Tanium™ Reputation ユーザーガイド

バージョン 5.0. 1

2020年 4月 01日

この文書の内容は予告なく変更されることがあります。また、本書に記載の内容は「現状のまま」提供されており、正確には万全を期しておりますが、Taniumの顧客販売契約に規定されている保証を除き、明示または暗黙を問わずいかなる保証もしません。別段の規定がない限り、Taniumはいかなる責任も負いません。TaniumおよびそのサプライヤはTanium Inc.がかかる損害の可能性を事前に通知されていたとしても、本書の使用または使用できないことから生じる、利益損失やデータ損失をはじめとする間接的損害や特別損害、結果的損害、および付随的損害に対して一切の責任を負いません。

本書で使用されているIPアドレスは、実際のアドレスであることを意図していません。本書に記載されている例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、例示の目的にのみ使用されています。例示コンテンツに実際のIPアドレスが使用されていたとしても、特別な意図はなく、偶然です。

最新のTanium製品のマニュアルについては、https://docs.tanium.com を参照してください。

Taniumは米国およびその他の国におけるTanium,Inc.の商標です。記載されているその他の社名、製品名、サービス名は各社の商標または登録商標です。

目次

Reputationの概要 **6**

レピュテーションアイテムのライフサイクル 6

レピュテーションアイテムがレピュテーションデータベースに追加される 6

レピュテーションアイテムがスキャンされる 6

WildFire 6

ReversingLabs A1000 7

ReversingLabs TitaniumCloud 7

VirusTotal 7

レピュテーションアイテムが再スキャンされる 7

Wildfire 7

ReversingLabs A1000 7

ReversingLabs TitaniumCloud 8

VirusTotal 8

アイテムがレピュテーションデータベースから削除される 8

ホワイトリスト/ブラックリスト 8

はじめに **10**

Reputationの要件 **11**

Taniumの依存関係 11

Tanium™ Module Server 11

サードパーティのソフトウェア 11

ホストとネットワークセキュリティの要件 12

ポート 12

セキュリティの除外 12

インターネットのURL 12
ユーザーロールの要件 12
Reputationのインストール 14
使用を開始する前に 14
Reputationのインポート 14
インストールを検証する 14
レピュテーションサービスの設定を構成する 14
次にやるべきこと 15
connectデータの構成 16
Palo Alto Networks WildFireレピュテーションソースを構成する 16
前提条件 16
設定を構成する 16
ReversingLabs A1000レピュテーションソースを構成する 17
前提条件 17
設定を構成する 17
ReversingLabsのTitaniumCloudレピュテーションソースを構成する 18
前提条件 18
設定を構成する 18
VirusTotalレピュテーションソースを構成する 19
前提条件 20
設定を構成する 20
レピュテーションスキャンのステータスを表示する 21
ホワイトリストまたはブラックリストデータの管理 22
データハッシュの追加 22
ハッシュをインポート 22

ハッシュのエクスポート 23
ハッシュを削 除 23
connectデータのエクスポート **24**
レピュテーションデータを表 示 する 24
レピュテーションデータを接 続 先 に送 信 する 24
レピュテーションサービスにデータを送 信 する 25
Reputationのトラブルシューティング **27**
ログを収 集 する 27
Reputationのアンインストール 27
再 インストール時 にデータが復 元 されるようにReputationをアンインストールする 27
再 インストールするときに最 初 から始 められるようにReputationをアンインストールする 28

Reputationの概要

Reputationを使用し、Palo Alto WildFire、ReversingLabs、VirusTotalなど、さまざまなソースからレピュテーションデータのリポジトリを構築できます。これらのソースは、ファイルハッシュの脅威レベルを決定します。Tanium™ Traceなどの他のTanium製品は、このデータを使用して、潜在的に悪意のあるファイルを示すことができます。レピュテーションデータをサポートされているTanium™ Connect接続先に送信することもできます。

レピュテーションデータベースは、*レピュテーションアイテム*から成るキャッシュです。構成すると、レピュテーションアイテムは*レピュテーションソース*でスキャンされます。レピュテーションソースは、レピュテーションアイテムが悪意のある、悪意のない、疑わしい、またはステータスが不明であるとみなされるかどうかを判断するサービスです。

レピュテーションアイテムのライフサイクル

Taniumプロセスがアイテムのステータスにアクセスしている間は、レピュテーションアイテムはデータベースに残ります。レピュテーションアイテムのステータスは、レピュテーションサービスおよびプロバイダの設定に基づいて最新の状態に保たれます。

レピュテーションアイテムがレピュテーションデータベースに追加される

最大データベースサイズを超えない限り、レピュテーションアイテムは次のシナリオでレピュテーションデータベースに追加されます。

- 新しいハッシュがTraceなどのTaniumプロセスによって識別されたとき。
- 保存されたQuestionの接続元からハッシュのリストがConnectに送信されたとき。

レピュテーションアイテムが最初に追加されるとき、悪意あるかどうかは不明です。レピュテーションアイテムの状態はほとんどの場合、不明または保留中です。

レピュテーションアイテムがスキャンされる

アイテムの初期スキャンにかかる時間は、構成されているレピュテーションサービスの設定によって異なります。

複数のレピュテーションサービスプロバイダが設定されている場合、レピュテーションソースごとにレピュテーションアイテムが作成されます。たとえば、単一のハッシュの場合、WildFire、ReversingLabs、およびVirusTotalの3つのレピュテーションアイテムが作成されます。

WILDFIRE

すべてのレピュテーションアイテムは、受信時にWildFireに送信されます。

REVERSINGLABS A1000

ReversingLabs A1000の設定によって、一度に送信されるハッシュ数と、APIが1分間に何回呼び出されるかが決まります。これらの設定の詳細については、17ページのReversingLabs A1000レピュテーションソースを構成するを参照してください。

REVERSINGLABS TITANIUMCLOUD

ReversingLabs TitaniumCloudの設定によって、一度に送信されるハッシュ数とAPIが1分間に何回呼び出されるかが決まります。これらの設定の詳細については、18ページのReversingLabsのTitaniumCloudレピュテーションソースを構成するを参照してください。

VIRUSTOTAL

VirusTotalの設定により、一度に送信されるハッシュ数と、APIが1分間に何回呼び出されるかが決まります。これらの設定の詳細については、19ページのVirusTotalレピュテーションソースを構成するを参照してください。

レピュテーションアイテムが再スキャンされる

レピュテーションは、時間の経過とともにレピュテーションアイテムに対して変化する可能性があります。アイテムが再スキャンされると、レピュテーションソースに対して再度チェックされます。再スキャンプロパティの設定の詳細については、14ページのレピュテーションサービスの設定を構成するを参照してください。

[Rescan Item Interval (アイテム再スキャン間隔)]はすべてのレピュテーションプロバイダタイプに対してグローバルに設定されています。この値は、アイテムが再スキャンされる頻度を決定します。たとえば、この値を1日に設定すると、データベース内のすべてのアイテムが毎日チェックされます。

WILDFIRE

アイテムは**[Rescan Item Interval (アイテム再スキャン間隔)]**でのみスキャンされます。

REVERSINGLABS A1000

ReversingLabs A1000がハッシュの新しい評価を取得すると、再スキャンするアイテムを設定できます。

[Maximum Age of New Items (新しいアイテムの最大経過時間)]設定がReversingLabs A1000のFirst Seen属性と比較されます。First Seen属性は、ReversingLabs A1000が最初にそのハッシュのインスタンスを記録した日付です。アイテムが構成された最大値より小さい場合、アイテムは再スキャンされます。新しいアイテムが再スキャンされる頻度は、**[Rescan Item Interval (アイテム再スキャン間隔)]**で設定します。

REVERSINGLABS TITANIUMCLOUD

ReversingLabs TitaniumCloudがハッシュの新しいレピュテーションを得るように、再スキャンするアイテムを設定できます。

[Maximum Age of New Items (新しいアイテムの最大経過時間)]設定がReversingLabs TitaniumCloudのFirst Seen属性と比較されます。First Seen属性は、ReversingLabs TitaniumCloud顧客がReversingLabs TitaniumCloudがそのハッシュのインスタンスを最初に記録した日付です。アイテムが構成された最大値より小さい場合、アイテムは再スキャンされます。新しいアイテムが再スキャンされる頻度は、**[Rescan Item Interval (アイテム再スキャン間隔)]**で設定します。

VIRUSTOTAL

VirusTotalの有料APIキーをお持ちの場合、VirusTotalはハッシュの新しい評価を取得するため、再スキャンするアイテムを設定できます。

[Maximum Age of New Items (新しいアイテムの最大経過時間)]設定がVirusTotalのFirst Seen属性と比較されます。First Seen属性は、VirusTotalの顧客からVirusTotalがそのハッシュのインスタンスを最初に記録した日付です。アイテムが構成された最大値より小さい場合、アイテムは再スキャンされます。新しいアイテムが再スキャンされる頻度は、**[Rescan Item Interval (アイテム再スキャン間隔)]**で設定します。

これらの設定を行うときは、API呼び出し回数をVirusTotalとの契約の範囲内に維持するように注意してください。

アイテムがレピュテーションデータベースから削除される

[Remove Item Interval (アイテムを削除する間隔)]の日数が過ぎて、そのアイテムが保存されたQuestionやその他のTaniumプロセスによってそのステータスを確認するためにクエリされなかった場合、そのアイテムはデータベースから削除されます。

ハッシュが再び見つかると、レピュテーションアイテムをデータベースに再追加することができます。

ホワイトリスト/ブラックリスト

Reputationホワイトリスト/ブラックリストは、誤検出または悪意があることがわかっているレピュテーションハッシュのリストです。ホワイトリスト/ブラックリストから特定のハッシュを追加または削除するか、リスト全体をエクスポートおよびインポートできます。

詳細については、22ページのホワイトリストまたはブラックリストデータの管理を参照してください。

この文書には、第三者が提供するコンテンツや製品(ハードウェアおよびソフトウェアを含む)、サービス(「第三者のアイテム」)に対するアクセス手段や、第三者のそうした情報そのものが含まれていることがあります。Tanium Inc.およびその関連会社は、(i)それらの第三者のアイテムに対して責任を負うものではなく、第三者のアイテムに関するすべての保証および責任を明示的に放棄し、(ii)お客様とTaniumとの間の有効な契約に明記されているのでない限り、かかる第三者のアイテムへのアクセスや、利用に起因する損失、費用または損害について責任を負いません。

また、この文書は、特定の第三者のアイテムの使用やTanium製品との組み合わせを求めるものでも、想定するものでもありません。そのような組み合わせによって生じた知的財産権の侵害について、Taniumおよびその関連会社は一切責任を負いません。第三者のアイテムとTanium製品の組み合わせが適切であるかどうか、また第三者の知的財産権を侵害しないかどうかの判定の責任はTaniumではなくお客様にあります。

はじめに

1. Taniumレピュテーションをインストールします。14ページのReputationのインストールを参照してください。
2. Reputationのソースを構成し有効にします。16ページのconnectデータの構成を参照してください。
3. Reputationホワイトリスト/ブラックリストを管理します。22ページのホワイトリストまたはブラックリストデータの管理を参照してください。
4. Reputationデータをエクスポートします。24ページのconnectデータのエクスポートを参照してください。

Reputationの要件

Reputationをインストールし、利用するには次の要件を満たす必要があります。

Taniumの依存関係

環境が以下の要件に適合していることを確認します。

コンポーネント	要件
Platform	7.2以降。
Tanium™ Client	クライアント要件はありません。
Tanium Connect	バージョン4.11以降(オプション)。
Tanium™ Trace	レピュテーションデータのバージョン2.0.5 (オプション)。
Tanium™ Incident Response	ハッシュデータの場合(オプション)。

Tanium™ Module Server

Reputationがインストールされると、Module Serverのホストコンピュータ上のサービスとして実行されます。使用状況によりますが、Module Serverへの影響は小さいです。

サードパーティのソフトウェア

Reputationを使用すると、いくつかの異なる種類のサードパーティ製ソフトウェアと統合することができます。具体的なバージョンがリストに掲載されていない場合は、そのソフトウェアのバージョン要件はありません。

- Palo Alto Networks Wildfire
- ReversingLabs A1000
- ReversingLabs TitaniumCloud
- VirusTotal

ホストとネットワークセキュリティの要件

Reputationを実行するには、特定のポートとプロセスが必要です。

ポート

Reputationの通信には、以下のポートが必要です。

コンポーネント	ポート	方向	目的
Module Server	17455	インバウンド	内部使用、外部からアクセスできません

セキュリティの除外

未知のホストシステムプロセスを監視およびブロックするためにセキュリティソフトウェアが環境内で使用されている場合、セキュリティ管理者はTaniumプロセスを干渉なく実行できるように除外を作成する必要があります。

表 1：レピュテーションセキュリティの除外

対象デバイス	プロセス
Module Server	`<Tanium Module Server>\services\reputation-service\node.exe`

インターネットのURL

不明なURLを監視してブロックするため、セキュリティソフトウェアが適用されている環境では、セキュリティ管理者は以下のURLをホワイトリストに追加しなければならない場合があります。

- reversinglabs.com
- virustotal.com
- wildfire.paloaltonetworks.com

ユーザーロールの要件

表 2：Reputationユーザーロールのアクセス許可

アクセス許可	Reputation Administrator (Reputation管理者)
Show Reputation (Reputationを表示)[1] Reputationワークベンチを表示する	2

アクセス許可	Reputation Administrator (Reputation管理者)
Reputation Read (Reputation読み取り) Reputation共有サービスへの読み取りアクセス	2
Reputation Write (Reputation書き込み)[3] Reputation共有サービスへの書き込みアクセス	2
Reputation Administrator (Reputation管理者) Reputation共有サービスへの管理アクセス	

[1] Reputationをインストールするには、管理者の予約済みロールが必要です。

[2] 提供された許可を示します。

[3] Reputation APIへのみアクセス権が必要な場合は、ユーザーに**[Reputation Write (Reputation書き込み)]**アクセス許可を追加できます。

表3：Tanium 7.1.314.3071以降用のReputation拡張ユーザーロールアクセス許可

アクセス許可	アクセス許可用コンテンツセット	Reputation Administrator (Reputation管理者)
Execute Plugin (プラグインの実行)	Reputation	

コンテンツセットとアクセス許可の詳細および説明については、Tanium Core Platformユーザーガイド：ユーザーとユーザーグループを参照してください。

Reputationのインストール

Reputationは**[Tanium Solutions (Taniumソリューション)]**ページからインストールできます。

使用を開始する前に

- リリースノートをお読みください。
- 11ページのReputationの要件を確認してください。
- Tanium Connect 4.10以前をインストールしている場合、最初にConnectをアンインストールするか、Connect 4.11以降にアップグレードする必要があります。詳細については、Tanium Connectユーザーガイド：Connectのアンインストールまたは Tanium Connectユーザーガイド：Connectをアップグレードするを参照してください。

Reputationのインポート

[Tanium Solutions (Taniumソリューション)]ページからReputationをインポートします。

1. メインメニューから、**[Tanium Solutions (Taniumソリューション)]**をクリックします。
2. **[Tanium Content (Taniumコンテンツ)]**セクションで、Reputation行を選択し、**[Import Solution (インポートソリューション)]**をクリックします。
3. **[Content Import Preview (コンテンツインポートのプレビュー)]**ウィンドウでパッケージを展開して、インストールされるTaniumコンテンツを確認することができます。**[Proceed with Import (インポートを続行)]**をクリックします。
4. インストール処理が完了したら、ブラウザをリフレッシュします。
5. メインメニューから、**[Tanium Services (Taniumサービス)] > [Reputation]**をクリックします。Reputationのホームページが表示されます。

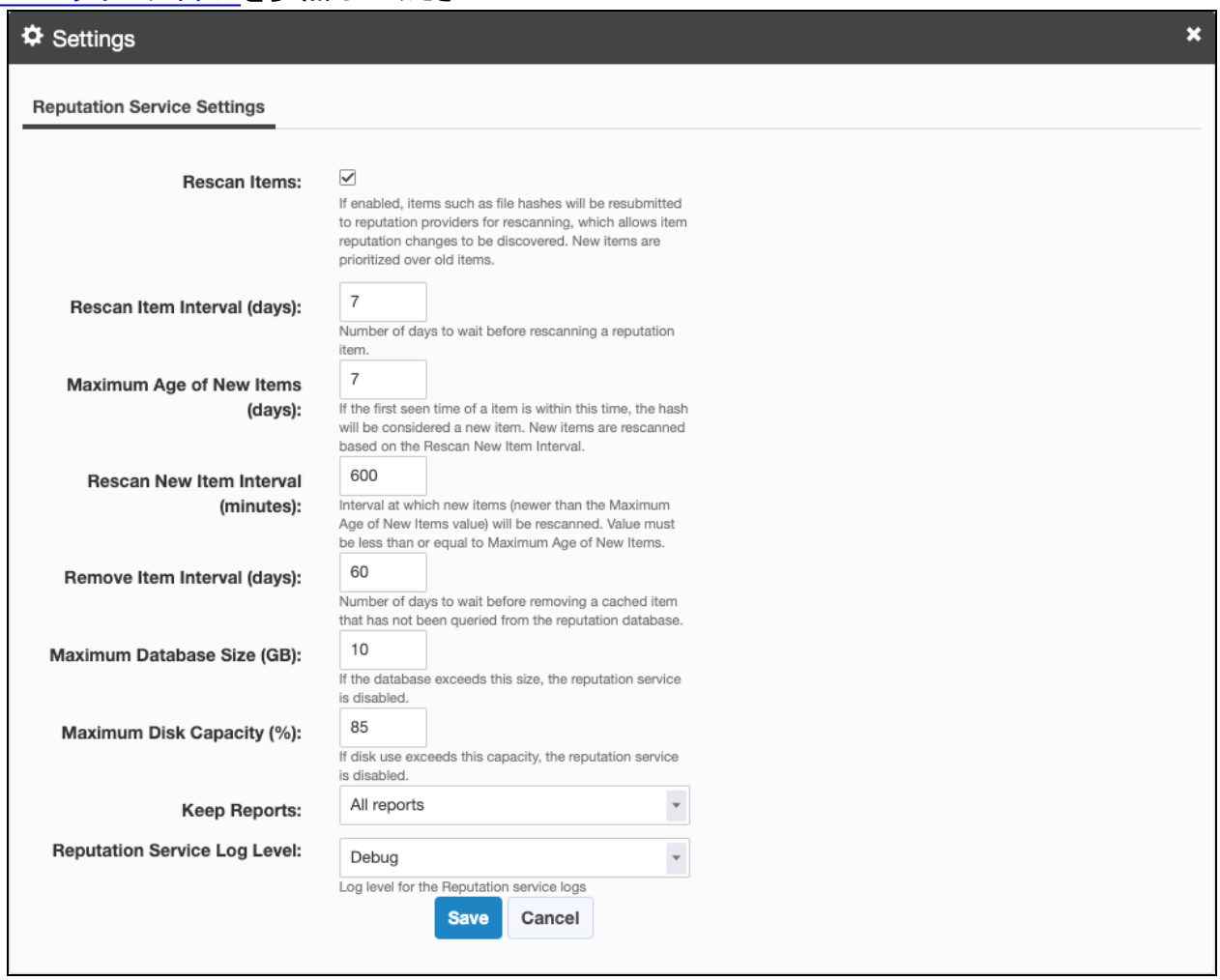
インストールを検証する

Reputationがインストールされていることを検証するには、**[Tanium Solutions (Taniumソリューションページ)]**ページに移動し、インストール済みのバージョンを確認します。

レピュテーションサービスの設定を構成する

レピュテーションサービスの設定によって、レピュテーションデータベースの内容が決まります。これらの設定は、レピュテーションソースでスキャンされるレピュテーションアイテムの頻度、新しいアイテムとしてのアイテムの長さ、およびレピュテーションステータスが参照されていない場合にアイテムをデータベースに保持する期間を決定します。これらの設定の詳細、およびこれらの設

定 がレピュテーションアイテムにどのように影 響 するかについては、6ページのレピュテーションアイテムのライフサイクルを参 照してください。



これらの設 定 を更 新 するには、設 定 をクリックします。

[Keep Reports (レポートを保 持)]設 定 は、レピュテーションソースからの完 全 なレポートをレピュテーションデータベースに保 存 するかどうかを決 定 します。すべてのレポートを保 持 するか、悪 意 のある、疑 わしいレポートのみを保 持 するかを選 択 できます。悪 意 のある、疑 わしいレポートだけを選 択 すると、データベースのスペースを節 約 できます。VirusTotalを接 続 元 として使 用 している場 合 は、レポートを保 持 オプションを使 用 して、拡 張 レポート情 報 を取 得 します。

次にやるべきこと

Reputationの使 用 については、10ページのはじめにを参 照してください。

connectデータの構成

Reputationは、特定のファイルハッシュに関する脅威情報をレピュテーションプロバイダに照会するサービスです。1つ以上のレピュテーションソースを設定して、レピュテーションデータのリポジトリを構築できます。

Palo Alto Networks WildFireレピュテーションソースを構成する

Palo Alto Networksのファイアウォールセキュリティポリシーを使用して疑わしいファイルを取得し、脅威分析のためにそれらをWildFireシステムに転送することができます。ファイルがマルウェアである場合、そのステータスがファイアウォールに報告されます。

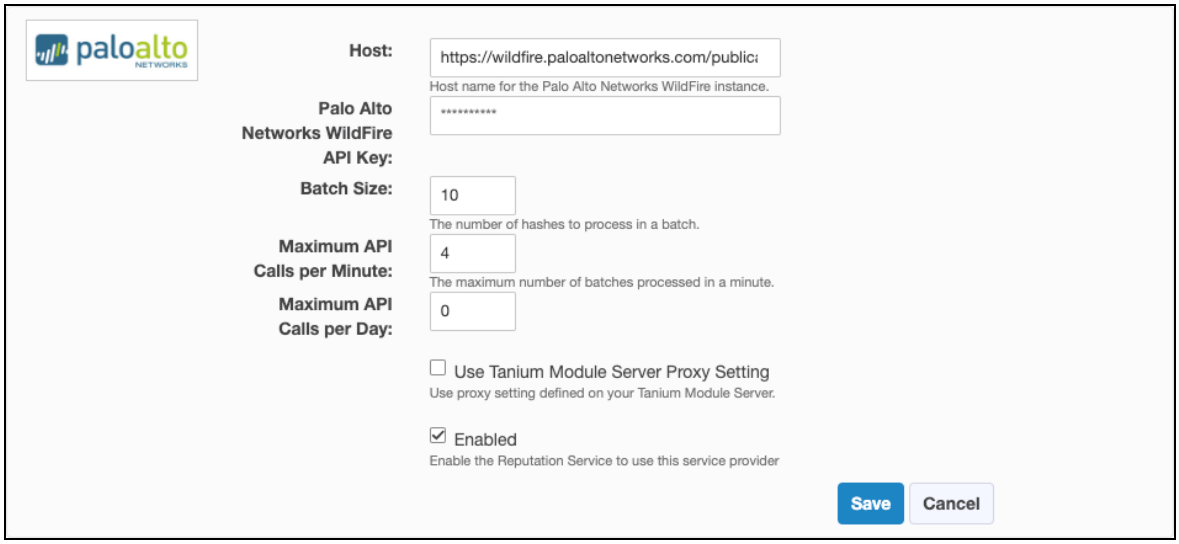
WildFire分析が完了すると、レピュテーションサービスは結果を照会し、レピュテーションデータを更新できます。

前提条件

- Cloud WildFire (wildfire.paloaltonetworks.com)または設定済みのWF-500 WildFireアプライアンスへの登録。
- Palo Alto Networksファイアウォール(Panorama有り/無し)

設定を構成する

1. ReputationホームページのPalo Alto Networks WildFireセクションで、設定 をクリックします。



2. WildFireインスタンスのホストとAPIキーを含む設定を指定します。

3. **[Enabled (有効)]**を選択し、レピュテーションソースを有効にし、**[Save (保存)]**をクリックします。

ReversingLabs A1000レピュテーションソースを構成する

ReversingLabsは企業がローカルにインストールしてファイルを分析し、API要求やWebインターフェイスを通じてレピュテーション結果を提供するアプリケーションです。

前提条件

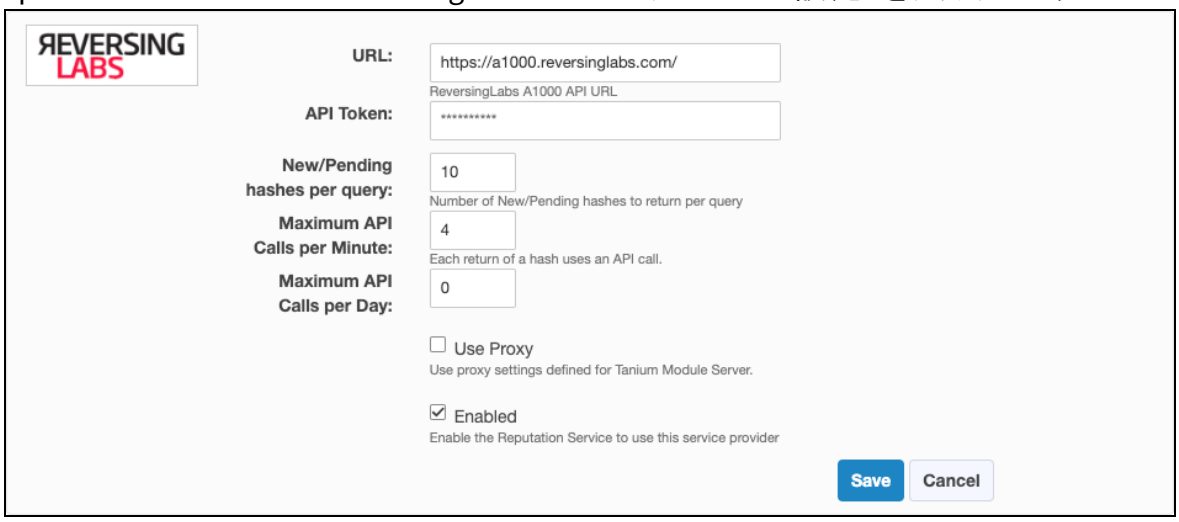
すでにReversingLabs APIトークンを持っている必要があります。ReversingLabsのアクセス権をまだ登録していない場合は、reversinglabs.comでセールスチームに連絡してください。

APIキーを取得するには:

1. ReversingLabsにログインします。
2. ユーザープロファイルアイコンをクリックします。
3. **[Administration (管理)]**を選択します。
4. **[Token (トークン)]**をクリックします。

設定を構成する

1. ReputationホームページのReversingLabs A1000セクションで、設定 をクリックします。



2. ReversingLabs A1000の資格情報を追加してください: APIへのアクセス**[URL]**と**[API Token (APIトークン)]**。
3. **[New/Pending hashes per query (クエリごとに新規/保留中のハッシュ数)]**と**[New/Pending queries per minute (1分あたりの新規/保留中のクエリ数)]**をReversingLabsとのAPI契約およびお客様のネットワーク要件に従って調整します。

4. **[Enabled (有効)]**を選択し、レピュテーションソースを有効にし、**[Save (保存)]**をクリックします。

ReversingLabsのTitaniumCloudレピュテーションソースを構成する

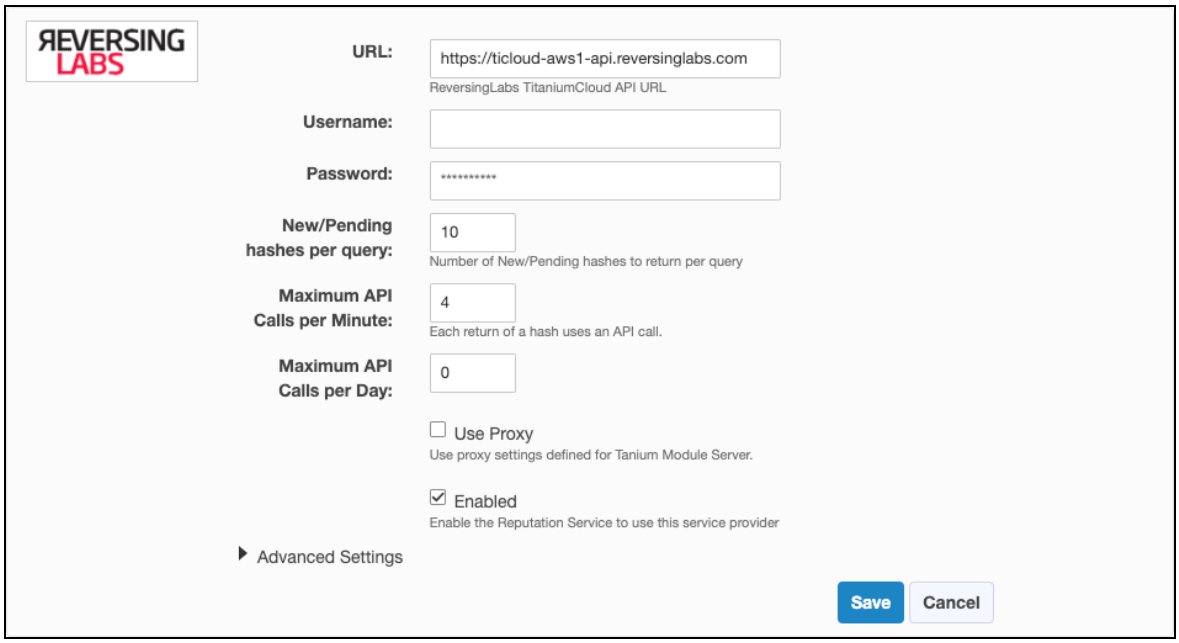
ReversingLabs TitaniumCloudは、ウイルス、ワーム、トロイの木馬、およびウイルス対策エンジンやWebサイトスキャナによって検出されるその他の種類の悪意のあるコンテンツを識別するためのファイル、ハッシュ、およびURLを分析するオンラインサービスです。レピュテーションサービスは、レピュテーションアイテムをReversingLabs APIに送信し、その結果をレピュテーションデータベースに返します。

前提条件

ReversingLabs TitaniumCloudアカウントをすでに持っている必要があります。ReversingLabs TitaniumCloudのアクセス権をまだ登録していない場合は、reversinglabs.comでセールスチームに連絡してください。

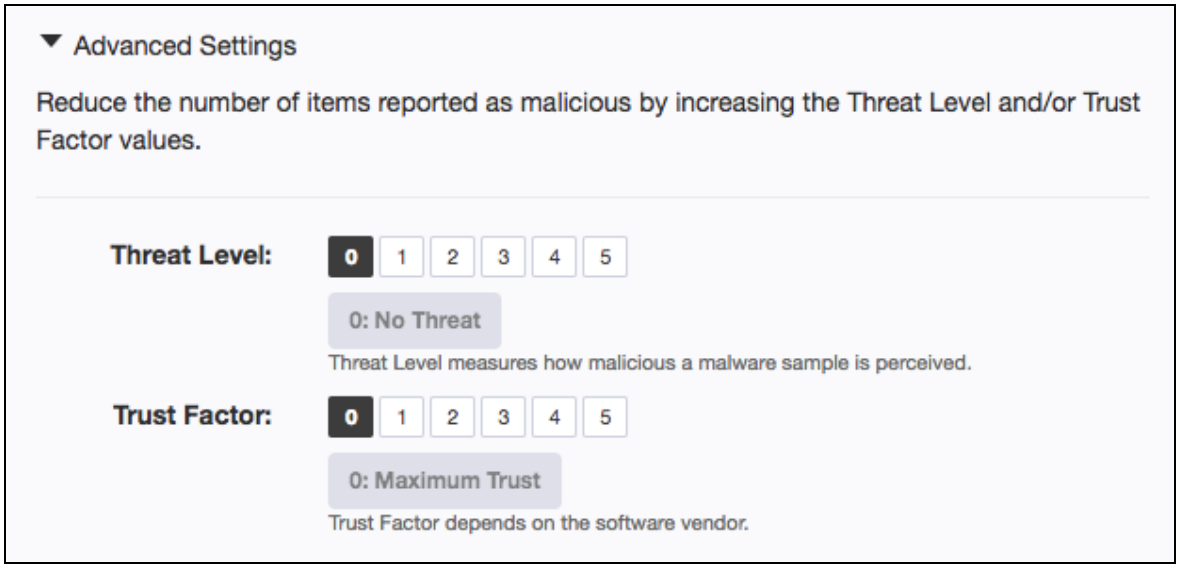
設定を構成する

1. ReputationホームページのReversingLabs TitaniumCloudセクションで、設定 をクリックします。



2. ReversingLabs TitaniumCloudの資格情報を追加する: APIアクセス用**[URL]**、**[Username (ユーザー名)]**、**[Password (パスワード)]**。

3. **[New/Pending hashes per query (クエリごとに新規/保留中のハッシュ数)]**と**[New/Pending queries per minute (1分あたりの新規/保留中のクエリ数)]**をReversingLabsとのAPI契約およびお客様のネットワーク要件に従って調整します。
4. 悪意があると報告されたアイテムの数を減らすには、**[Advanced Settings (高度な設定)]**を展開して**[Threat Level (脅威レベル)]**と**[Trust Factor (トラストファクター)]**の設定を調整します。



> **ヒント：[Threat Level (脅威レベル)]**を`0`に、**[Trust Factor (トラストファクター)]**を`0`に設定すると、最大数の悪意のあるアイテムに関するレポートが発生します。**[Threat Level (脅威レベル)]**を`5`に、**[Trust Factor (トラストファクター)]**を`5`に設定すると、最少数の悪意のあるアイテムに関するレポートが発生します。

5. **[Enabled (有効)]**を選択し、レピュテーションソースを有効にし、**[Save (保存)]**をクリックします。

VirusTotalレピュテーションソースを構成する

VirusTotalは、ウイルス、ワーム、トロイの木馬、およびウイルス対策エンジンやWebサイトスキャナによって検出されるその他の種類の悪質なコンテンツを特定するためのファイル、ハッシュ、およびURLを分析するオンラインサービスです。レピュテーションサービスはレピュテーションアイテムをVirusTotal APIに送信し、結果をレピュテーションデータベースに返します。

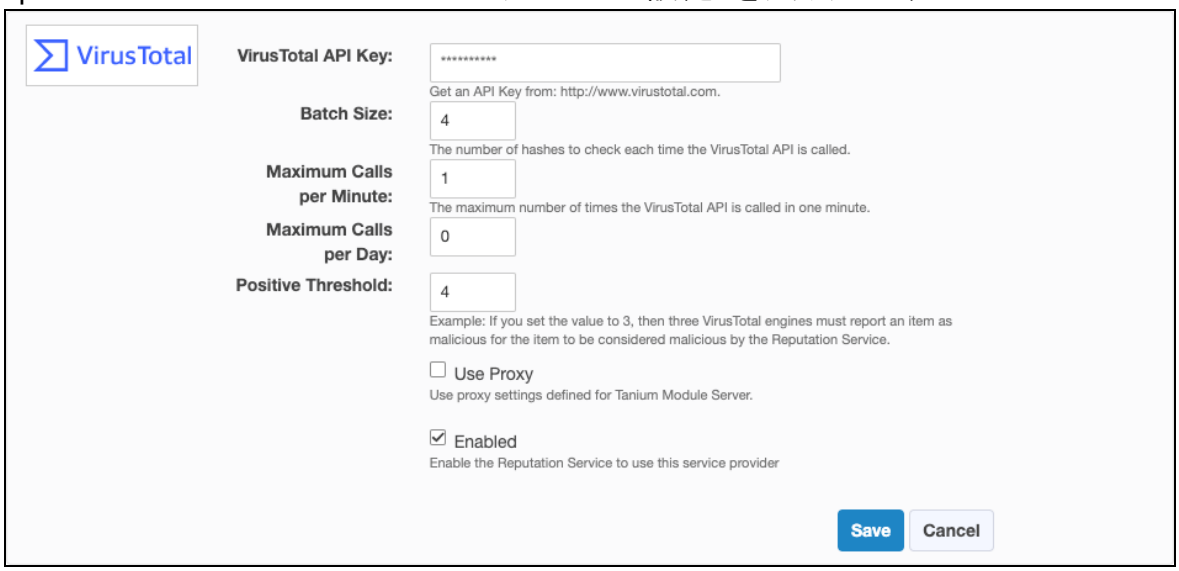
前提条件

VirusTotal APIキーをvirustotal.comで登録します。VirusTotalは、APIキーを使用してカタログにクエリを提供します。適切なAPIキーの種類を判断するには、VirusTotal APIの使用ポリシーを参照してください。

VirusTotalウェブサイトでAPIキーを取得するには、ログインして*[your_user_image]* > **[Settings (設定)]** > **[API Key (APIキー)]**をクリックします。

設定を構成する

1. ReputationホームページのVirusTotalセクションで、設定 をクリックします。



2. APIキーを含むVirusTotalの設定を指定します。
   - **[Batch Size (バッチサイズ)]**と**[Maximum Calls per Minute (1分あたりの最大通話数)]**の設定をVirusTotalとの契約に基づいて調整します。
   - **[Positive Threshold (陽性のしきい値)]**は潜在的な脅威またはマルウェアとみなされるためにハッシュ上になければならない陽性レポート数です。

     > **ヒント：** 値が低く設定されている場合、VirusTotalレポートに偽陽性のものが含まれている可能性が高くなります。

     例： 値を`3`に設定した場合、3つのVirusTotalエンジンは、アイテムを悪意のあると報告してアイテムをConnectに送信する必要があります。
     値を`0`に設定すると、しきい値が無効になります。VirusTotalエンジンが悪意のあるアイテムとして報告すると、そのアイテムはConnectに送信されます。

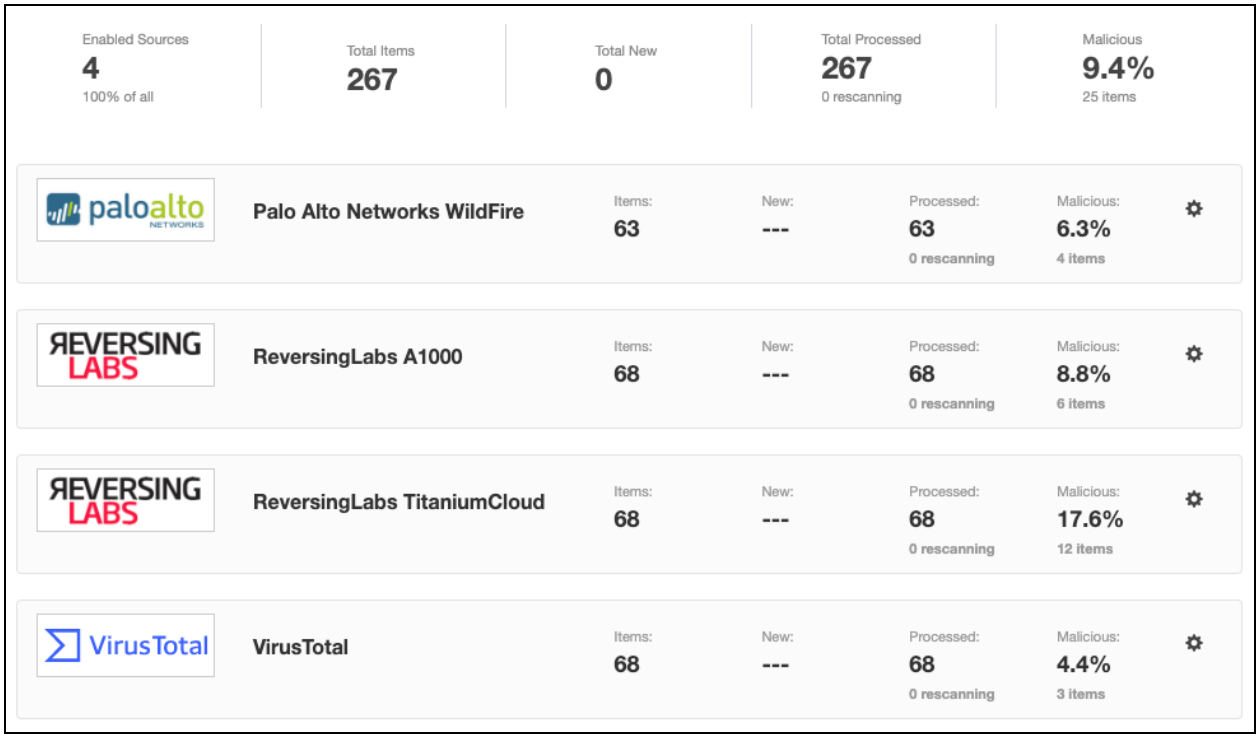
     VirusTotalのレピュテーションの結果は次のように決定されます。

- Malicious (悪意のあるもの): 陽性の数がしきい値より大きい場合
- Suspicious (疑わしいもの): 陽性の数がゼロよりも大きいが、しきい値よりも小さい場合
- Non-malicious (悪意のないもの): 陽性の数がゼロの場合
- Unknown (不明): データがない場合

3. **[Enabled (有効)]**を選択し、レピュテーションソースを有効にし、**[Save (保存)]**をクリックします。

レピュテーションスキャンのステータスを表示する

Reputationホームページページには、レピュテーションアイテムの総数、および各レピュテーションソースに関する次の情報が表示されます。



- **Items (アイテム)**: このレピュテーションソースのレピュテーションアイテムの合計数
- **New (新規)**: このレピュテーションソースでスキャンする必要があるレピュテーションアイテム
- **Processed (処理済み)**: このレピュテーションソースでスキャンされたレピュテーションアイテム
- **Malicious (悪意のある)**: 全レピュテーションアイテムのうちの悪意のあるアイテムの割合

ホワイトリストまたはブラックリストデータの管理

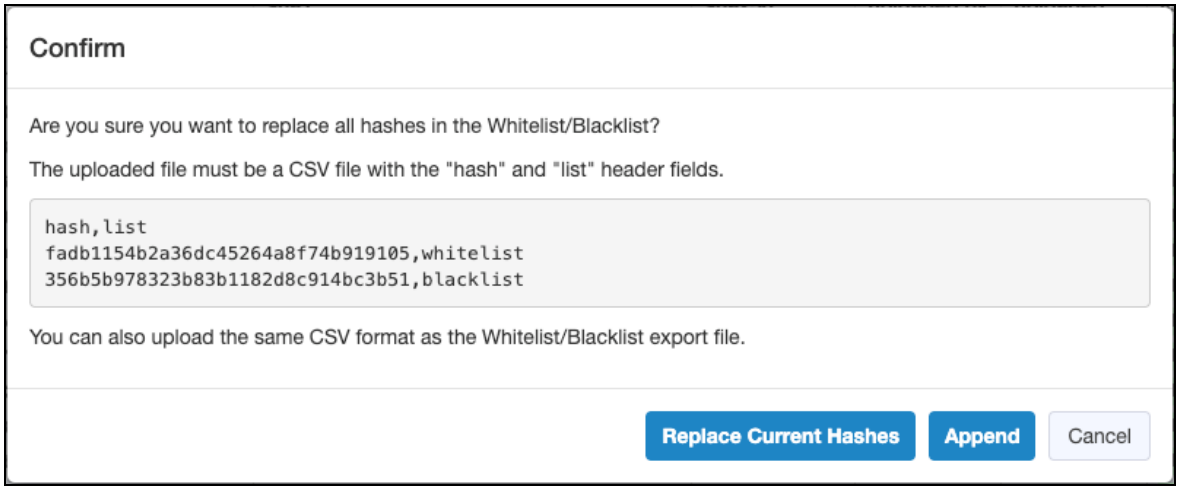
ホワイトリストまたはブラックリストに登録されているハッシュのリストを表示するには、Reputationホームページから**[Whitelist/Blacklist (ホワイトリスト/ブラックリスト)]**をクリックします。ファイルハッシュを検索、レピュテーションの追加、インポート、エクスポート、または削除をすることもできます。

データハッシュの追加

1. Reputationホームページから、**[Whitelist/Blacklist (ホワイトリスト/ブラックリスト)]**をクリックし、次に**[Add Hashes (ハッシュを追加)]**をクリックします。
2. ブラックリストに悪意あるものとして知られているハッシュを追加するには、ハッシュを入力し、**[Blacklist (ブラックリスト)]**を選択してから**[Save to Blacklist (ブラックリストに保存)]**をクリックします。
3. ホワイトリストに誤検出であることが判明しているハッシュを追加するには、ハッシュを入力し、**[Whitelist (ホワイトリスト)]**を選択してから**[Save to Whitelist (ホワイトリストに保存)]**をクリックします。

ハッシュをインポート

1. Reputationホームページから、**[Whitelist/Blacklist (ホワイトリスト/ブラックリスト)]**をクリックして、次に**[Import Hashes (ハッシュをインポート)]**をクリックします。



2. 現在のハッシュを置き換えるには、**[Replace Current Hashes (現在のハッシュを置き換える)]**をクリックし、CSV形式のファイルまたは以前にエクスポートされたホワイトリスト/ブラックリストを選択します。
3. 現在のハッシュを追加するには、**[Append (追加)]**をクリックし、CSV形式のファイルまたは以前にエクスポートされたホワイトリスト/ブラックリストを選択します。

> **注意：** Reputationは、異なるタイプのハッシュが同じファイルを表すときに、サービスプロバイダから学習することによって、重複レコードの統合を自動的に処理します。

手動でハッシュを統合する場合は、既存のホワイトリスト/ブラックリストファイルをエクスポートし、そのファイルを編集して特定の行の適切な列にハッシュを追加し、**[Replace Current Hashes (現在のハッシュを置き換える)]**オプションを使用して更新したファイルをインポートします。

ハッシュのエクスポート

1. Reputationホームページから、**[Whitelist/Blacklist (ホワイトリスト/ブラックリスト)]**をクリックします。
2. 特定のハッシュをエクスポートするには、1つ以上のハッシュを選択し、エクスポート をクリックします。
3. すべてのハッシュをエクスポートするには、**[Download All (すべてダウンロード)]**をクリックします。

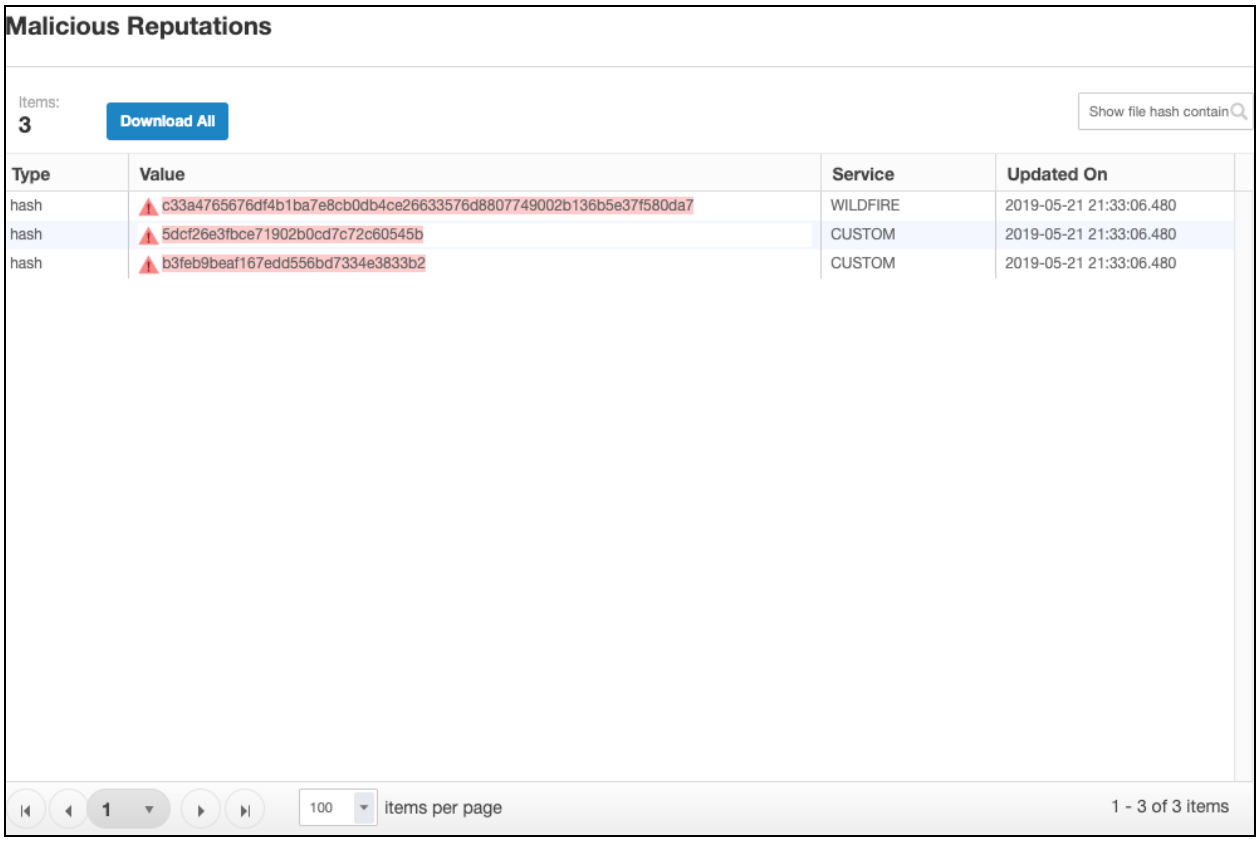
ハッシュを削除

1. Reputationホームページから、**[Whitelist/Blacklist (ホワイトリスト/ブラックリスト)]**をクリックします。
2. 特定のハッシュを削除するには、1つ以上のハッシュを選択し、削除 をクリックします。
3. すべてのハッシュを削除するには、**[Delete All (すべて削除)]**をクリックします。

connectデータのエクスポート

レピュテーションデータを表示する

Reputationがレピュテーションサービスから取得した悪意のあるハッシュのリストを表示するには、Reputationメニューから**[Malicious Reputations (悪意のあるレピュテーション)]**をクリックします。



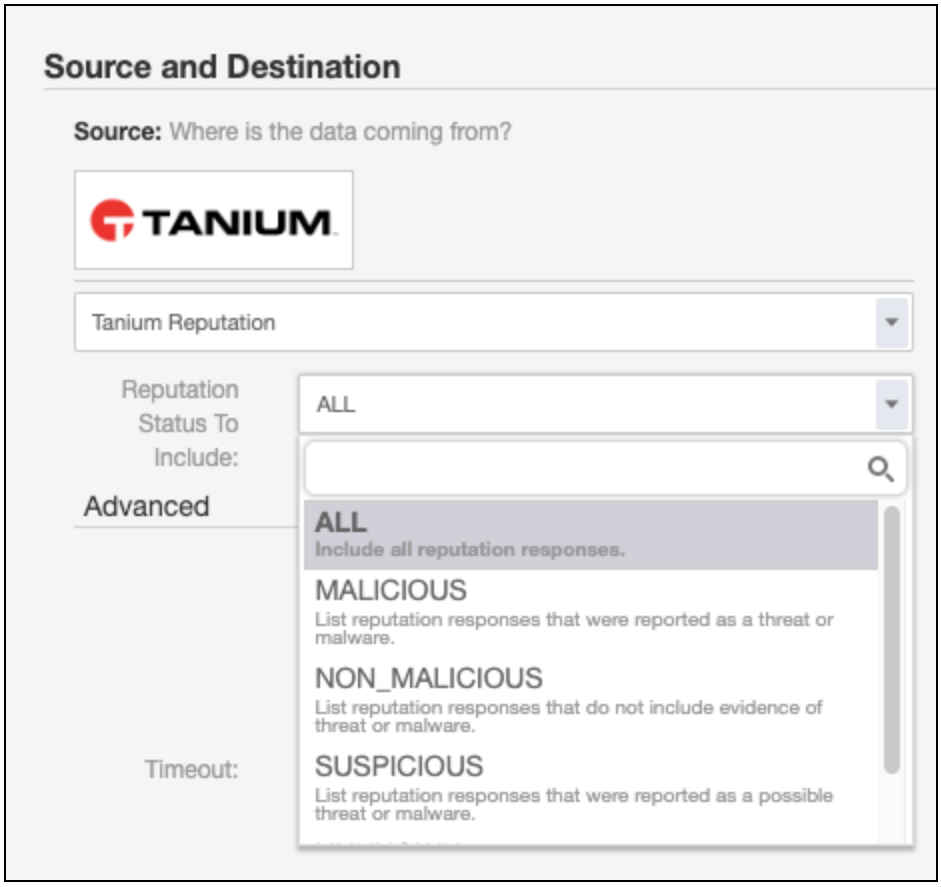
悪意のあるステータスまたは保留ステータスのハッシュのみがリストされます。

トレースでは、ライブエンドポイントまたはスナップショットのハッシュ評価を表示できます。詳細については、Tanium Traceユーザーガイド：Traceでレピュテーションデータがどのように機能するかを参照してください。

レピュテーションデータを接続先に送信する

Connect 4.11以降を使用して、レピュテーションデータベースにあるデータを任意のConnectに送信するための接続を作成できます。たとえば、悪意のあるアイテムが見つかった場合に電子メール通知を作成するように接続を構成することができます。

1. Connectメニューで**[Connections (接続)]**をクリックします。
2. **[Create Connection (接続の作成)] > [Create (作成)]**をクリックし、新規の接続を作成します。
3. 接続元を選択する際、**[Tanium Reputation]**を選択します。



含めるレピュテーションステータスを選択することもできます。

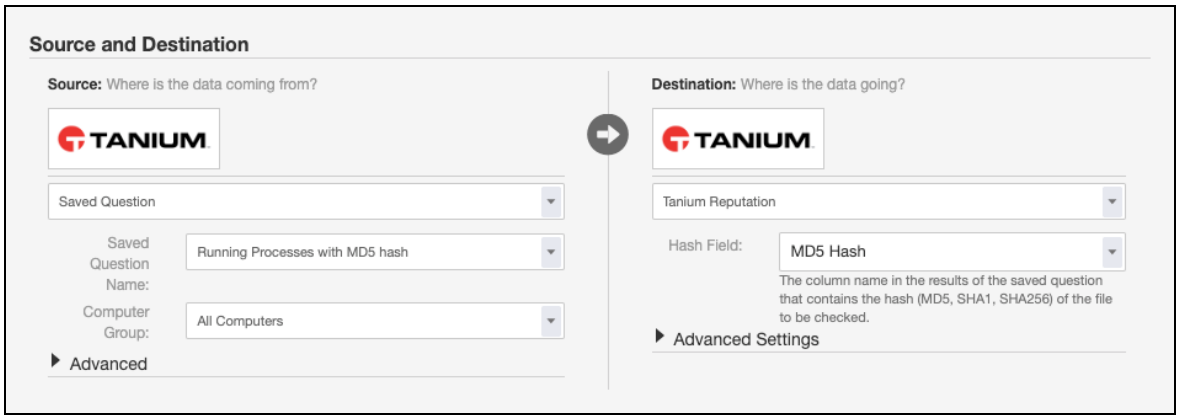
4. その接続の接続先設定を構成します。

注意：送信元として**[Tanium Reputation]**を使用する接続を初めて実行すると、使用可能なすべてのレピュテーションアイテムが取得されます。その後の接続の実行では、最後に接続が実行されてからのレピュテーションの変更のみが取得されます。

レピュテーションサービスにデータを送信する

環境からのハッシュを使用してレピュテーションデータを事前入力する場合は、レピュテーションサービスに接続先としてデータを送信できます。このコンテンツが事前設定されている場合、レピュテーションサービスは、レピュテーションソースからのアイテムのステータスを照会することができます。

1. Connectメニューで**[Connections (接続)]**をクリックします。
2. **[Create Connection (接続の作成)] > [Create (作成)]**をクリックし、新規の接続を作成します。
3. ソースについては、**[Running Processes with MD5 Hash (ハッシュを使用して実行中のプロセス)]**など、ハッシュを返す保存されたQuestionを選択します。
4. 送信先については、**[Tanium Reputation]**を選択し、**[Hash Field (ハッシュフィールド)]**の適切なハッシュタイプを選択します。



重要：各レピュテーションサービス接続先は、特定のハッシュ列名用に構成されています。入力する各ハッシュタイプに対して、別々の送信先を使用する必要があります。たとえば、異なる保存されたQuestionからMD5とSHA1の両方のハッシュを作成する場合、**[Hash Field (ハッシュフィールド)]**の異なる値を持つ2つの接続先を作成します。

Reputationのトラブルシューティング

トラブルシューティングのために情報を収集してTaniumに送信するには、ログなどの関連情報を収集します。

ログを収集する

情報は、ブラウザでダウンロードできるZIPファイルとして保存されます。

1. ProductNameのホームページからヘルプ をクリックし、**[Troubleshooting (トラブルシューティング)]**タブをクリックします。
2. **[Collect (収集)]**をクリックします。`reputation-support.[timestamp].zip`ファイルがローカルのダウンロードディレクトリにダウンロードされます。
3. Taniumサポートケースフォームにzipファイルを添付するか、担当のテクニカルアカウントマネージャに送信してください。

Tanium Reputationは、`reputation-service.log`ファイルにログ情報を保存しています(ファイルの場所：`\Program Files\Tanium\Tanium Module Server\services\reputation-service`ディレクトリ)。

Reputationのアンインストール

基本的なReputation共有サービスのアンインストールは、後でReputationの再インストールを決定した場合に収集したデータが復元されるように設計されています。「クリーン」を開始し、データを復元したくない場合もあります。これを行うには、手動でいくつかのファイルを削除する必要があります。

> **重要：** Reputationをアンインストールまたは再インストールする前に、テクニカルアカウントマネージャに相談してください。

再インストール時にデータが復元されるようにReputationをアンインストールする

1. 管理者ロールを持つユーザーとして、Tanium Consoleにサインインします。
2. メインメニューから、**[Tanium Solutions (Taniumソリューション)]**をクリックします。
3. **[Tanium Solutions (Taniumソリューション)]**セクションで、**[Reputation]**行を選択し、**[Uninstall Solution (ソリューションをアンインストール)]**を選択します。

4. サマリを確認して[**Proceed with Uninstall (アンインストールを続行)**]をクリックします。
5. 確認のプロンプトが表示されたら、パスワードを入力します。

後でReputation共有サービスをインポートすると、前のデータが復元されます。

再インストールするときに最初から始められるようにReputationをアンインストールする

1. 27ページの再インストール時にデータが復元されるようにReputationをアンインストールする。
2. `\Program Files\Tanium\Tanium Module Server\services\reputation-files\`ディレクトリを手動で削除します。

`reputation-files`ディレクトリを削除すると、既存のすべてのReputationデータが削除されます。ログ、出力、Reputationデータベース、およびその他のReputationデータはすべて削除されます。後でReputation共有サービスをインポートしても、前のデータは復元されません。