに表示されない場合、アプリケーションをアップグレードした後に、次の手順に従います。

1. [All] > [Fix Scripts] に移動します。
2. 「Tenable - Create SG Connections」というタイトルの修正スクリプトレコードを開きます。
3. [Run Fix Script] をクリックします。



4. 実行後、[SGC 接続] テーブルのレコードを確認します。
5. 既存のレコードが SG 接続モジュールに表示されるようになりました。

## ファームウェアインストールテーブルに、同じ構成項目 CI の重複エントリが表示されます

- この重複が発生するのは、ServiceNow が同じ CI レコードに対して 2 つの異なるソースネイティブキーを生成し、複数のエントリが作成されていたためです。

## SGC Central モジュールから Connection レコードを設定中に、プロセスが固まった場合またはページが応答しなくなった場合：

- ページを更新し、最初から設定手順を再開します。

## Zurich リリースでは、ユーザーが Guided Setup を完了すると、構成手順を変更または再起動することはできません。

- この制限に対処するため、ServiceNow では、ガイド付き設定の代わりに SGC Central (post-Zurich) を導入しました。SGC Central Workspace で、ユーザーは新しい接続をより柔軟に作成および設定できるようになりました。
- SGC Central の使用に関する詳細な手順については、[SGC Central Guided Setup \(SGC Central ガイド付きセットアップ\)](#) を参照してください。