

# SentinelOne

## 導入開始手順

株式会社TTM

2019/11/21

Rev.1.0.4

# 本ガイドの趣旨

本ガイドは、SentinelOneを導入する企業のシステム管理者様向けの内容です。利用開始前にすべてのページをお読みください。

ご不明な点は、メールもしくはチャットでお問い合わせください。

[SentinelOneサポートセンター]

LINE公式： <https://lin.ee/4nAgjm0>

Email: [support@to-tm.com](mailto:support@to-tm.com)

TEL: 03-6823-5903



LINE公式  
サポート窓口

# Index

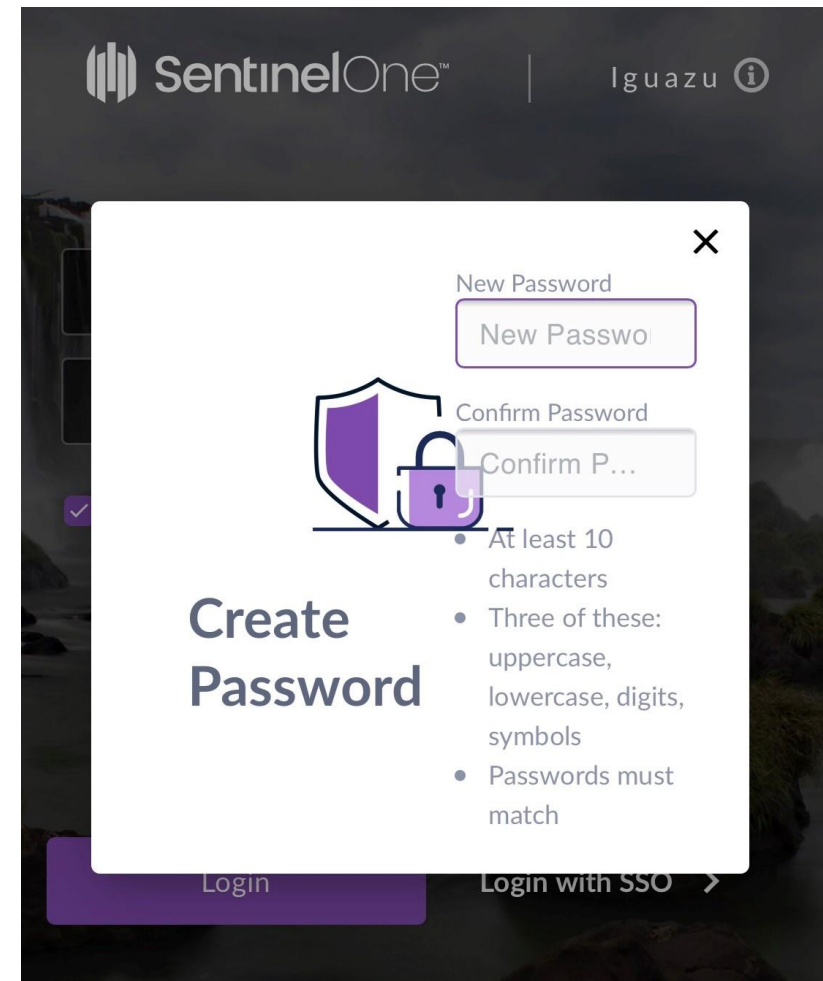
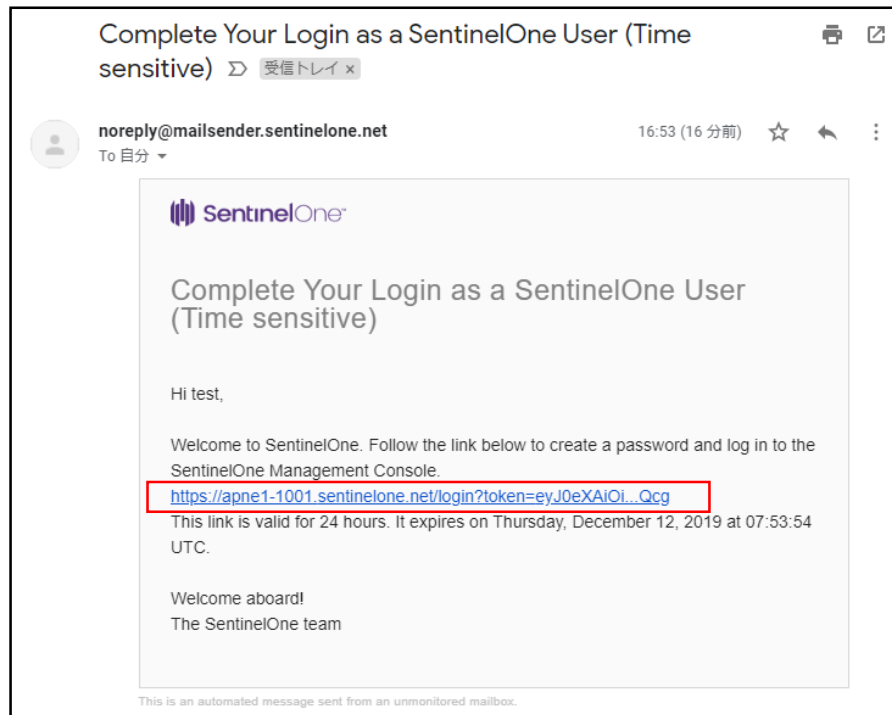
1. パスワードの設定
2. 管理画面にログイン
3. パスワードの変更
4. 管理者の追加
5. サイトを選択
6. インストーラを入手
7. トークンを入手
8. インストール作業
9. デバイスの確認
10. アラートメールの設定
11. 自動対応モードへの移行

# パスワード設定メール

パスワードを設定

- ・ 10文字以上
- ・ 大文字、小文字、数字、記号のうち3種類

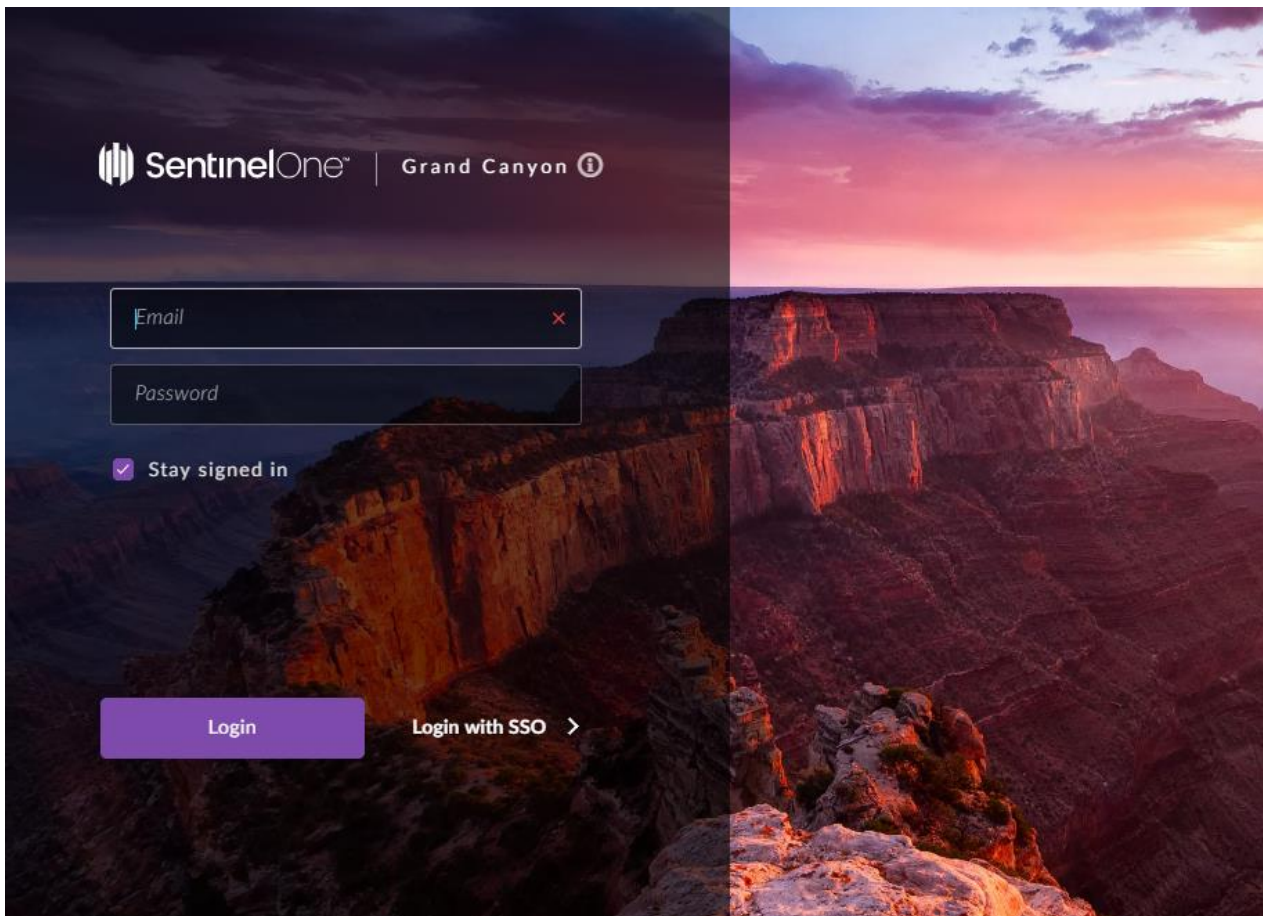
届いたパスワード設定メールのリンクをクリック



# 管理画面にログイン

管理画面URL

<https://apne1-1001.sentinelone.net>



## ログイン情報

Email	管理者様のメールアドレス
Password	メールアドレス宛にパスワード設定メールが届いているので24時間以内に登録手続きをお願いします。  期限を過ぎてしまった場合ご連絡ください。

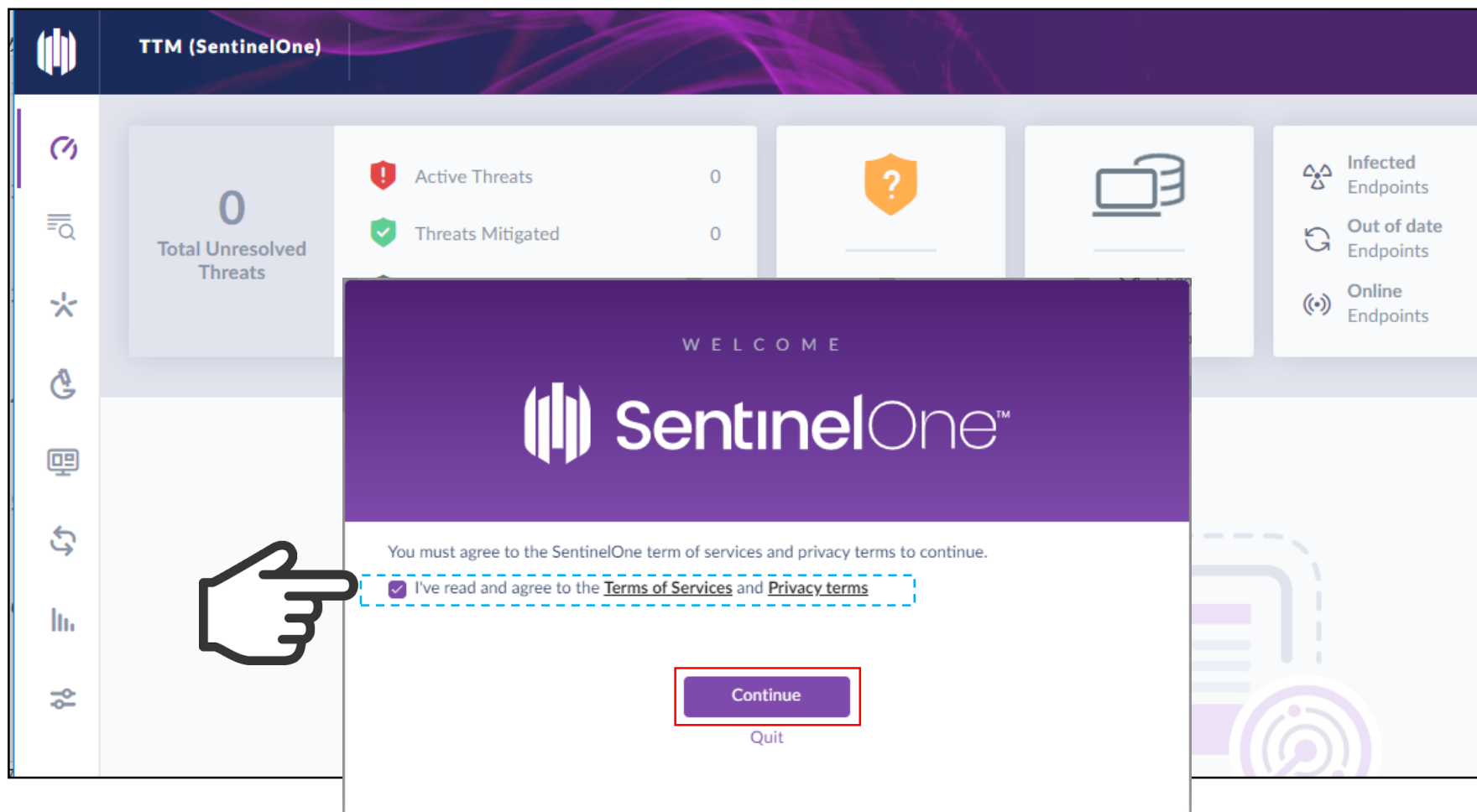
※ご不明な場合、お問い合わせください

Email: [support@to-tm.com](mailto:support@to-tm.com)

TEL: 03-6823-5903

# ログイン完了

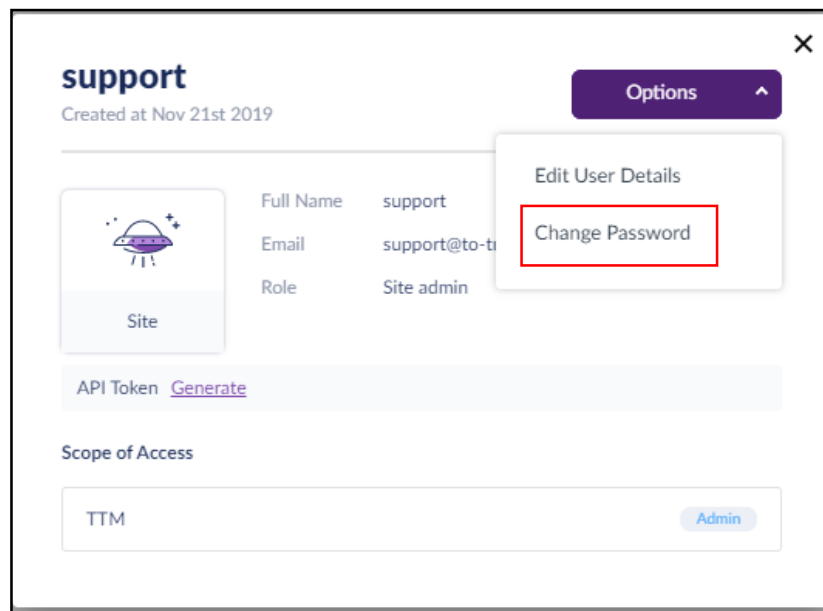
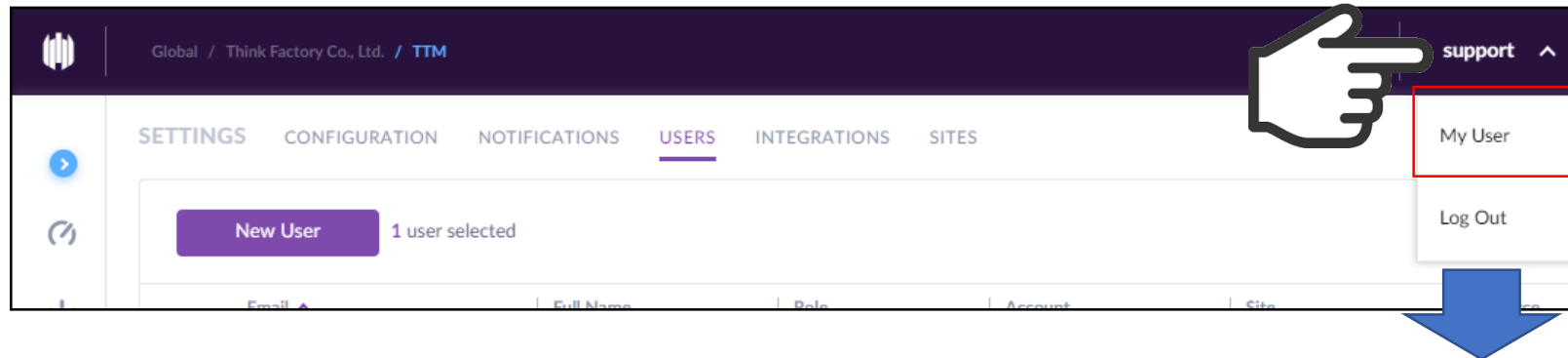
初回ログイン時のみ、利用規約に同意する必要があります。



※日本語バージョンの管理画面は近日リリース

# 管理者パスワードの変更

初回ログイン後、初期パスワードは必ず変更してください。

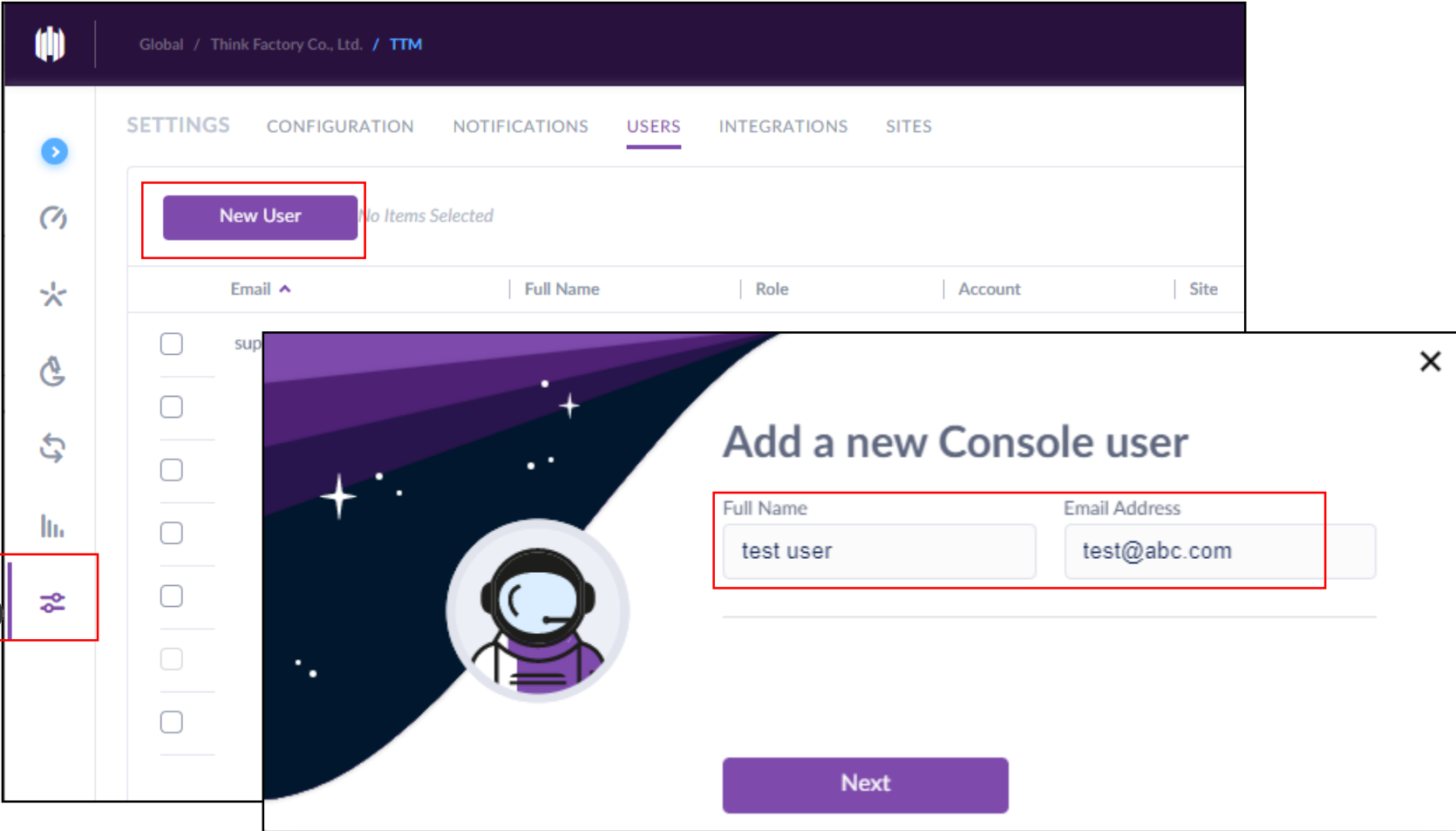


※パスワードを忘れてしまった場合、サポートまでご連絡ください。

# 管理者の追加

追加するユーザーのメールアドレスを登録 → パスワード設定メールが届く

Settings



Global / Think Factory Co., Ltd. / TTM

SETTINGS CONFIGURATION NOTIFICATIONS **USERS** INTEGRATIONS SITES

New User No Items Selected

Email ^	Full Name	Role	Account	Site
<input type="checkbox"/> sup				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

## Add a new Console user

Full Name Email Address

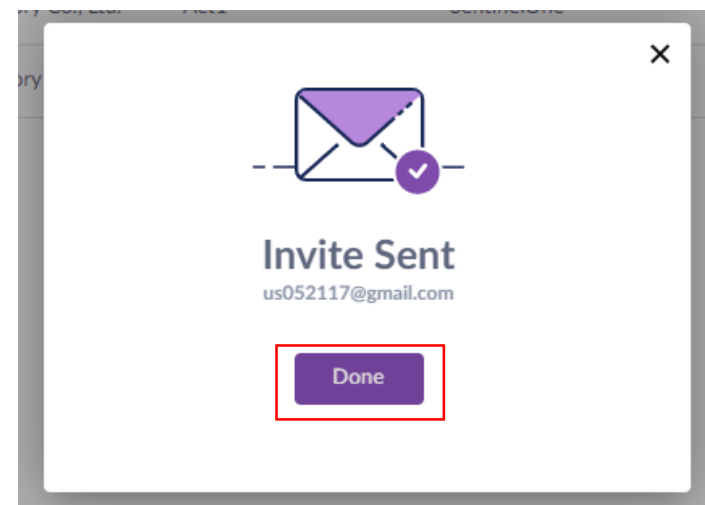
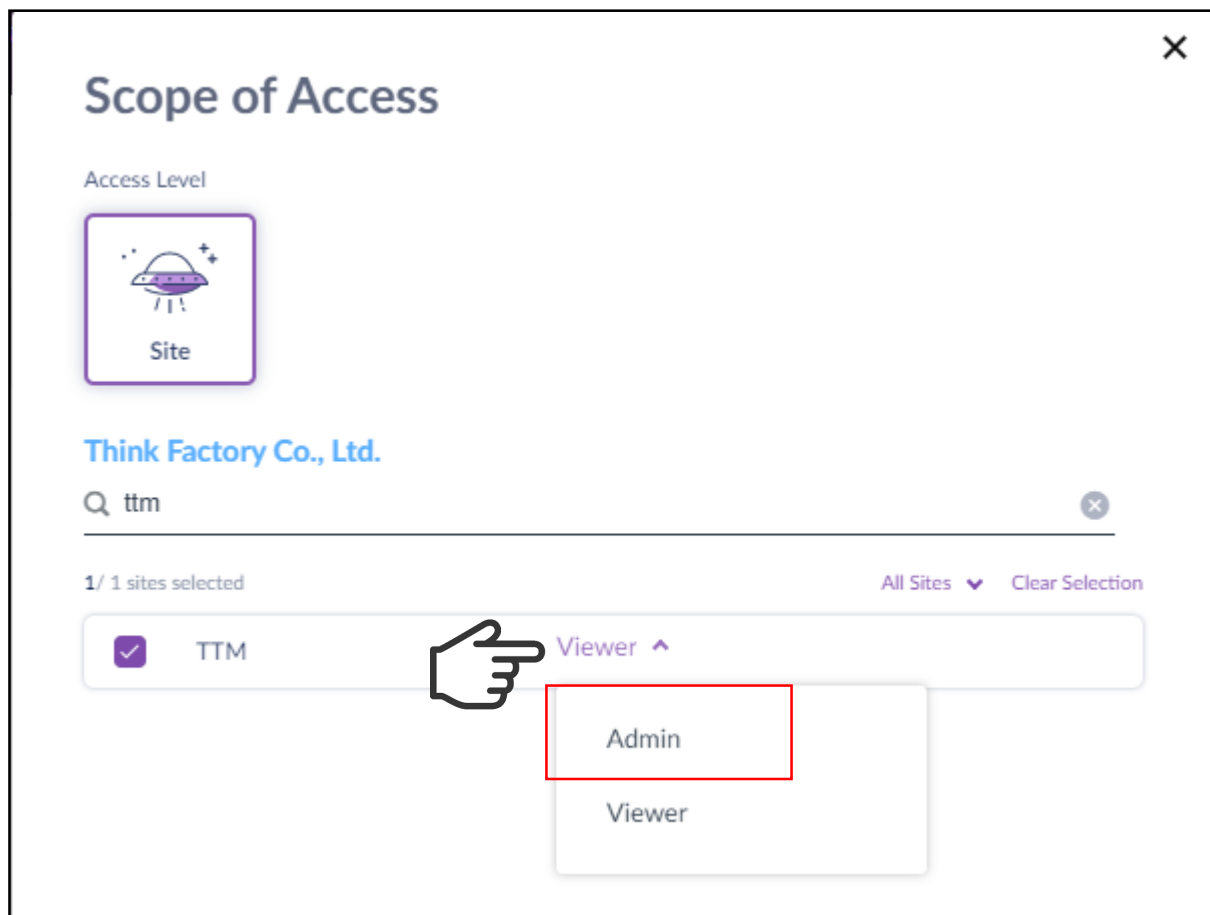
test user test@abc.com

Next



# 管理対象のサイトを指定

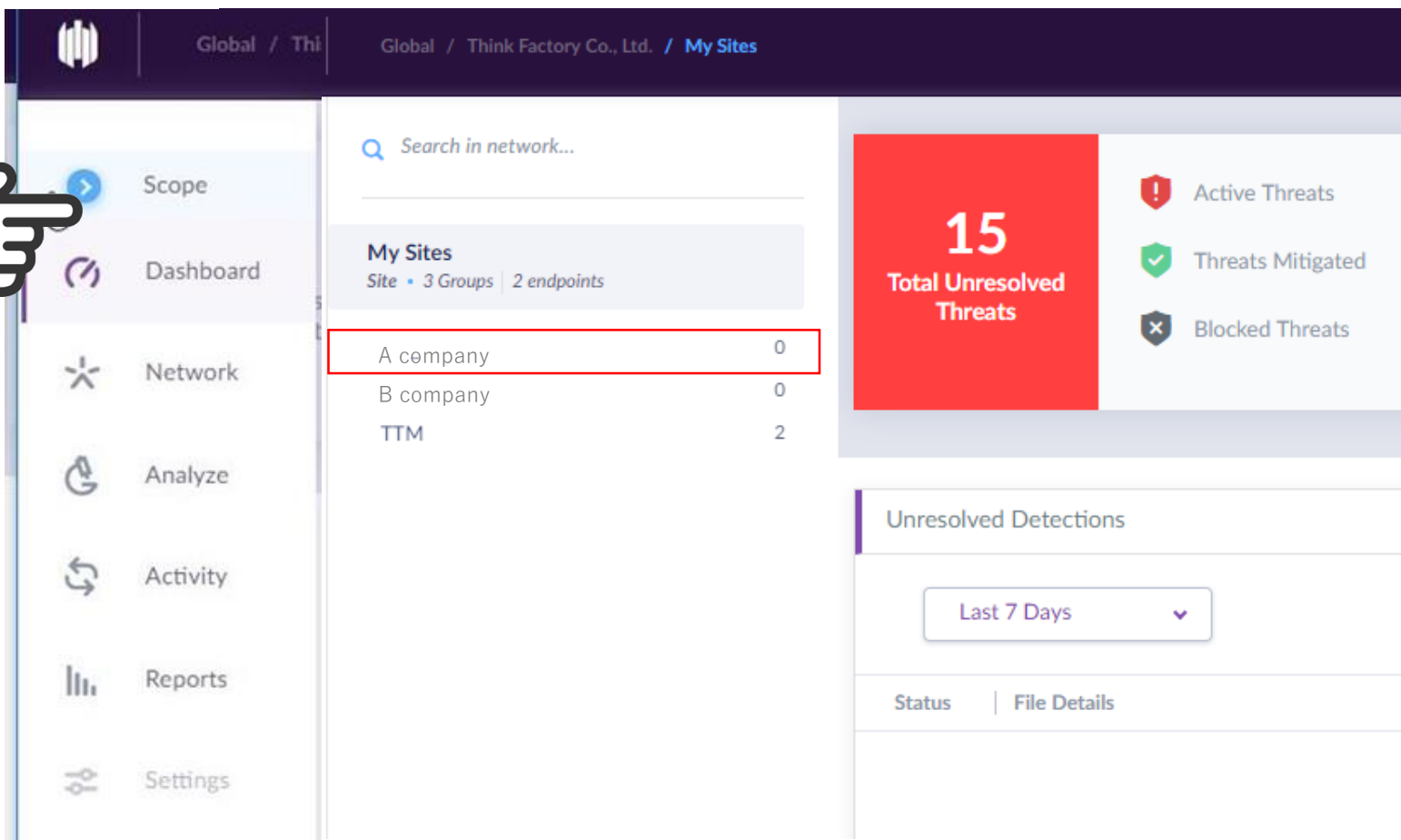
Adminを選択する事で、設定変更が可能になります。



# サイトを選択

Scopeを開き、エンドユーザーごとにテナント切り替え(複数企業で契約している場合)

Scope



The screenshot displays the 'My Sites' section of a security dashboard. The left sidebar contains a menu with 'Scope' highlighted. The main content area features a search bar, a table of sites, and a summary card for 'Total Unresolved Threats'.

My Sites	
Site • 3 Groups   2 endpoints	
A company	0
B company	0
TTM	2

Summary Card: 15 Total Unresolved Threats

- Active Threats
- Threats Mitigated
- Blocked Threats

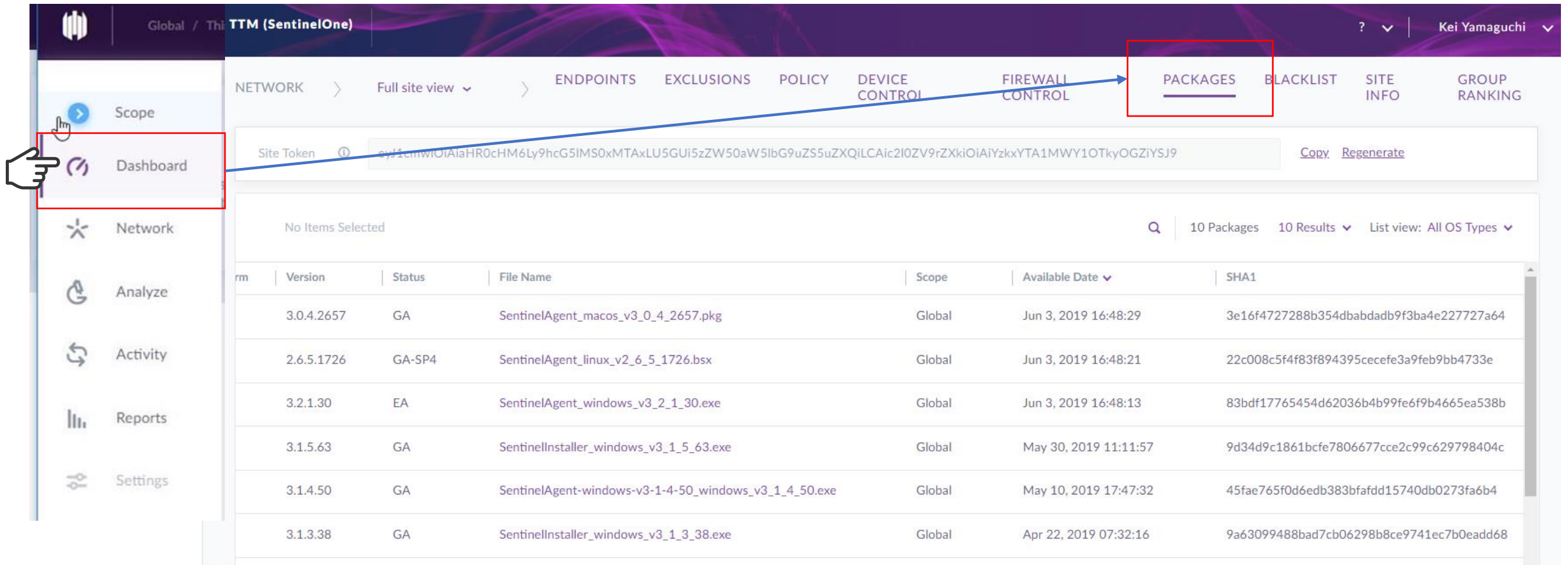
Unresolved Detections

Last 7 Days

Status | File Details

# インストーラを入手

## -Packagesを開く

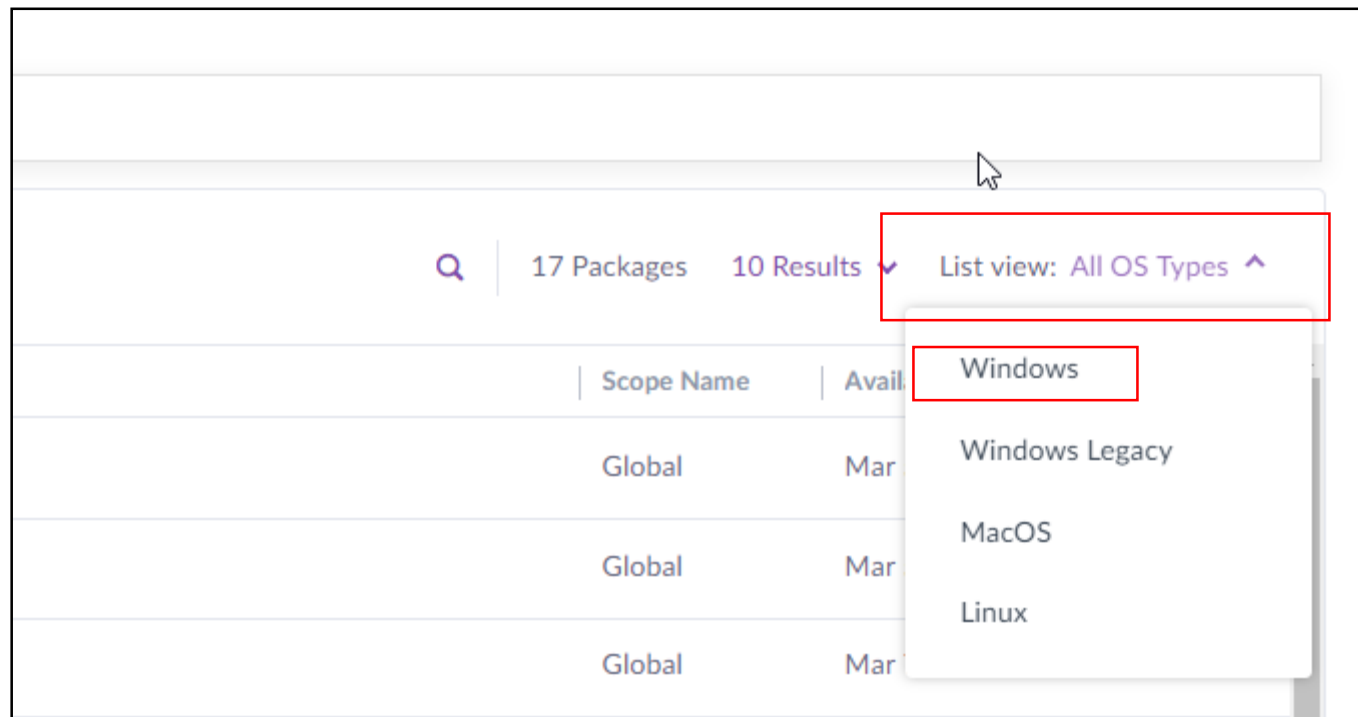


The screenshot displays the SentinelOne TTM (SentinelOne) interface. The left sidebar contains navigation options: Scope, Dashboard, Network, Analyze, Activity, Reports, and Settings. The top navigation bar includes tabs for NETWORK, ENDPOINTS, EXCLUSIONS, POLICY, DEVICE CONTROL, FIREWALL CONTROL, and PACKAGES. The PACKAGES tab is highlighted with a red box. Below the navigation bar, a Site Token is displayed with a 'Copy' and 'Regenerate' link. The main content area shows a table of installed packages. The table has columns for Name, Version, Status, File Name, Scope, Available Date, and SHA1. The table lists several packages, including SentinelAgent\_macos\_v3\_0\_4\_2657.pkg, SentinelAgent\_linux\_v2\_6\_5\_1726.bsx, SentinelAgent\_windows\_v3\_2\_1\_30.exe, SentinelInstaller\_windows\_v3\_1\_5\_63.exe, SentinelAgent-windows-v3-1-4-50\_windows\_v3\_1\_4\_50.exe, and SentinelInstaller\_windows\_v3\_1\_3\_38.exe.

Name	Version	Status	File Name	Scope	Available Date	SHA1
SentinelAgent_macos_v3_0_4_2657.pkg	3.0.4.2657	GA	SentinelAgent_macos_v3_0_4_2657.pkg	Global	Jun 3, 2019 16:48:29	3e16f4727288b354dbabdad9f3ba4e227727a64
SentinelAgent_linux_v2_6_5_1726.bsx	2.6.5.1726	GA-SP4	SentinelAgent_linux_v2_6_5_1726.bsx	Global	Jun 3, 2019 16:48:21	22c008c5f4f83f894395cecefe3a9feb9bb4733e
SentinelAgent_windows_v3_2_1_30.exe	3.2.1.30	EA	SentinelAgent_windows_v3_2_1_30.exe	Global	Jun 3, 2019 16:48:13	83bdf17765454d62036b4b99fe6f9b4665ea538b
SentinelInstaller_windows_v3_1_5_63.exe	3.1.5.63	GA	SentinelInstaller_windows_v3_1_5_63.exe	Global	May 30, 2019 11:11:57	9d34d9c1861bcfe7806677cce2c99c629798404c
SentinelAgent-windows-v3-1-4-50_windows_v3_1_4_50.exe	3.1.4.50	GA	SentinelAgent-windows-v3-1-4-50_windows_v3_1_4_50.exe	Global	May 10, 2019 17:47:32	45fae765f0d6edb383bfafdd15740db0273fa6b4
SentinelInstaller_windows_v3_1_3_38.exe	3.1.3.38	GA	SentinelInstaller_windows_v3_1_3_38.exe	Global	Apr 22, 2019 07:32:16	9a63099488bad7cb06298b8ce9741ec7b0eadd68

# インストーラを入手

- ご利用のOS種類を選択



※Windows Legacyは、XPや2003サーバーなど旧OS

# インストーラを入手

## -最新のインストーラ

“Version”のカラム名をクリックし、新しい順に並べ替える。

最新バージョン v3.4.4.51 ※2019/11/10現在

Global / Think Factory Co., Ltd. / My Sites / TTM

NETWORK ENDPOINTS EXCLUSIONS POLICY DEVICE CONTROL **PACKAGES** BLACKLIST SITE INFO GROU

Site Token eyJ1cmwiOiAiaHR0cHM6Ly9hcG5lMS0xMDAxLnNlbnRpbmVsb25lIm5ldCIsICJzaXRlX2tleSI6IChyNzVlODMzMmEyODRjNTQ2In0=

No Items Selected

Actions	Platform	Version ▼	Status	Download
	Windows	3.4.1.7	EA	SentinelAgent_windows_v3_4_1_7.exe
	Windows	3.3.3.29	GA	SentinelAgent_windows_v3_3_3_29.exe
	Windows	3.3.2.24	GA	SentinelAgent-windows-v3-3-2-24_windows_v3_3_2_24.exe
	Windows	3.2.4.54	GA	SentinelAgent_windows_v3_2_4_54.exe
	Windows	3.1.7.70	GA-SP4	SentinelAgent_windows_v3_1_7_70.exe
	Windows	3.1.5.63	GA	SentinelAgent_windows_v3_1_5_63.exe

# サイトトークンを取得

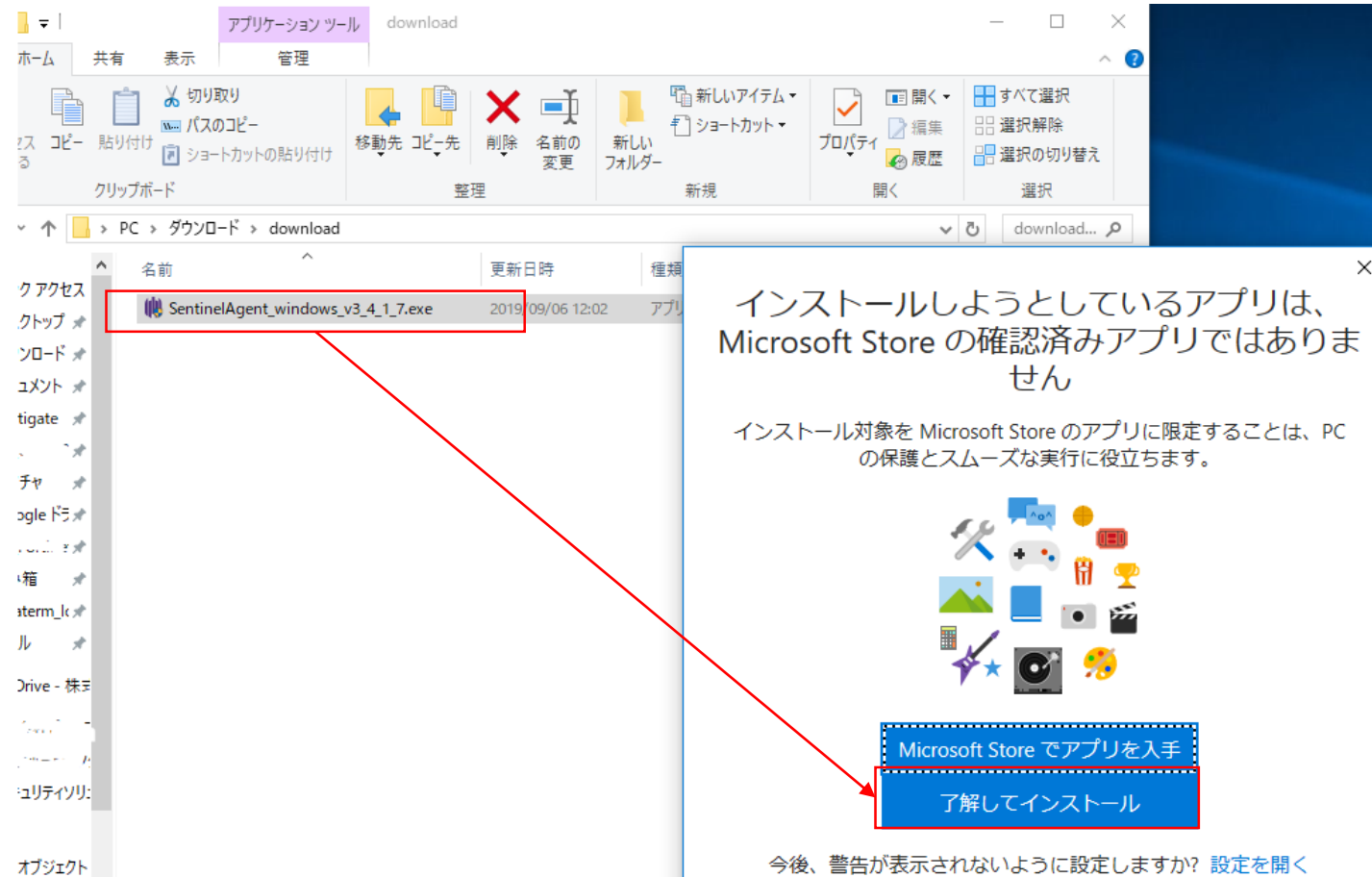
インストール時に入力を求められるキー、  
サイト毎に固有の値になっており、これにより接続先のサイトを識別する。

The screenshot shows the TTM (SentinelOne) web interface. The top navigation bar includes links for Dashboard, Visibility, Network, Analyze, Applications, and Activity. The main content area is titled 'Full site view' and contains tabs for ENDPOINTS, EXCLUSIONS, POLICY, DEVICE CONTROL, FIREWALL CONTROL, PACKAGES, BLACKLIST, and SITE INFO. The 'PACKAGES' tab is selected, displaying a table of installed packages. A red dashed box highlights the 'Site token' field, which contains a long alphanumeric string. A blue arrow points to the 'Copy' button next to the token. The 'Regenerate' button is also visible.

Version	Status	File Name	Scope	Available Date	SHA1
3.4.2657	GA	SentinelAgent_macos_v3_0_4_2657.pkg	Global	Jun 3, 2019 16:48:29	3e16f4727288b354dbabdadbf
5.5.1726	GA-SP4	SentinelAgent_linux_v2_6_5_1726.bsx	Global	Jun 3, 2019 16:48:21	22c008c5f4f83f894395cecefe

# インストール作業

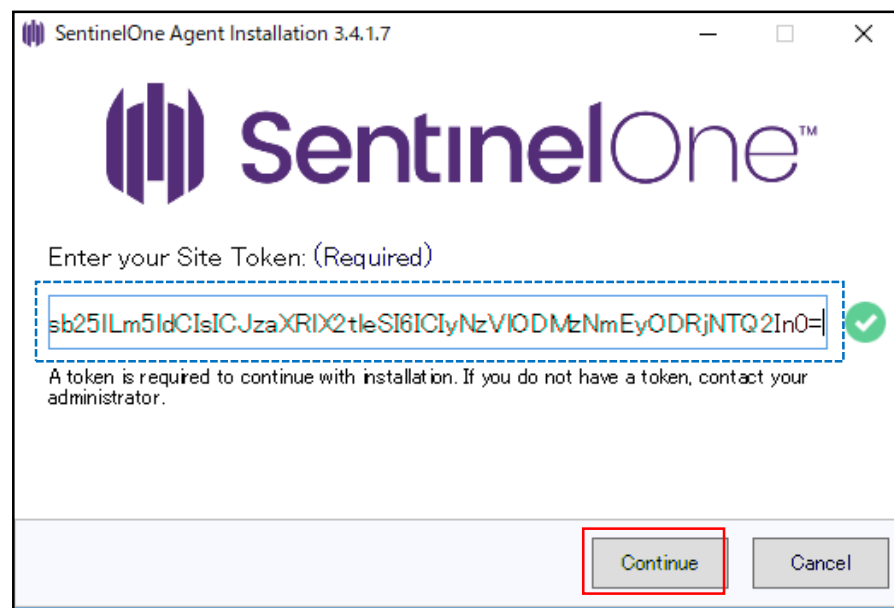
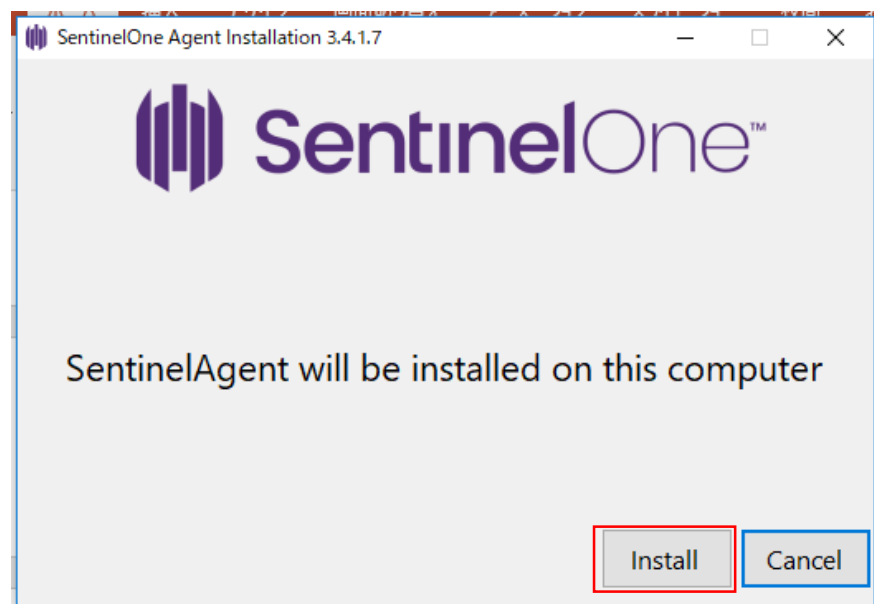
Windows10の例



# インストール作業

## -Site Tokenの入力

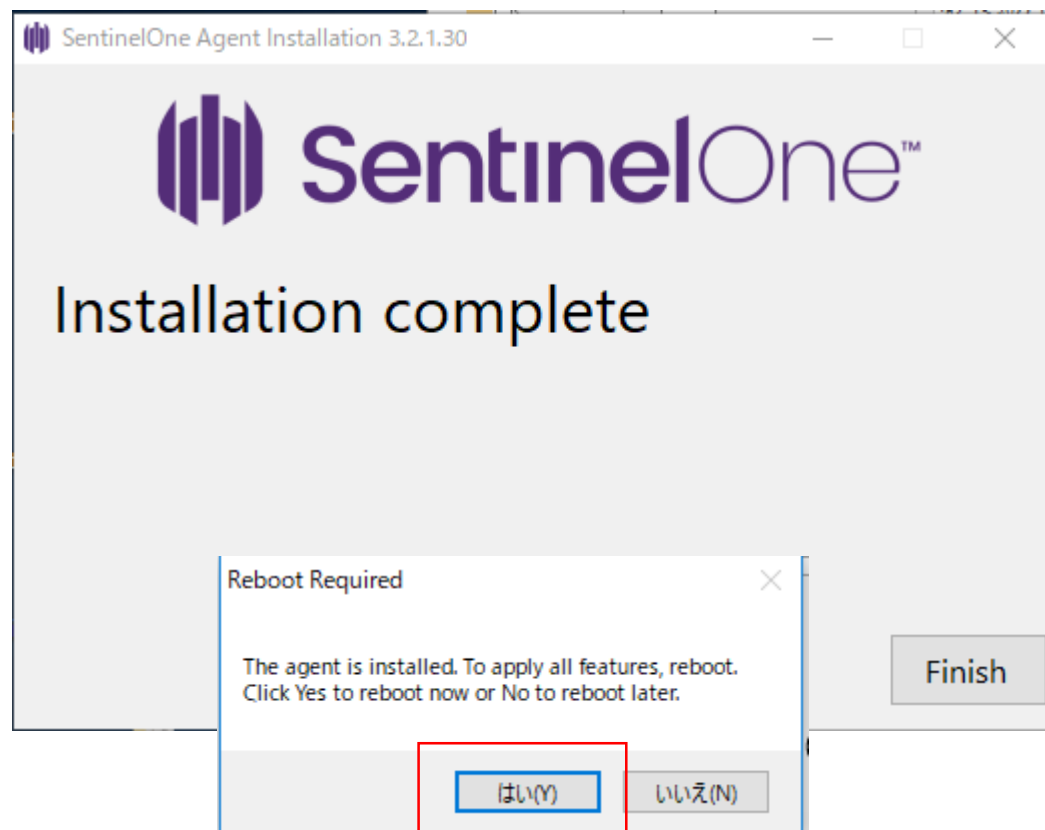
事前を取得しておいたSite Tokenを入力





# インストール完了

インストール完了後、端末の再起動が発生します



# デバイスの確認


ステータスがPendingになっている場合、初回再起動が完了していない事を示している。

TTM (SentinelOne)

NETWORK > Full site view > **ENDPOINTS** EXCLUSIONS POLICY DEVICE CONTROL FIREWALL CONTROL

Select filters...

Actions Group No Items Selected

<input type="checkbox"/>	Endpoint Name	Site	Last Logged In User	Group	Domain
<input type="checkbox"/>	 <b>DESKTOP-QJI503V</b> <u>Pending request</u>	TTM	Yamag	Default Group	WORKG

Pending

# アラートメールの設定

Settings -> NOTIFICATIONS -> Recipients

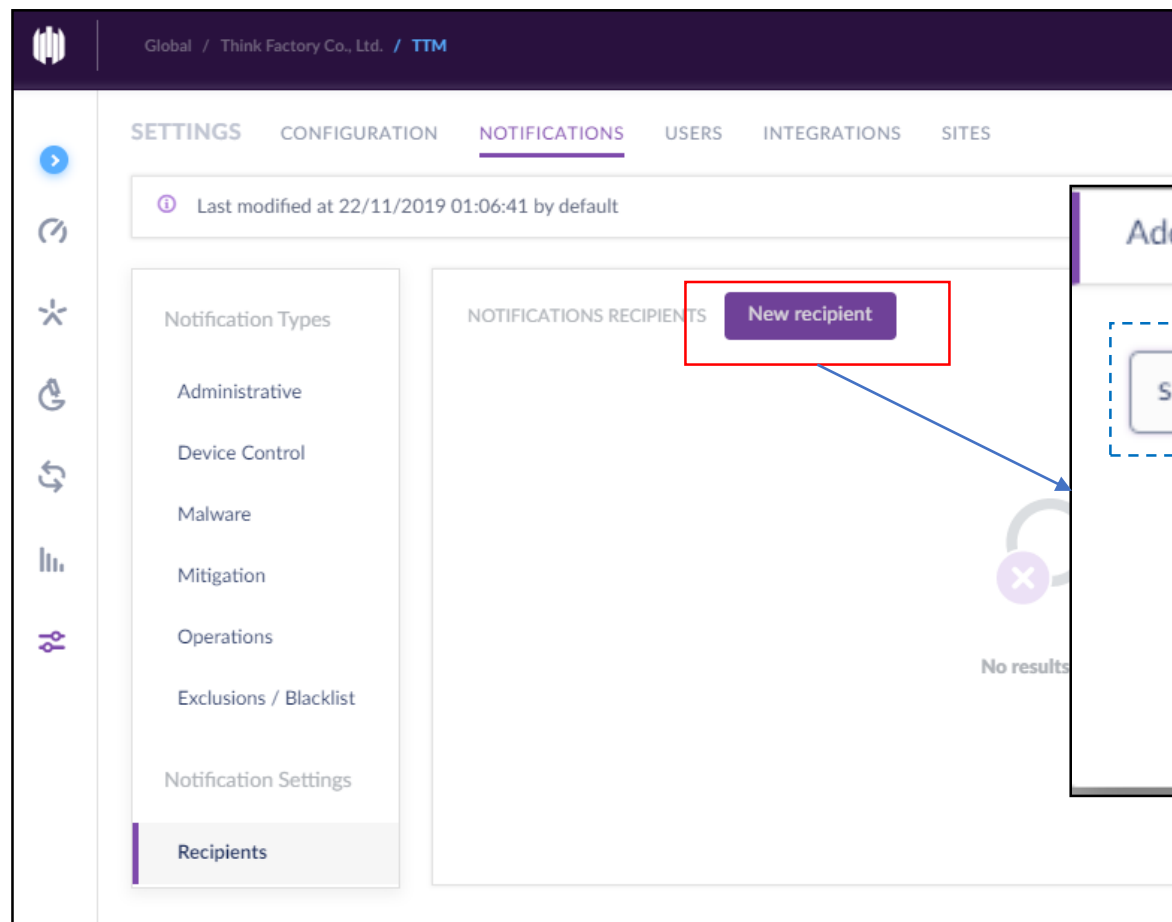
Settings

The screenshot shows the TTM settings interface. The 'SETTINGS' tab is selected in the top navigation bar. The left sidebar contains a list of settings categories: Notification Types, Administrative, Device Control, Malware, Mitigation, Operations, Exclusions / Blacklist, and Notification Settings. The 'Administrative' category is currently selected. The 'Recipients' option under 'Notification Settings' is highlighted with a red box. A blue arrow points from the 'Recipients' option to the 'NOTIFICATIONS' tab in the top navigation bar. Another blue arrow points from the 'NOTIFICATIONS' tab to the 'Recipients' option in the left sidebar. The main content area displays the 'ADMINISTRATIVE NOTIFICATIONS' settings. It includes a table with columns for 'Notification Type', 'Email', and 'Status'. The 'Email' column has a sub-header 'No Recipients, SMTP configured'. The 'Status' column has a sub-header 'No Sy'. The table lists various notification types with checkboxes for enabling email notifications. The 'Cloud marked the suspicious activity as resolved' notification type has its checkbox checked.

Notification Type	Email	Status
Notification recipients modified	No Recipients, SMTP configured	<input type="checkbox"/>
Agent Logging Aborted	No Recipients, SMTP configured	<input type="checkbox"/>
Agent UI Settings Modified	No Recipients, SMTP configured	<input type="checkbox"/>
Anti Tampering Modified	No Recipients, SMTP configured	<input type="checkbox"/>
Auto decommission configuration modified	No Recipients, SMTP configured	<input type="checkbox"/>
Auto decommission days modified	No Recipients, SMTP configured	<input type="checkbox"/>
Cloud marked the suspicious activity as resolved	No Recipients, SMTP configured	<input checked="" type="checkbox"/>
Cloud unresolved a threat	No Recipients, SMTP configured	<input type="checkbox"/>
Configuration action modified	No Recipients, SMTP configured	<input type="checkbox"/>

# アラートメールの設定

## -受信メールアドレスの指定



アラートを受け取るメールアドレスを指定

Add Recipient

support@test.com

Add recipient

Quit

# アラートメールの設定

## -アラートサンプル



管理画面へリダイレクトされるので、インシデント対応を実施します。



# 自動対応モードへの移行

Network -> POLICY

標準設定では、AIエンジンの調整期間として検知モードに設定されています。  
導入後、過検知が発生しない事を確認した上で、自動対応モードへの切り替えを推奨しています。

## [自動対応ポリシーの設定例]

- ① リスク高のマルウェアを検知した場合
- ② 自動でプロセス停止(Kill)、  
ファイルを隔離(Quarantine)
- ③ 自動ネットワーク遮断はしない

# アンインストール手順

2 種類のアンインストール方式があります

## ①PUSH方式アンインストール

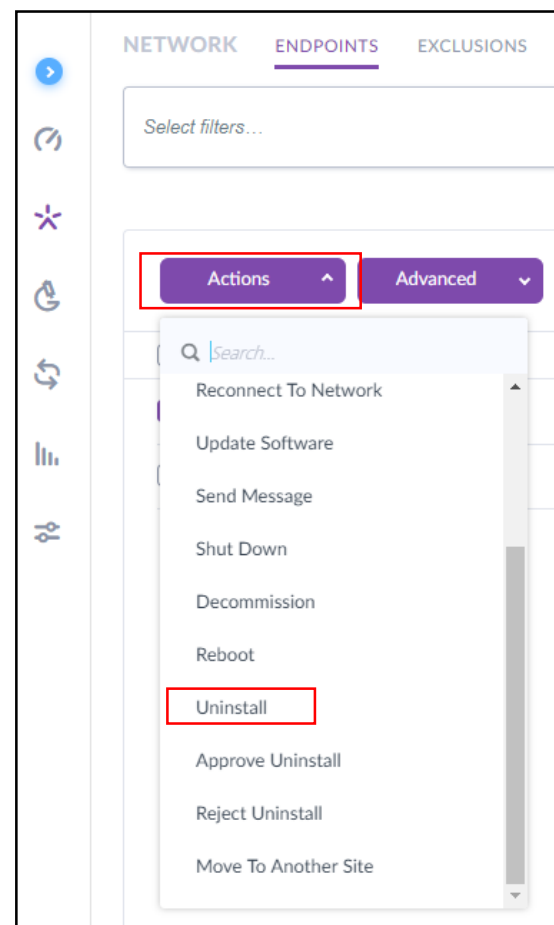
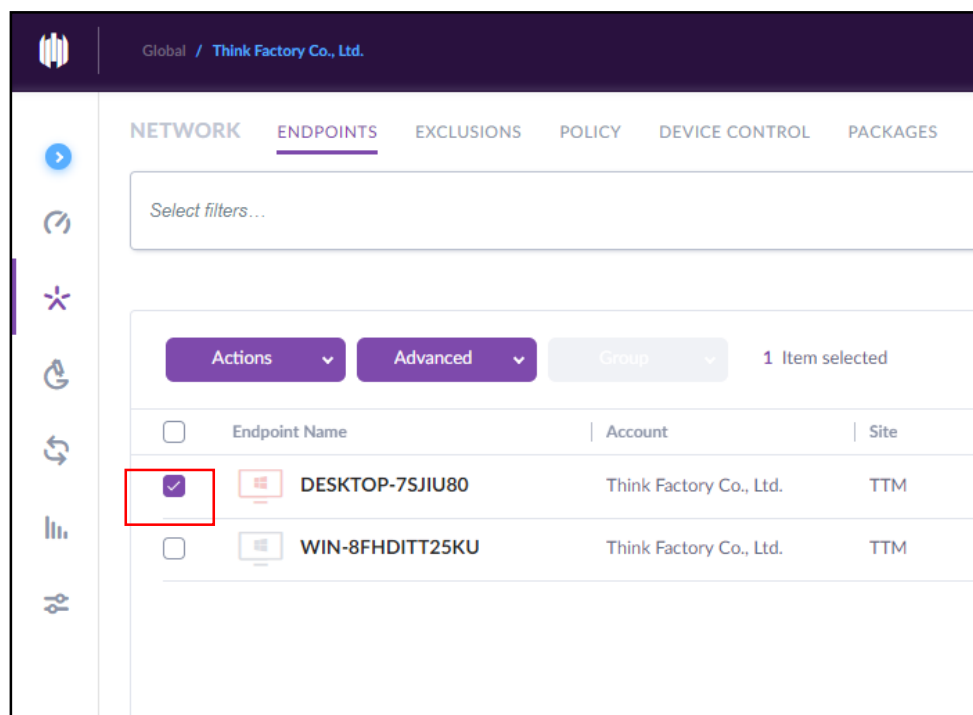
->管理者主導のサイレントアンインストールする方式

## ②リクエスト型アンインストール

->ユーザーが実施し、管理者が承認する方式

# アンインストールの方法① (Push型)

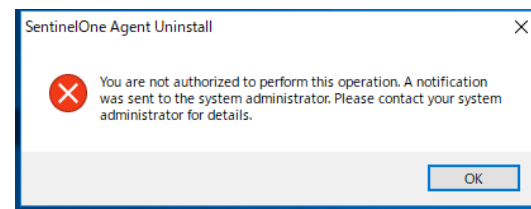
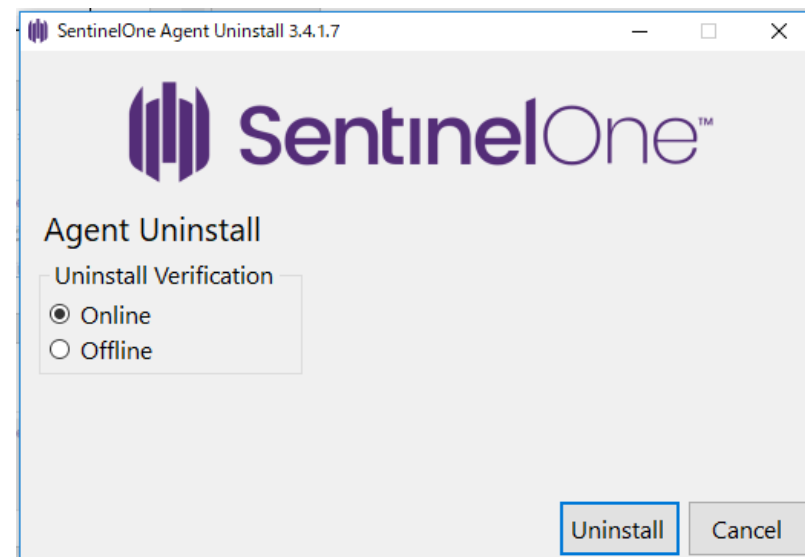
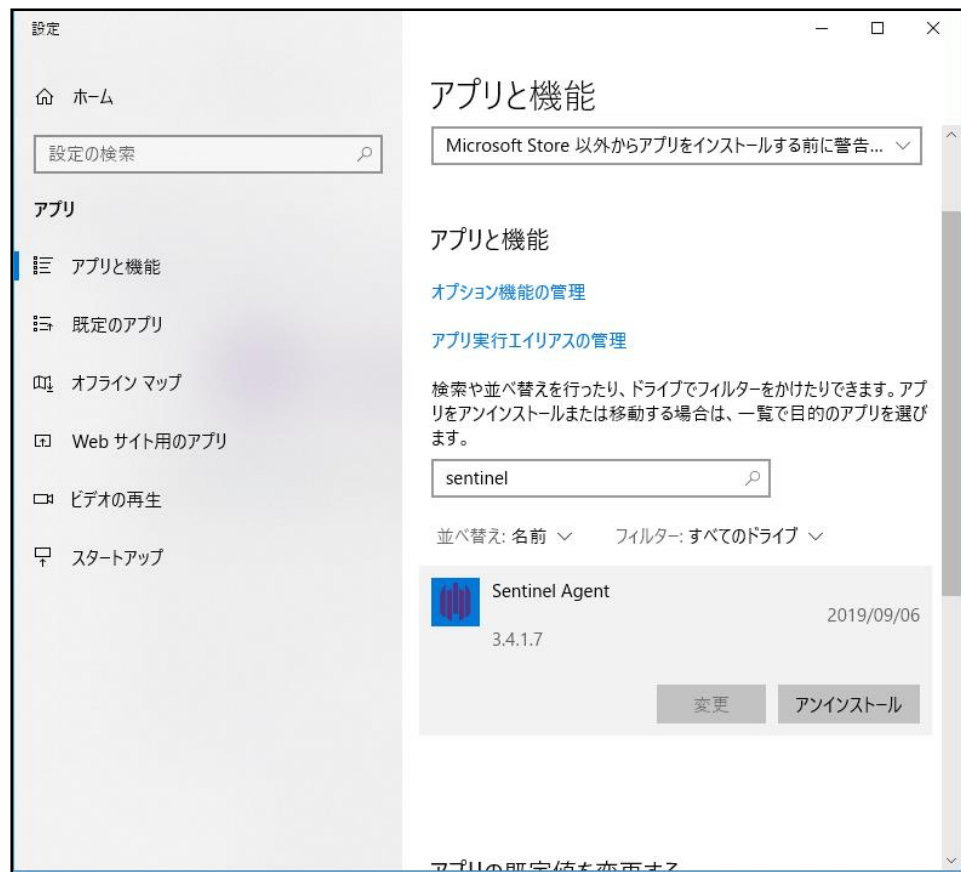
管理画面側からプッシュでアンインストールする。





# アンインストールの方法②（リクエスト型）

一旦アンインストール失敗する



# アンインストール許可

②（リクエスト型）

Pending requestになっているデバイスを選択

The screenshot illustrates the steps to approve the uninstallation of a device. It is divided into three main sections connected by blue arrows:

- Endpoint List:** A table with columns for selection, endpoint name, and account. The device **DESKTOP-QJI503V** is highlighted with a red box. It has a checkmark in the selection column and is marked as "Pending request" and "Pending Uninstall".
- Actions Menu:** A dropdown menu is open for the selected device. The "Approve Uninstall" option is highlighted with a red box.
- Confirmation Dialog:** A modal window titled "DESKTOP-QJI503V will be uninstalled. Do you want to continue?" is shown. The "Approve" button is highlighted with a red box.

アンインストールを許可する